# D4.4 Code of Best Practices for Investigation Order in criminal proceedings

Proposal for 100 Best Practices

**March 2019**

## Best practices for EUROpean COORDination on investigative measures and evidence gathering

"This report was funded by the European Union's Justice Programme (2014-2020)



http://eurocoord.eu

**Version** Final

**Preparation date**: February 2019

**Deliverable** D4.

**Work Package: 4**

**Authors:** Lorena Bachmaier Winter

**Approved by Coordinator on:** 11 March 2019

**Dissemination level:** Public

## Contents

## 1. LIST OF ABBREVIATIONS

AFSJ Area of Freedom, Security and Justice

CBP Code of Best Practices

CE Constitución Española ("Spanish Constitution")

CPC Italian Criminal Procedure Code

CJEU Court of Justice of the European Union

DEIO Directive regarding the European Investigation Order in criminal matters

EAW European Arrest Warrant

ECHR European Convention on Human Rights

ECtHR European Court of Human Rights

EDP European Delegated Prosecutor(s)

EEW European Evidence Warrant

EIO European Investigation Order

EOMF Estatuto Orgánico del Ministerio Fiscal español

EPO European Production/Preservation Order

EPOC European Production/Preservation Order Certificate

EPPO European Public Prosecutor's Office

EU European Union

FD Framework Decision

FD EAW Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between MSs

FGE Fiscalía General del Estado ("Public Prosecutor's Office")

ICPC Italian Criminal Procedure Code

ISP Internet Service Provider

It. Const. Italian Constitution

LD Legislative Decree

LECrim Ley de Enjuiciamiento Criminal española

LRM Ley 23/2014, de 20 de noviembre, de reconocimiento mutuo de resoluciones penales en la Unión Europea

LORPM Ley Orgánica Reguladora de la Responsabilidad penal del menor

MLA Mutual Legal Assistance

MS Member State(s)

OJ Official Journal

OLAF Office européen de lutte antifraud

PCPC Polish Criminal Procedure Code

PR EPO Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters, COM(2018) 225 final

STC Tribunal Constitucional Español ("Spanish Constitutional Court")

TEU Treaty on the European Union

TFEU Treaty on the Functioning of the European Union

TOC Transnational organised crime

UK United Kingdom

VAT Value-added Tax

## 2. Executive Summary

1. The implementation of the EIO represents a major step forward in the building up of a single Area of Freedom Security and Justice by simplifying the transnational gathering of evidence in criminal matters. The long road until the adoption of the Directive on the EIO shows how difficult it is to come to agreement in the field of criminal matters. The different level of protection of human rights and its diverse meaning in the different national Constitutions, still causes some reluctance towards the acceptance of the mutual recognition principle of certain investigative measures within criminal proceedings. Therefore, it would be unrealistic to think that the implementation of the EIO Directive will automatically change the system of cross-border collection of evidence or create a free movement area for the circulation of the criminal evidence, at least not immediately.
2. The EIO is an instrument based on the mutual recognition principle, but that still keeps many features of the former conventional mutual legal assistance principle. By introducing similar grounds for non-execution as those applied to the MLA system, the principle of mutual recognition is clearly nuanced: the idea that the executing authority will deal with the request made through the EIO as if it were a domestic judicial assistance request, is still quite far off. And it may not be possible to advance at a quicker pace towards a "single evidence area", because the free circulation of evidence still entails huge challenges for the national criminal justice systems, as well as for the protection of the fundamental rights of the defendants
3. In the drafting of this proposal for a Code of Best Practices (CBP), which aims at providing useful guidance in applying the EIO, the issue of striving the right balance between the efficiency in the cooperation and the protection of the fundamental rights and the fairness of the proceedings, has been a continuous challenge and it cannot be stated that the right balance has always been achieved. But it may be worth to explain that in proposing ways to act in the use of the EIO, the approach adopted has been the following: promote the principle "pro cooperation" in all cases where this would not harm or affect the level of protection of human rights.
4. In that context, three concepts can define the main features of the proposed best practices: flexibility, fluent communication and proportionality.
5. **Flexibility** should be the core principle to be applied with regard to the grounds for refusal. Being positive –and necessary– that the executing authorities are able to invoke a ground for refusal against the recognition or execution of an EIO when the cooperation requested would run counter their own security interests and their conception and regulation of the fundamental rights, flexibility is the main guideline to be applied. When facing a request via EIO, national competent authorities should not seek primarily for grounds for refusal, but they should rather, try to overcome those obstacles that hinder the cooperation.
6. This brings us to the second element, which is crucial for finding the right balance, the **principle of proportionality**. This third concept plays a main role in the present CBP as many of the guidelines are focused precisely on how to deal with the assessment of proportionality, both in the issuing and in the executing State.

Proportionality an necessity are the pre-requisite for granting any investigative measure that affects fundamental rights, and precisely in this context is were the diverse understanding of what is proportionate that can trigger several grounds for refusal.

7. Connected with such diversities, in overcoming all the possible obstacles and trying to promote the swift and smooth cooperation, the third element that is underlined in this CBP is the need for **communication:** States and every single practitioner shall endeavour to establish fluent consultation channels with the authorities of the other MSs involved in the issuing and execution of EIOs. Keeping open the channels for direct communication between the authorities involved, overcoming the legal obstacles as well as the cultural and linguistic barriers, is not only to be defined as the right attitude, but the only acceptable attitude in a single European AFSJ. The mentality of the judicial authorities involved has to evolve to see themselves as practitioners working in a single endeavour: the fight against cross-border crime with the respect of the rights of the defendant in such a transnational setting.
8. Having these three elements in mind –**flexibility**, **proportionality** and **continuous communication**– the Code of Best Practices has collected 100 guidelines that should aid in using the EIO. Each of those best practices is preceded by an analysis of the problems or questions detected, so that the reasons for defining the precise proposed best practice are made clear. Not all questions that may arise have been addressed, but those that have been identified as more relevant, be it because they affect fundamental rights, because they are already subject to much debate, because they affect numerous cases, or because they have a direct impact in the daily work of practitioners and the effectiveness of the judicial cooperation. Therefore issues that do not pose any legal or practical problems have been mostly disregarded. The project team is aware that this is not a complete guide, but it has nevertheless tried to be as comprehensive as possible.
9. Within those 100 best practices or guidelines, there are three which cannot strictly be defined as a "best practice" as they are more properly a legislative recommendation. The name recommendation has been kept in order to make clear the difference, although still included in the CBP.
10. Many of the guidelines are based on the practical experience the project team has been able to collect, although many other proposed guidelines are the result of our own desk research, as there was no practical experience on that. Nevertheless it has been considered useful to set guidelines on how certain provisions should be interpreted for the case the doubts arise in the practice.
11. Most of the best practices identified in the present Code have been subject to public discussion, in order to check them with practitioners, but not all of them could be subject to the public feedback, as they were collected only by the end of 2018, due to the delayed implementation of the DEIO in several countries. Further discussion might be needed, and this is why it has been opted to keep the form of "*proposed* best practice".
12. There is one important point that has not been included in the CBP, because it does not qualify as such. Nevertheless, it has been it should be stressed here that it should be considered the possibility of filing preliminary references to the ECJ during the pre-trial stage. As only judges are competent to file preliminary

references to the ECJ –while the majority of the EIOs will be handled by public prosecutors as judicial authorities under Article 2 DEIO–, in case of doubts regarding the interpretation of the EU law related to the EIO, it should be possible that a national judge could refer the questions to the ECJ. This would allow building up a uniform interpretation on the meaning of this legal instrument, which would benefit the protection of the defendant's rights as –strengthening the legal certainty and contributing to certain harmonisation– as well as the efficiency in the judicial cooperation.

13. The expectations put on the EIO are very high, and they should not be lowered or even destroyed in the process of transposing this Directive into the national legal orders. After more than a decade of efforts in negotiating this Directive, it is the moment for the MSs to ensure the efficient implementation of the EIO, demonstrating that an effective system of judicial cooperation in the gathering of evidence is one step forward in the establishment of the ASFJ, and that this can also be achieved in compliance with the fundamental rights of the defendants. Ensuring the rule of law in the European Union requires fighting cross-border criminality, but to that end, it is still necessary to keep on working on strengthening the mutual trust among the EU Member States. Steps should be taken also towards advancing in setting common standards on the admissibility –and thus also exclusionary rules– of evidence.
14. This CBP has been written by Prof. Dr. Lorena Bachmaier Winter, Full Professor of Complutense University and Prof. Dr. Marien Aguilera Morales, Professor of Complutense University, with the support of Dr. Costanza di Francesco. We would like to express our gratitude to all the practitioners that have shared generously their experience with us, as well as the rest of the members of the EuroCoord team, whose analysis on the three countries studies as served as a useful starting point in the drafting of this CBP.

## 3. INTRODUCTION

1. The final aim of the EuroCoord Project is to present a Code of Best Practices (CBP) on the use of the European Investigation Order (EIO) in the EU. A "Code" of best practices in the legal field tries to identify a set of guidelines and ideas that should represent the most efficient, logical, and useful course of action. It should highlight the most efficient way to apply the EIO in cross-border criminal investigations, and give guidance to those who will use it, mainly judges, public prosecutors, and defence lawyers on behalf of the defendants.
2. Best practices can be developed by a public authority, such as a regulator, a private governing or management body, or as in this case, a group of scholars, analysing the legal framework and the good practices identified in applying those laws. As in other fields –management or industry– the aim of a set of best practices is to give guidance for an efficient completion of tasks, by applying excellence standards. In the present case, differently from other branches where best practices are commonplace and are frequently based on measurable benchmarks and quality standards also subject to be quantified, efficient implementation and development of legal instruments, cannot be reduced to quantitative indicators. The implementation of the EIO and its best use is not linked mainly to a profit-cost analysis, but other variables play a much crucial role.
3. When addressing what should be the guidelines to be applied in using the EIO, a judicial cooperation instrument based on the mutual recognition principle, all perspectives and interests involved in the transnational criminal procedure have to be taken into account: the efficiency in managing the requests for cooperation –issuing, executing, transfer, admissibility of evidence–, as well as the protection of fundamental rights of the defendants and other parties acting in a criminal procedure. Efficiency in fighting crime –cross-border crime in this case– has to be assessed always *vis a vis* with the "excellence" in complying with the tasks of protecting the human rights.

4. Finding such a balance in a CBP on the EIO is nothing but easy, as all criminal law scholars, human rights organisations and policy-makers, very well know, and the danger in making the system more efficient for the prosecution in certain cases may end up in curtailing defence rights for which democratic societies have fought for centuries. Underlining these difficulties is important to make clear that in elaborating this CBP the drafters have focused both on providing guidance on the EIO to become an efficient tool in prosecuting transnational crime within the Area of Freedom, Security and Justice (AFSJ), but giving equal attention to the necessary procedural safeguards in the process of gathering evidence to ensure the fair trial rights.
5. A CBP in principle has no binding effect, no strict normative effect, as the addressees as a rule may opt to follow it or not. However, if the CBP is supported and adopted by a public authority, its effect would resemble to a recommendation –soft law at the best–, as best practices generally dictate the recommended course of action. Not following it or manifestly acting against it as a rule will not produce immediate legal consequences, but mainly a loss of opportunity in the path towards excellence in terms of efficiency and protection of human rights. In this exercise for identifying way for "excellence" and balancing the competing interests, the economic factor cannot be forgotten either. Despite the claim that this factor is by far not as relevant as the two others in achieving the objectives of the criminal procedure, it has nevertheless a huge impact in practice, and even more in international judicial cooperation practice.

### 3.1. Some remarks on the methodology

6. The initial proposal of this Project was based on the analysis of the rules and practical experience of three selected countries: Spain, Italy and Poland. The limited scope of the countries covered intended to gather an in-depth analysis of the rules and practice of these countries in cross-border criminal investigations and the use of the EIO, despite acknowledging its limits. The selection as based, not only upon affinity of the partners, but because these three countries present a highly interesting scenario in the filed of cross-border

criminality: Spain because of its geographical location has played an important role as the entrance way of drug trafficking operations coming from South American drug producers; Italy for its structural and historical experience in fighting mafia-type crimes; and Poland. The practice in Poland was to be followed, not only because of its importance as EU-border state –and therefore also suffering heavily the phenomenon of transnational organised crime (TOC)–, but also because the extensive use they have made in the past of the European Arrest Warrant (EAW) as issuing authority. This high number of EAW stemming from Poland triggered the heated debate on the proportionality principle in cross-border judicial cooperation. The strict application of the principle of legality in some countries (e.g. the Polish or the Czech criminal justice system) collided with the rational distribution of economic resources other MSs considered should be applied also in the criminal policy field.

7. While the choice of the three countries object of this study was completely justified, the partners in the project had to face several problems during the development of the tasks foreseen within the project. The first problem encountered was that at the time of preparing the first draft on the Code of Best Practices, there was no legal implementation nor practical experience in one of the chosen countries, namely in Spain. Due to the late transposition of the EIO Directive (DEIO), which only entered into force on the 2nd July 2018, until then no practical experience could be provided. With regard to the two other countries –Italy and Poland–, which had already transposed the Directive, there was hardly any practical experience in their use due to its recent transposition.
8. It is only during the second half of 2018 where some more meaningful data could be collected, mainly upon direct contacts with practitioners and some preliminary available statistics. This situation has clearly impacted the methodology initially foreseen for the drafting of this CBP. This explains, why the team entrusted with the draft of the CBP (Universidad Complutense), decided to gather information from other countries and complement the information found in the three national reports prepared by the EuroCoord partners with other sources.

9. In elaborating the set of guidelines which constitute the CBP on the EIO the first step consisted in identifying the problems in implementing the EIO. These problems are related either to the DEIO itself, to the legal framework adopted at the national level, to the resources devoted to the implementation –human and other resources–, or to other structural and/or institutional reasons. Once relevant problems were identified, the most salient ones were selected, in order to be addressed in the CBP. Therefore, this proposed CBP does not cover all possible issues that might appear in the using of the EIO in the EU, but only those aspects that might need additional clarification, a common approach or interpretation. The aim is not to provide a complete handbook on the use of the EIO, nor to present a deep study on all the problems detected, but to provide guidance in applying the instrument, precisely in areas where its implementation raises questions.
10. Finally, it was identified which standards were achieved –or should be achieved– in practice, trying where possible to quantify/qualify the problem to analyse the solution and draft the guideline. Checking these finding with practitioners has been done in as much as possible. Nevertheless, it has to be pointed out that the present CBP has not been tested in a scientific way. To achieve such a scientific conclusion, empirical testing of the proposed guidelines and thus the implementing of the identified best practices as an improvement measure and a solution to the problem detected, should be further followed.
11. Moreover, as mentioned above, the short time the EIO has been in force, has not allowed checking thoroughly the impact or even feasibility of certain standards identified as positive –present or future– practices. This means that the present Code of Best Practices can be viewed as a "work in progress", subject to further improvements and broader testing. This is the reason why many of the guidelines shall be presented rather than as an identified standard already applied, as the best answer to a problem that can arise. This option has been considered the most useful at the present scenario in order to be able to set out guidelines for future implementation in areas where the practice has not been established yet.

12. The purpose of this project is to identify practices that would aid in improving the implementation of the EIO in the whole EU, balancing the always present tension between efficiency in the investigation/prosecution of crime and the protection of fundamental rights. The aim is not to analyse how the future EU criminal policy and the EU judicial cooperation in criminal matters should be defined. EU legislative policy or setting guidelines in which direction should the EU advance in order to overcome the detected problems are objectives that fall out of this project, which is primarily focused in finding best practices and setting guidelines in the use of the EIO. This is important to underline, because being focused on the implementation of the EIO, any other critical analysis on what should had been done by the EU legislator or what could have been improved in the establishment of a set of rules in transnational criminal evidence, is beyond our scope.
13. The extensive literature on transnational evidence, the EIO and the protection of fundamental rights in the EU criminal proceedings has been identified and studied, but a detailed analysis of such important scholarly scientific production has only been taken into account in so far it might be useful for elaborating guidelines for the practical implementation.
14. Being the focus on the practical implementation of the EIO, to foster efficient cooperation in evidence gathering and transfer, while respecting fundamental rights in both executing and issuing State, a broader analysis on how this instrument is in compliance with the aims of establishing a single AFSJ, is a question that will not be further addressed. It goes without saying that in order to create a real single AFSJ, more approximation of the investigative measures and the procedural safeguards, as well as common rules on admissibility of evidence should be adopted. The EIO is still somewhat halfway between the mutual recognition principle and the traditional MLA instruments,[1] as the MS where not willing to advance further in harmonising investigative measures. It is true that the mutual trust which is the basis of the mutual recognition still needs

[1] See, for example E. Sellier, A. Weyembergh "Criminal procedural laws across the European Union – A comparative analysis of selected main differences and the impact they have over the development of EU legislation" study for the European Parliament, LIBE Committee (PE 604.977), 2018.

to be strengthened, because some MS still approach the cooperation proceedings with marked distrust. Although these shortcomings have been taken into account when elaborating the present proposal for a CBP, a critical analysis of the progress of the single AFSJ in criminal matters, has been deliberately left out in this project, as it only seeks to propose solutions to ensure that the EIO is used in an efficient, coherent way, providing legal certainty and that it serves to the purpose it has been adopted –to improve the efficiency of cooperation while safeguarding fundamental rights–.

15. The proposed CBP will include very precise guidelines, addressed at practitioners, but not general recommendations on legislative policy. It aims to provide a tool for practitioners to find guidance, not to set principles on how the AFSJ should be further built.
16. UCM team wants to thank all the stakeholders who have not only expressed their support in carrying out this research but have also actively help in identifying the problems and the possible solutions, have shared their positive and negative experiences and have generously devoted their time to filling out questionnaires and attending further queries. I want also to express my special gratitude to the International Cooperation Unit of the Spanish General Prosecutor's Office, the Spanish Desk of Eurojust, as well as the members of the EJN, who really contributed in identifying best (and worse) practices along diverse EU MSs, and allowed us to elaborate these guidelines beyond the domestic experience of the three MSs (Spain, Italy and Poland) the project is mainly focused on.

## 4. SCOPE OF APPLICATION OF THE EIO AND THE REPLACEMENT OF THE "CORRESPONDING PROVISIONS" UDNER ART. 34 DEIO

17. Starting from the definition of an EIO, the scope can be better identified: "an EIO is judicial decision which has been issued or validated by a judicial authority within criminal proceedings to carry out an investigative measure for gathering evidence within the EU, except those MSs which are not bound by it" (Art. 1 DEIO in connection with Art. 4 DEIO).
18. Any cross-border request for judicial cooperation for the gathering of evidence

in criminal proceedings shall be done by way of an EIO, except when its application is expressly excluded (as for the Joint Investigation Teams) or there is a specific provision that applies as *lex specialis*.[2]

Art. 34 DEIO establishes the replacement of the "corresponding provisions"[3]

19. Art. 34.1 DEIO reads:

> "Without prejudice to their application between MSs and third States and their temporary application by virtue of Article 35, this Directive replaces, as from 22 May 2017 the corresponding provisions of the following conventions applicable between the MSs bound by this Directive:
> (a) European Convention on Mutual Assistance in Criminal Matters of the Council of Europe of 20 April 1959, as well as its two additional protocols, and the bilateral agreements concluded pursuant to Article 26 thereof;
> (b) Convention implementing the Schengen Agreement;
> (c) Convention on Mutual Assistance in Criminal Matters between the MSs of the European Union and its protocol."

22. As the DEIO is not biding for Denmark and Ireland, the said MLA Conventions and other existing bilateral or multilateral agreements will continue to be applicable to the gathering of evidence in criminal matters to those Member States (MSs). While the territorial scope is clear, the material scope of the "replacement" is not so evident as it affects only to the "corresponding provisions" included in such conventional instruments. This term refers to the rules on cross-border gathering of evidence and only those are "replaced", albeit the specific repealing of the EEW by way of Regulation 2016/95, of 20 January 2016.

23. The DEIO only replaces "corresponding rules" of the Conventions listed under

[2] Requests for criminal records (Council Framework Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Record Information System (ECRIS)) or some requests on e-evidence under the Proposal for a Regulation on the European Preservation and Production Order (Proposal from the Commission for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters, COM/2018/225 final). The relationship between these two instruments will be discussed later.

[3] On the term "corresponding provisions", see the PhD work of T. Ramphal, "Conflict of Laws in Judicial Cooperation in Criminal Matters between the Member States of the European Union: the case of the European Investigation Order Directive", presented at the Leiden University in 2018, p. 27 ff. (used by courtesy of the author); see also the thorough analysis of Art. 34 DEIO by J. Espina, "The EIO and its relationship with other cooperation instruments: basic replacement and compatibility rules", *eucrim*, 2019 (forthcoming).

Art. 34.1 DEIO, but not other agreements or arrangements if those bilateral or multilateral instruments further strengthen the aims of the EIO, simplify the procedures and respect the level of safeguards set out in the DEIO. This means that DEIO is compatible with other bilateral agreements that provide an even more favourable legal framework for facilitating the cross-border evidence gathering, while respecting the same safeguards. In any event, the replacement rule is not affected by Art. 34.3 DEIO: even if the provisions of the Conventions listed under Art. 34.1 DEIO would be more favourable to the aims of the EIO, resorting to them would not be possible, as the replacement of theses rules is mandatory, regardless any other factors[4].

**1) Proposed best practice:** The MLA Conventions will also still be applicable to those acts of judicial cooperation that are not aimed at gathering evidence (not "corresponding provisions" pursuant Art. 34.1 DEIO), such as service of documents and summons (Art. 5 EU MLA Convention 2000), spontaneous exchange of information (Art. 7 EU MLA Convention 2000), returning of objects to the injured party (Art. 8 of EU MLA Convention 2000) or information with a view to opening proceedings by another country (Art. 21 EU MLA Convention 1959). Letters rogatory shall be used for requesting such judicial cooperation.

## 5. TYPES OF MEASURES: IDENTIFYING THE COERCIVE MEASURES

24. The DEIO covers all the investigative measures, except those that are specifically excluded. When regulating the requirements, the DEIO

[4] In favour of this interpretation, there is the CJEU judgment C-296/08, although related to the EAW, but which can be applied here in analogous way. Similarly to Art. 34 DEIO, Art. 31 FD EAW provided for a replacement rule, and in that regard the CJEU said: "Article 31(2) of the Framework Decision allows the Member States to continue to apply bilateral or multilateral agreements or arrangements in force at the time of adoption of the decision, or to conclude such bilateral or multilateral agreements or arrangements after the entry into force of the decision in so far as they allow the prescriptions of the decision to be extended or enlarged and help to simplify or facilitate further the procedures for surrender of persons who are the subject of European arrest warrants. However, that provision cannot refer to the conventions mentioned in Art. 31(1) of the Framework Decision, since the objective of the decision is precisely to replace them by a simpler and more effective system (...)" (paras. 54 and 55).

differentiates mainly between “coercive” and “non-coercive” measures. As it is known, there is not a uniform definition of what shall be considered a coercive measure, and the Explanatory Note of the DEIO does only give some hint: those measures affecting that do not infringe the right to privacy or the right to property are, for example, non-coercive measures (Recital 16).

25. While the DEIO does not define the concept of “coercive measures”, it requires different conditions and provides for different grounds for refusal for the EIOs related to coercive measures. This is why it is important to identify what is a coercive measure or not. The distinguishing feature of a coercive measure is whether it affects fundamental rights –of the suspect, the accused or a third party–, and whether the domestic legislation requires for such measure a judicial warrant.[5] Following these criteria, some measures may be considered coercive even though they do not imply coercion (e.g. interception of telephone and interception of telecommunications). On the other hand, there may be measures affecting fundamental rights –and all investigation measures affect in some way or another the fundamental rights of the individuals, precisely the privacy, albeit to a different extent–, that are not subject to judicial warrant and therefore the domestic law does not classify them within this category.
26. As has been mentioned, although the coercive nature of a measure is defined according to the domestic legislation of the MSs, the DEIO foresees a differentiated treatment depending on whether the measure requested is coercive or not. This different regime encompasses: (1) the duty/possibility of replacing the requested measure with another one; and (2) the grounds for refusal.
27. Thus, regarding the measures that are considered coercive under the national legal framework of a MS, the DEIO imposes their replacement when the investigative measure indicated in the EIO does not exist under the law of the State or it exists, but it would not be available in a similar domestic case (Art. 10 (1) DEIO). Furthermore, the executing authority may also have recourse to

[5] Recitals 16 and 30 DEIO.

an investigative measure other than that indicated in the EIO when the same result could be achieved through less intrusive means (Art. 10 (3) DEIO)[6]. Moreover, all the grounds for refusal are applicable to these measures, without any restriction.[7]

28. The rules are different for non-coercive measures under the national law of the executing state. On the one hand, non-coercive measures, as a rule, may not be replaced by the executing authority[8]. On the other hand, these measures are "immune" from certain grounds for refusal. In particular, they may not be refused upon lack of double incrimination, nor due to the fact that the measure is restricted to a list or category of offences or is punishable only by a certain threshold[9].

### 5.1. Coercive measures in Spain, Italy and Poland

29. Domestic legislation does not provide with a definition of "coercive measure" for the aims of application of the EIO. However, in the light of the implementation of Art. 10 (2) DEIO in Spain and Italy[10], it is confirmed that these measures are considered at the national level as "investigative measures which restrict fundamental rights[11]", as opposed to non-coercive measures.
30. Regarding the recourse to a different type of measures that the one indicated in the EIO, Spain has a complete correlation between coercive measures and measures restrictive of fundamental rights. Therefore, the Spanish executing authorities may (shall) switch investigative measure if they fulfil certain requirements; and the measures requested restrict the fundamental rights enshrined in the Spanish Constitution.

[6] This possibility turns into an obligation in Spain (Art. 206. 2 LRM), Italy (Art. 9 § 5 LD n. 108/2017, 21 June 2017).

[7] Art. 11 DEIO.

[8] Art.10 (2) d DEIO.

[9] Art.11 (2) DEIO.

[10] Poland is a special case. In this Country, Art. 10(2) DEIO has been implemented in Art. 589zi § CPC; this provision does not make any reference to fundamental rights.

[11] In Poland, these measures are considered as coercive measures in a broad sense or *measures for evidential purposes*.

31. In Italy, on the contrary, only those measures which affect the right to freedom and property, are considered coercive measures[12].
32. Nevertheless, the following schemes presents a non-exhaustive list of measures which fall within the scope of EIO application, divided between coercive or non-coercive measures in each of the three MSs studied:

| **SPAIN** | |
|---|---|
| **COERCIVE MEASURES** | **NON-COERCIVE MEASURES** |
| ○ Controlled deliveries of drugs and other prohibited substances (Art. 263 bis LECrim).<br><br>○ Infiltration by police officers[13] (Art. 282 bis LECrim).<br><br>○ Obtention of biological samples for DNA profiling, as well as inspections, recognition and physical intervention[14] (Art. 363. II, 778.3 and 520.6 c LECrim).<br><br>○ Entry and search of the premises or of the domicile[15] (Art. 545 ff. LECrim). | ○ Evidence necessary to prove the offence, such as the judicial inspection of the crime scene, the recovery of assets or proceeds derived from the offence or the autopsy (Art. 326 and ff. LECrim).<br><br>○ Evidence necessary to identify the offender and his circumstances as well as the identification parade, the photographic reconnaissance or the report on the conduct of the suspect (Art. 368 ff. LECrim).<br><br>○ Interrogation of the suspect (Art. 385 |

[12] Art. 9 § 5 LD in relation with Art. 13 and 14 It. Const.

[13] Art. 282 bis LECrim provides that this investigative technique can be authorised both by the judge and by the public prosecutor (who has to inform immediately the judge). However, it is only the judge who can authorise the infiltration of the so-called "IT undercover agent".

[14] This measure does not require a judicial authorisation nor the consent of the suspect when the obtaining of samples or biological traces does not entail a body searches, that is when "abandoned" biological are collected, STC 206/2007, 24 September 2007, and 199/2013, 5 December 2013, and 43/2014, 27 March 2014.

[15] No judicial authorisation is necessary for the entry and search of public spaces when there is no pending procedure. No judicial authority is necessary when the holder of the right

| | |
|---|---|
| | ff. LECrim) |
| ○ Detention and opening of written and telegraphic correspondence (Art. 579 ff. LECrim). | ○ Interrogation of the witnesses and the victim (Art. 410 ff. LECrim) |
| ○ **Search of documents or personal belongings** (Art. 573 ff. LECrim). | ○ **Confrontations between the suspect and/or the witnesses** (Art. 451 ff. LECrim) |
| ○ Interception of telephone and telematic communications (Art. 588 ter ff. LECrim). | ○ Expert evidence report (Art. 456 ff. LECrim) |
| ○ Access to electronic data or associated information held by the service providers (Art. 588 ter j LECrim). | ○ Access to the IP address of a device (Art. 588 ter k LECrim). |
| | ○ Identification of computer terminals through the capture of identification codes (Art. 588 ter l LECrim). |
| ○ Capturing and recording of oral communications using electronic means (Art. 588 quater a ff. LECrim). | ○ Identification of the owner or the data of any means of communication (Art. 588 ter m LECrim). |
| ○ **Use of technical devices to capture the image and tracking devices** (Art. 588.quinquies ff. LECrim). | ○ Order to retain data or information included in a computer system (Art. 588 octies LECrim). |
| ○ **Search of computers** (Art. 588 sexies a ff. LECrim). | |
| ○ **Remote search of computer** | |

to privacy concerned gives his consent or when there is a red handed offence (*fragrante delicto*) (Art. 18.2 CE); or in cases of exceptional or urgent need (Art. 553 LECrim).

| | |
|---|---|
| **equipment** (Art. 588 septies a LECrim). | |

| **ITALY** | |
|---|---|
| **COERCIVE MEASURES** | **NON-COERCIVE MEASURES** |
| ○ Check the identity of the suspect by taking fingerprints (Art. 349 § 2) or by taking a hair or saliva sample (Art. 349 § 2 *bis* ICPC)<br>○ Personal, home and electronic searches (Art. 352 ICPC)<br>○ Seizure (Art. 353 ICPC).<br>○ Forced collection of biological samples from living person (Art. 224 *bis* and 359 *bis* ICPC).<br>○ Inspections of persons, places and objects **(**Art. 244 and ff. ICPC).<br>○ Body searches, domicile searches (Art. 249 and ff. ICPC).<br>○ Seizure of correspondence (Art. 254), of electronic data at the premises of providers of computer, electronic and | ○ Check the identity of the suspect (for instance by the exhibition of personal documents) (Art. 349 § 1 ICPC)<br>○ Gathering information from the suspect (Art. 350 ICPC)<br>○ Gathering information from the person who may provide useful information for the investigation (Art. 351 and 362 ICPC)<br>○ Gathering information from a person co-accused in a joined proceedings (Art. 351 § 1 *bis* and 363 ICPC).<br>○ Not repeatable technical ascertainment (Art. 360 ICPC).<br>○ Informal identification of persons and objects (Art. 361 ICPC).<br>○ Confrontation among persons already examined or questioned (Art. 211 |

| | |
|---|---|
| telecommunication services (254-*bis* ICPC**)**.<br><br>○ Interception of face-to face conversations (Art. 266 § 2 ICPC)<br><br>○ Interception of telephone and electronic communications (Art. 266 ff. LECrim). | ICPC).<br><br>○ Identification of persons (Art. 213 ICPC)<br><br>○ Judicial simulation (Art. 218 ff. ICPC)<br><br>○ Expert evidence (Art. 220 ff. ICPC) where it does not require actions affecting personal freedom.<br><br>○ Documentary evidence (Art. 240 ff. ICPC)<br><br>○ Gathering of telephone traffic data (Art. 132 LD no. 196 of 30 June 2003; Art. 24 Law no. 167 of 20 November 2017) |

### 5.2. Is it possible to consider as coercive measures some of the investigative measures that can be ordered by the Public Prosecutor in Spain?

33. In Spain, the distinction between restrictive and non-restrictive measures of fundamental rights is relevant not only with regard to the application of Art. 10 and 11 DEIO, replacement and refusal of the requested measure)[16], but also with regard to the authorities competent to issue, recognise and execute an EIO[17].

[16] See also Art. 206 and 207 LRM.
[17] Art. 187 (1 and 2) LRM.

34. The problem remains how to identify those investigative measures that could be ordered by the public prosecutor despite affecting fundamental rights (e.g. controlled delivery of drugs, undercover police operations or investigation of assets)[18]. Can these measures be considered as coercive? The answer is not easy. For the aims of issuing an EIO, these measures may be considered as non-coercive, and thus they can be included in an EIO issued by the public prosecutor.

35. Viewed from the perspective of the execution, it would me more adequate to treat these measures as coercive measures, as this would allow to replace them for a less intrusive measure and also apply to them the so-called test of proportionality. This solution seems to be the most respectful with the protection of fundamental rights.

**2) Proposed best practice:** When the measure requested by the EIO is the controlled delivery of drugs or undercover police operations, the Spanish executing authorities shall treat these measures as measures restricting fundamental rights, with results in the ability to replace the measure or deny its recognition and implementation for any of the grounds for refusal foreseen by the LRM.

### 5.3. Shall non-coercive measures be automatically recognised in the executing State?

36. As has been seen, non-coercive measures are not subject to be substituted by other less restrictive measures: the presumption that they are available in every state applies, following Art. 10 (1) DEIO. But they are still subject to the grounds for refusal, although some of them will not apply to those measures.

37. Despite this limitation, it is however possible that the competent authority of the executing MS does not recognise the measure based on other grounds. So, for example, if the executing MS is Spain and the requested measure is the interrogation of a suspect who is under the age of 16, the execution of this

[18] See FGE, Circular 4/2013 of 30 December 2013 "sobre diligencias de investigación" ("Instructions of the Prosecutor's General Office on investigative measures"), pp. 19-25.

measure may be considered contrary to fundamental rights[19] and, thus, its recognition may be refused.

**3) Proposed best practice:** When the EIO requires the execution of a non-coercive measure, as a rule, the executing authority shall not analyse if it should be substituted by a less intrusive measure, and as a rule it shall not be refused, because such a measure shall exist in all MS. However, this does not mean that it shall be recognised automatically or that the general grounds for refusal do not apply.

## 6. TYPES OF PROCEEDINGS

### 6.1 Does the EIO apply to administrative sanctioning proceedings? Which ones?

38. The types of proceedings for which the EIO can be issued are defined under Art. 4 of the DEIO and these are criminal proceedings "brought by, or that may be brought before, a judicial authority in respect of a criminal offence under the national law of the issuing State" (para. (a)); or other administrative or judicial sanctioning proceedings, "where the decision can give rise to proceedings before a court having jurisdiction, in particular, in criminal matters" (paras. (b) and (c)). In other words, Art. 4 DEIO covers any procedure "criminal in nature" regardless how do the national laws label it, and regardless the type of authority that imposes the sanction, in so far, the proceedings may end up being revised before "in particular" a court with criminal jurisdiction.

39. This provision allows issuing EIOs within these types of proceedings. Neither in Italy, Spain or Poland exist these types of proceedings. It would cover the penal orders or road traffic administrative infringements (*Ordnungswidrigkeiten*) regulated, for example, in Germany. Art. 4 DEIO is clearly explained by the intention to include in its scope of application the administrative sanctioning proceedings that can be reviewed "in particular" before a criminal court. The boundaries of what is to be considered as "criminal proceedings" within the scope of the EIO are still somewhat vague.

[19] Art. 207(1) d LRM.

40. The CJEU had the opportunity to define this concept in the judgment on the case *Marián Baláž*[20], dealing with a fine imposed by an administrative authority (*Verwaltungsstrafbehörde*) for a road traffic offence to pay a fine of EUR 220, together with an imprisonment sanction in case the payment was not done within a certain time limit. The Austrian administrative authorities asked to a Court in the Czech Republic to recognize the certificate with the fine, as Mr Baláž had been informed of his right to challenge the decision before a court having jurisdiction "in particular" in criminal matters, which filed the preliminary question to the CJEU.

"(1) Must the term "court having jurisdiction in particular in criminal matters" in Article 1(a)(iii) [of the Framework Decision] be interpreted as an autonomous concept of European Union law?
(2a) If the answer to the first question is in the affirmative, what general defining characteristics must a court of a State which can, on the initiative of the person concerned, hear that person's case in relation to a decision issued by an authority other than a court of law (an administrative authority) have in order to qualify as a "court having jurisdiction in particular in criminal matters" within the meaning of Art. 1(a)(iii) of the Framework Decision?
(2b) May an Austrian independent administrative tribunal (unabhängiger Verwaltungssenat) be regarded as a "court having jurisdiction in particular in criminal matters" within the meaning of Art. 1(a)(iii) of the Framework Decision? (…)"

41. In her opinion[21] Advocate General Sharpston clearly opts for an autonomous concept of "court having jurisdiction in particular in criminal matters" and fills it in, not with a organic-organizational approach, but with a approach based on substantive and procedural guarantees

42. The CJEU did clearly follow the opinion of the Advocate General and decided thus that the concept of a "court having jurisdiction in particular in criminal matters" is an autonomous concept of Union law and must be interpreted as covering any court or tribunal which applies a procedure that satisfies the

[20] CJEU (Grand Chamber) C‑60/12, *Marián Baláž*, 14 November 2013.

essential characteristics of criminal procedure.[22] In other words, punitive administrative decisions that constitute a financial penalty also fall under the scope of the Framework Decision, but only if they comply with the procedural safeguards appropriate to criminal matters.

**4) Proposed best practice:** The EIO applies also to administrative sanctioning proceedings and administrative authorities –if recognized as competent authorities– can also issue EIOs, even for the purpose of administrative punitive enforcement, as long as the procedural safeguards appropriate to criminal matters do apply. In identifying if a certain administrative proceeding falls within the scope of the EIO, the criteria set out by the CJEU in the *Baláž* case are to be followed.

**6.2 Administrative proceedings for petty offences. Can a proportionality test be undertaken? By issuing authority, executing authority or both?**

43. The EIO does not establish a minimum threshold for issuing an EIO, save for certain measures and with regard to the double criminality requirement. This means that an EIO can be issued to obtain any kind of evidence for any kind of proceeding as long as it falls within Article 4 DEIO.
44. This has caused already a problematic situation with EIOs issued within administrative proceedings, when the proportionality is at stake. Should there be a kind of proportionality check in terms of cost-public interest before resorting to the judicial international cooperation by way of an EIO? This question will be addressed later, when dealing with the conditions for issuing an EIO, as the proportionality check is an element to be discussed with regard to any EIO, regardless the type of proceedings. Anyhow, it can already be advanced that the issuing authorities should undertake a check on the proportionality of the measure regarding the public interest and the costs, and the executing authority can activate the consultation procedure as established under Article 6.3 DEIO. On the other hand, if the information/evidence sought can be

[22] CJEU (Grand Chamber) C‑60/12, *Marián Baláž*, 14 November 2013, para. 42.

obtained by way of police cooperation or inter-administrative cooperation, those channels should be preferred.

**5) Proposed best practice:** The issuing authority within an administrative sanctioning procedure for a petty offence should evaluate whether it is proportional to issue an EIO for obtaining the information/evidence needed. MSs should elaborate internal instructions as to how the use of the EIO should be balanced against the possible costs that it may entail, when facing the sanctioning of a petty administrative offence. Information that can be obtained by way of police cooperation or cooperation with administrative bodies, such as the domicile of identity of a person, should be requested by those channels, rather than through an EIO.

### 6.1. The specific question of OLAF investigations: do they fall within the scope of an EIO?

45. OLAF is competent to exercise the powers of investigation conferred upon the Commission by the relevant Union acts, 'in order to step up the fight against fraud, corruption and any other illegal activity affecting the financial interests of the European Union'.
46. OLAF does not have sanctioning powers: OLAF's investigations conclude with a report that is sent to the national authorities, which are not compelled to take any action. This report indicates the facts established and the precise allegations, as well as recommendations on the appropriate follow-up to be undertaken at the national level. However the EU legal framework provides that the final report constitutes admissible evidence in administrative or judicial proceedings in the MSs in the same way and under the same conditions as administrative reports drawn up by national administrative inspectors. OLAF is thus de facto acting in the pre-field of criminal investigations and its legal framework obliges OLAF to apply with procedural safeguards that are common for criminal procedure as to secure the admissibility of evidence in the criminal law follow-up.

47. OLAF conducts proper autonomous investigations. Various investigative activities can be performed by OLAF investigation units; the most relevant, which require the authorisation of the Director-General, are: interviews with persons concerned and witnesses, the inspection of EU premises (in internal investigations) and on-the-spot checks of economic operators (in external investigations). As regards external investigations, OLAF can conduct on-the-spot checks according to Regulation No. 2988/95 and Regulation No. 2185/96. These regulations do not lay down an exhaustive EU law procedure, but refer to sectorial regulations and to national law. This entails that the extent of OLAF's powers may vary from one country to another. According to these regulations, checks and inspections shall be prepared and conducted in close cooperation with the MSs concerned; MSs' authorities may participate therein and normally they do so, at least at the beginning of the inspection; however, on-the-spot checks are carried out under OLAF's authority.
48. Within the scope of their investigations, could OLAF issue an EIO? The answer is not easy, because it is not properly a "criminal proceeding" to the aim of imposing a sanction, but rather a preliminary investigation that can trigger a criminal procedure and whose files can be used as criminal evidence.
49. No definitive answer can be given in this CBP regarding the use of the EIO within the OLAF investigation proceedings. Nevertheless, in so far as the division between administrative and criminal proceedings in some areas is blurred, it could be considered that the use of certain instruments of horizontal cooperation could be also applicable, under certain circumstances, in administrative investigations that are closely linked to a criminal procedure.
50. Although the implications of expanding the use of the EIO also by certain administrative authorities, have to be counterbalanced with an increase in the procedural safeguards for the persons investigated, it should not be excluded that OLAF could be regarded as "issuing authority" of an EIO, subject of course of validation by either a national authority involved in the investigation or by the EPPO, if the investigation falls within the competence of the EPPO.

**6) Proposed best practice:** Although a "best practice" cannot be identified or established here, but according to the autonomous concept of "criminal

proceedings" of the CJEU and the nature of the investigations carried out by OLAF, it should not be excluded that OLAF could issue EIOs, subject, of course, the required validation procedure by a "judicial authority".

### 6.2. How to deal with EIOs when it is not clear that it has been issued within a criminal proceeding (or proceedings under Art. 4 (b) and (c) DEIO)? Is the EIO limited to gathering evidence "for investigating a crime"?

51. The question arises in cases where the aim of "gathering evidence" would point to the EIO, but it is unclear if such a request is issued within a criminal procedure or within the aims of the criminal procedure. Recital 25 DEIO provides application of the DEIO for carrying out an investigative measure "at all stages of criminal proceedings, including the trial phase". "Including trial phase" is to be interpreted that beyond the sentence, an EIO could not be issued? Several examples will show the difficulties identified in this regard.
52. Example 1) Could an EIO be issued to gather evidence to find out the whereabouts of a person subject to a EAW, thus for the means of the enforcement of a detention order? The case took place in Spain, where another MS (Italy), after having issued an EAW, issued an EIO for intercepting communications of the person to be detained. The Spanish authorities refused the execution of such an EIO, on the grounds that the aim of such interception of the communications was not to gather evidence on a criminal offence, but to detain a person; and that the measure in Spain could only be executed within a criminal investigation, and a procedure on the execution of an EAW does not lead to the opening of a criminal investigation in Spain.

53. Example 2) A person convicted is released on parole and in order to check if he/she is complying with the conditional sentence (including e.g. ban to leave the country), could an EIO be issued to gather evidence on this infringement of the probation or conditional release? Could it be interpreted as an analogy to an "investigative measure within criminal proceedings", those issued for ensuring the enforcement of the sentence?

54. Cases where control on the enforcement of a sentence is needed, but that would not fall within the Framework Decision 2008/947/JHA[23] in so far the judgment and the probation decision had not been transferred to another MS (on reasons of the legal of residence of the sentenced person), could the EIO be used for gathering evidence in this context.

55. It could be argued that such a stage is part of the criminal proceedings, as in some MS the enforcement is within the jurisdiction of the criminal court or another judicial authority, and may be considered as part of the criminal procedure (e.g. Spain). However, in other MSs, the final judgment puts an end to the criminal procedure and other non judicial authorities are entrusted with the enforcement. The general term "criminal proceedings", does not give the precise answer on the scope of the EIO, as there is no uniform understanding on what the "criminal proceeding" entails (when it starts and when it ends).

56. Example 3) Could an EIO aimed at gathering bank information for the enforcement of a criminal conviction sentence that orders the confiscation of assets, be issued?
57. At the sight of these examples, it has to be recognised that there are arguments in favour and against extending the application of the EIO to the enforcement stage of a criminal sentence. In some cases such stage would amount to another ordinary criminal investigation. For example, in those systems where the breach of a protection order (or a ban to approach a certain person o place) would constitute another criminal offence: breach of sentence. Investigating if there has been such a breach would definitely fall within the concept of a criminal investigation.
58. Shall the solution to this question revolve around the definition of what is "criminal proceeding"? It seems that such an approach is not very useful, as it would lead us to confirm once again that there is no common uniform

[23] Council Framework Decision 2008/947/JHA of 27 November 2008 on the application of the principle of mutual recognition to judgments and probation decisions with a view to the supervision of probation measures and alternative sanctions.

understanding of the scope of "criminal proceedings".

59. On the other side, if the measure is not covered under the EIO, such evidence should be able to be requested via MLA Convention. Therefore refusing to apply/execute the EIO would mean, that the issuing authority should resort to the MLA rules. In practice this would mean, changing the forms, and issuing a letter rogatory for obtaining such evidence. This approach does not seem to be an efficient solution.

**7) Proposed best practice:** It is advocated to interpret the concept "criminal proceedings" also covering those stages that, according to the national law of the issuing State, are within the criminal jurisdiction, such as the enforcement stage or the breach of the conditions of parole.

### 6.3. Specific consideration to non-conviction based confiscation orders. Can an EIO be issued for gathering information/evidence about assets to be confiscated under a non-criminal confiscation procedure?

60. Within the system of non-criminal sanctions, the non-conviction based confiscation of assets merits a specific analysis. Following the 2005 United Nations Convention against Corruption[24] and the Council of Europe Conventions of 1990 and 2005 concerning confiscation of the proceeds of crime,[25] many countries have regulated non-conviction based confiscation or civil forfeiture measures for combatting serious offences –mainly corruption-related offences– which entail unjust enrichment. Within the European Union the EU Directive 2014/42 on "Non-conviction based confiscation" has set the legal framework for these measures.[26]

[24] See Art. 31.8: "States Parties may consider the possibility of requiring that an offender demonstrate the lawful origin of such alleged proceeds of crime or other property liable to confiscation…".

[25] ETS No. 141 and ETS No. 198. On the international instruments on confiscation of criminal assets, see generally N. Rodríguez García, "El decomiso de activos ilícitos", Cizur Menor, 2017, p. 55 ff.

[26] Directive 2014/42/EU of the European Parliament and of the Council of 3 April 2014 on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union, O.J. L127/39, 29.4.2014.

61. Although linked to criminal prevention, they are considered proceedings *in rem* and non-criminal sanctions. While closely linked to criminal acts and proceedings,[27] this type of confiscation can be applied without any link to the criminal conviction. For this reason it is described as preventive and also can qualify as a compensatory measure. Therefore the Strasbourg Court has examined these proceedings *in rem* under the civil limb of Art. 6 ECHR, with the consequence that the criminal procedure safeguards do not apply. It is accepted that when confiscation does not require a prior conviction because it targets the dangerousness of criminal property, it does not constitute a penalty.[28]
62. The Court has stated that, for the purposes of the civil limb of Art. 6.1 ECHR, there is nothing arbitrary in the reversal of the burden of proof onto the respondents in the forfeiture proceedings *in rem*, as long as there are substantiated facts of an enrichment that does not match with the income of the defendant.[29]
63. Nevertheless, due to their aims as crime-control measures, and without entering here at analysing the level of safeguards that these sanctions should comply with, for the aims of this CBP it has to be determined if an EIO could be issued within these proceedings. Could an EIO be issued to find out the location of the unlawful assets and to serve as evidence in these de facto punitive non-criminal proceedings?
64. If the aim of the judicial cooperation request is to freeze assets within criminal proceedings, such request would fall within the scope of the EIO according to Art. 4 DEIO. The next step would be to determine what is the aim sought with

[27] On the different types of non-conviction based confiscation measures in Europe see the comprehensive comparative analysis of J.P. Rui, U. Sieber, "Non-Conviction-Based Confiscation in Europe. Bringing the Picture Together", *in* Rui, J.P./Sieber, U. (eds.), *Non-Conviction-Based Confiscation in Europe*, Berlin, 2015, pp. 245-304.

[28] In this sense also J.P. Rui, U. Sieber, "Non-Conviction-Based Confiscation in Europe. Bringing the Picture Together", op. cit, pp. 254-55. M. Panzavolta, "Forfeiture and Fundamental Rights: Open Questions in the Twenty-First Century", *in* Ligeti K./Simonato M. (eds.), *Chasing Criminal Money. Challenges and Perspectives on Asset Recovery in the EU*, Oxford, 2017, pp. 25-52, p. 51.

[29] See ECHtR, *Grayson and Barnham v. the United Kingdom,* App no 19955/05, 15085/0623, September 2008. Although the Court has stated that in checking such factual basis, it will not act as a fourth judicial instance, therefore as a rule it will not question those domestic findings ECtHR*, Bochan v. Ukraine,* App no 22252/08, 5 February 2015.

the order of freezing assets, to use it as evidence or to apply the accessory consequence of confiscation of the proceeds of crime. In the first case, the EIO could be issued, in the second case, the specific EU instrument on the freezing and confiscation of assets should be applied.

65. More difficult is to determine how to proceed when the confiscation measure is requested without connection to a criminal conviction. The issue regards to the non-criminal forfeiture of assets, not related to a criminal conviction, in those proceedings where the confiscation is in itself the "sanction", but it can also be the evidence for imposing such "sanction".

66. First it has to be checked if such proceedings fall within the scope of Art. 4 DEIO. If they could be considered "criminal proceedings" following the autonomous concept of the CJEU, it should be admitted that such authority could issue an EIO. The next question is to determine what is the aim of the identification and freezing of the assets. Locating and identifying the assets of a certain "suspect" in this context is the prerequisite to apply the possible reversal of the burden of proof that would allow the confiscation of such assets as a "non-criminal" sanction. In strict terms the assets are not elements of proof of a criminal infringement, nor will they serve to proof an illicit activity, but serve as the basis of the presumption that, if their licit origins are not proven, it can be presumed they are illicit. Although not strictly aimed at being used as evidence of a criminal activity, they are requested for "evidentiary purposes", for being used as the basic fact to apply an evidentiary presumption.

**8) Proposed best practice:** It should be accepted that an EIO is issued for identifying and freezing assets to establish the factual basis of the non-conviction based confiscation measure. However, resorting to the EIO and justifying the use of this instrument because the close link of the assets to the evidentiary procedure, should not avoid to apply the rules on distribution of the sums confiscated among the MSs involved in such confiscation. Such distribution of assets should be governed by the rules provided in the Regulation (EU) 2018/1805 on the mutual recognition of freezing orders and

confiscation orders.[30]

### 6.4. Specific reference to the tracking devices or geo-location buggers on cars, vessels or other objects (with no interception of conversations)

67. Several questions have arisen already in practice, due to the diverse use of such tracking devices and also its different aim. When a car/vessel is being tracked with a geo-location device by the authorities in country A, and the car crosses the border and enters into another MS, or even crosses the territory of several MSs, how to proceed? Is the EIO applicable? Shall the measure be authorised? Under which circumstances?
68. First it has to be distinguished between the tracking that falls within police surveillance for cross-border pursuit; and a surveillance measure adopted within a criminal investigation. As noted above the rules on CISA will be applicable if it is a police surveillance measure.
69. If the tracking-up device has been installed for evidence purposes within a criminal procedure, such measure would fall within the scope of application of the DEIO. Next step is to identify, which rules of the DEIO are applicable.
70. Some countries have entered bilateral agreements to regulate these cross-border technical surveillance measures (Czech Republic), while others simply refuse such measures in their territory, for not being allowed under their domestic rules (Germany).
71. If the installing of a geo-location device in an object (car/vessel, or others) were to be considered an investigative measures implying the gathering of evidence in real time", Art. 28 DEIO would be applicable. If it were considered an interception of communication", then rules under 31 DEIO would be applicable. Technically if the device only records the movement of the object, it is not an "interception of communication" at least not a "human communication interception". The device may use however the same channels as those used for intercepting communications, in so far it resembles an "interception of

[30] Regulation (EU) 2018/1805 of the European Parliament and of the Council of 14 November 2018 on the mutual recognition of freezing orders and confiscation orders OJ L 303, 28.11.2018.

communication". The measure affects fundamental rights in a less intrusive way than the interception of communications, as it does not necessarily provide information of a person (differently from mobile phones which are generally more personalised items[31]).

72. As this investigative measure as a rule does not need technical assistance from the territory where the object is located, it would be sensible to apply Art. 31 DEIO: notify the relevant State where the object is located and from where it sends signals.

73. Practice seems to be diverse. Italy reports on the practice they have been experiencing with Germany, in the use of such devices: Italian authorities have acted following Art. 31.1 DEIO, and notified the relevant authority of such MS on the crossing of a tracked car; and Germany has ordered the measure to be stopped for not being provided in their territory (Art. 31.3 (a) DEIO in connection with 10.1 (a) DEIO). NE practitioner reported that if they foresee that the car/vessel is likely to cross the border, then they would issue an EIO and later ask for permission to use the information gathered as evidence.

**9) Proposed best practice:** The issuing State should notify the "affected" State (once they have knowledge of it), to make them aware of the "interception"; the notified State should not oppose to the measure on the sole ground that it is not provided in their territory. The treatment of this measure should not be equalled to a coercive measure[32] as it does not encroach seriously upon the privacy or the property or other fundamental rights. This is why the flexible approach of the "affected" territory is advisable. As to the admissibility of evidence, this should lie exclusively within the forum court.

### 6.5. Covert investigations, in particular on-line undercover investigations

74. Identifying best practices on the EIO regarding covert investigations (officers acting under covert or false identity) has not been possible, due to the secrecy and confidentiality rules that apply to them. Establishing guidelines on its use

[31] For example, US Supreme Court, *Carpenter v. United States*, Certiorari to the United States Court of Appeals for the Sixth Circuit, 22.6.2018.

[32] See Recital 16.

might not be appropriate within this project, not having such background information. Nevertheless, some comments are worth to be made here.

75. This measure is not subject to the principle of mutual recognition, as it requires in any event an agreement between issuing and executing State. Art. 29 DEIO mainly sets out this principle and which rules shall apply to the covert investigation (*lex loci*). So far, this investigative measure is relevant within the EIO as it may be requested through this channel, but it is governed by the rules both parties agree. However it is important to clarify here whether Art. 29 also applies to on-line covert investigations, where the covert investigative measure can be carried out without the technical assistance of the affected territory.
76. Such on-line covert investigations have a mixed nature as they entail at the same time the use of a covert or false identity, but it acts within the communication process, and it does record communications. In that vein, it affects to the right to the informational self-determination and also the right to privacy. The issue here is to determine which rules of the DEIO are applicable to this measure.
77. Three scenarios are to be distinguished: 1) the issuing State requests the executing State to carry out the measure by employing their own covert agent; 2) the requesting State seeks to employ its own covert agent, but needs technical assistance from the "affected" State; 3) the issuing State seeks to employ its won covert agent and does not need technical assistance from the other State.
78. The first situation is the one covered by Art. 29: an agreement is needed to carry out such an investigative measure. The second one is a covert investigation, but the assistance of the State is not strictly needed for the officers to act under covert or false identity: the false identity is given by the issuing authority and the support to keep such identity and introduce himself into the environment to be investigated is not technically needed.

**10) Proposed best practice:** If the assistance of another MS is required for the interception –but not for the covert operation–, then it appears reasonable that the rules for the EIO on interception of communications should be applied. We are inclined to support this interpretation, and not subject every on-line covert

investigation to the signature of a previous agreement. It would not be consistent with the logic of cyberspace and cybercrime investigations. Thus, the same requirements, conditions and grounds for refusal applicable to interception of telecommunications provided under Art. 30 DEIO, should apply.

79. The third situation, where not even the technical assistance is needed to carry out the covert on-line investigative measure, should respect the provisions under Art. 31 DEIO.

**11) Proposed best practice:** In cases where not even the technical support of the affected State is necessary to carry on the online covert investigation, provisions of Art. 31 DEIO should be followed: notify the other MS where the measure is going to have effects (if known), and the executing State at the view of the intrusiveness of such measure, should decide on it in accordance with Art. 31.3 DEIO. Same principles established for the measure on interception of telecommunications without technical assistance, are to be applied here.

## 7. RELATIONSHIP OF THE EIO WITH OTHER INSTRUMENTS

### 7.1. Exchange of information between tax administrations and the EIO

80. The request of tax data falls within the scope of the EIO in accordance with Art. 3 DEIO, and therefore it should be possible for the authority investigating a tax offence to issue an EIO –provided that the other conditions for it are given–, in order to collect the tax information needed for the criminal proceedings as covered by Art. 4 DEIO.

81. The question that arises here is which instrument should be used. Should the requesting authority prior to the issuing of the EIO ask the national tax agency to collect such information by way of means provided for under the Directive 2011/16/EU (from tax agency to tax agency)[33]? Could the information exchange

[33] Directive 2011/16/EU of 15 February 2011 on administrative cooperation in the field of taxation and repealing Directive 77/799/EEC. On this Directive see, for example, J.M. Calderón Carrero, "Hacia una nueva era de cooperación fiscal europea: las Directivas 2010/24 UE y 2011/16 UE de asistencia en la recaudación y de cooperación administrativa en materia fiscal", *Rev. Contabilidad y Tributación,* núm. 343, 2011, pp. 49-86; S. De Miguel Arias, "Algunos aspectos de la protección jurídica de los obligados tributarios ante los

regulated under Directive 2011/16/EU be used by the tax agencies for gaining access to data of a taxpayer for the purposes of a criminal investigation?

82. In principle, nothing should prevent the judicial authority investigating the criminal offence to claim the data needed directly from the tax authorities of the State of the forum, if those data are already within such tax administration. In this case, pursuant to Art. 16 of the Directive 2011/16, the information "communicated between MSs in any form pursuant to this Directive shall be covered by the obligation of official secrecy and enjoy the protection extended to similar information under the national law of the MS which received it". However, this same Art. authorizes the disclosure of the information transmitted from another State in two cases: "1) for the assessment and enforcement of other taxes and duties covered by Article 2 of Council Directive 2010/24/EU of 16 March 2010 concerning mutual assistance for the recovery of claims relating to taxes, duties and other measure; and 2) in connection with court and administrative proceedings that may involve penalties, initiated as a result of infringements of tax law, without prejudice to the general rules and provisions governing the rights of defendants and witnesses in such proceedings." It should be recalled that the EU Directive 2011/16 of 15 February 2011 does not apply to data related to VAT.

83. Following these provisions, should the investigating criminal authority, prior to issuing of the EIO, consider the possibility of getting such data from the domestic tax agency? When assessing the need and proportionality of the EIO, shall the issuing authority consider whether such data could be obtained without recourse to the international judicial cooperation?

84. From a practical standpoint, any judicial authority which knows or can foresee that information required for the tax offense criminal investigation may be obtained from its own national tax administration, will refrain from undertaking the efforts of issuing an EIO. To this end, the requesting authority should know whether the relevant information is already available at the national tax agency. This may not always be the case.

---

requerimientos de información en la Unión Europea", *in* F.A. García Prats (ed.), *Intercambio de información, blanqueo de capitales y lucha contra el fraude fiscal,* Madrid, 2014, pp. 379-397.

85. From the point of view of the assessment of the proportionality principle, Art. 6.1 DEIO does not seem to require that, prior to issuing an EIO the authority exhausts other ways of collecting the same evidence without recourse to international judicial cooperation. Art. 6.1 DEIO requires the issuing authority to assess the proportionality and necessity of the measure for the purposes of the criminal proceedings and on the other hand, the executing authority shall assess the proportionality of the measure requested to determine if the required information can be obtained by less intrusive means (Art. 10.3 DEIO). Apart from these situations, nowhere in the EIO Directive is it stated that its issuing is subsidiary of other instruments or ways to obtain the information or evidence required for the criminal proceedings. The subsidiarity of the EIO is neither a requisite for the issuing, nor could its execution be refused on the basis that the requesting authority could have obtained the evidence in its own country or through other mechanisms.

86. Finally, it would be questionable if the authority investigating the criminal tax offense, instead of issuing an EIO, should claim from the national tax agency that they request the tax information needed by way of the exchange system provided for under Directive 2011/16/EU, for the purposes of the criminal investigation. Within this project and with the information we have been able to collect from practitioners it can be concluded that the instrument of cooperation and exchange of information between tax administrations is not intended to serve for requesting evidence needed in criminal proceedings.

87. One thing is that the data transferred in the context of an administrative tax investigation can be used in criminal proceedings, but another thing altogether would be to understand that the information exchange channel between tax administrations could serve to circumvent the international judicial cooperation mechanisms. In support of this interpretation, it might be argued that Art. 1.3 EU Directive 2011/16 expressly states that the Directive "shall not affect the application in the MSs of the rules on mutual assistance in criminal matters". In any event, a much deeper analysis, taking into account the different regulations in the MSs, should be carried out. For the moment, following conclusion can be drawn:

**12) Proposed best practice:** The instrument of cooperation and exchange of information between tax administrations is not intended to serve for requesting evidence needed in criminal proceedings. Before issuing an EIO to request tax information needed for the criminal proceedings, the authority may check if such information is already within the tax authority of the forum, but this is not a pre-requisite to issue the EIO or to determine the necessity of the EIO.

### 7.2. Relationship between the EIO and Art. 29 of the EAW FD

88. Art. 29 of the EAW FD[34] on "Handing over property" reads:
89. "At the request of the issuing judicial authority or on its own initiative, the executing judicial authority shall, in accordance with its national law, seize and hand over property which:
90. (a) may be required as evidence, or
91. (b) has been acquired by the requested person as a result of the offence."
92. This rule was adopted in a time where there was no EIO, and thus it was considered convenient that within the surrender procedure, the property of the person subject to the EAW that might be necessary as evidence, be handed over together with the detained person. The same would apply to the proceeds of crime. Art. 34 on the DEIO (Relations to other legal instruments, agreements and arrangements) does nto make any refrence to the FD EAW. The question now is to determine if this rule has been superseded byt he EIO Directive in application of the principles of *lex posterior derogat anterior* and the principle of priority application of the *lex specialis*.
93. To answer this question, first it should be analysed if the provisions of the EIO are incompatible with those contained in Art. 29 FD EAW. This does not seem to be the case: it does not seem to be contradictory to request the property that might be needed as evidence within the EAW procedure: this would simplify the use of forms and the transfer proceedings of the property. However, Art. 29 FD EAW has a very limited scope, as it does only cover "property" of the person to

[34] Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between MSs.

be surrendered, and not investigative measures.

**13) Proposed best practice:** Within the EAW proceedings it is still possible to request property as defined under Art. 29 FD EAW to be sent together with the arrested person. This should not be considered as incompatible with the DEIO.

### 7.3. Cross-border evidence gathering in the EPPO Regulation: the EIO and the assignment system

94. The EPPO will be an indivisible Union body operating as one single Office as established in Article 8.1 of the Regulation. But for the purpose of obtaining evidence, it continues to operate on the basis of the principle of national territoriality, applying the national law of the place of execution to investigative measures.[35] With regard to cooperation in cross-border investigations, the first thing that the Regulation emphasizes is that the European Delegated Prosecutors (EDP) "shall act in close cooperation by assisting and regularly consulting each other in cross-border cases" (Article 31.1 Regulation). This is the basic premise that any system of international judicial cooperation should comply with, despite the fact that the EPPO cannot be classified as a model of inter-state cooperation, since the authorities that request and provide the cooperation are integrated into the same supranational structure. Once the EDPs are appointed by the European Public Prosecutor's Office, even though they keep their powers and functions as national prosecutors, they become part of the supranational structure at the decentralized level.

95. Since there will be at least two EDPs in each MS, the Regulation provides for cross-border cooperation to be carried out between them through the so-called "assignment system": the handling EDP assigns the needed measure to one of

[35] See also L. Kuhl, "The European Public Prosecutor's Office – more effective, equivalent and independent criminal prosecution against fraud?", *eucrim*, 2017/3, p. 139. On the negotiations regarding cross-border investigation of the EPPO and the assignment system, although with regard to the text before the adoption of the EPPO Regulation, see H.H. Herrnfeld, "The draft regulation on the establishment of the European Public Prosecutor's Office - issues of balance between prosecution and defence", *in* C. Briére, A. Weyembergh (eds.), *The needed balances in EU criminal law*, Oxford, 2017, pp. 382-412, pp. 402 ff.

the EDPs of the State where it has to be carried out (Article 31.1 EPPO Regulation).[36]

96. The measures that may be assigned are those listed in Article 30 of the Regulation, which are measures restrictive of fundamental rights that every MS must make available for these investigations, for cases where the offence has at least a maximum penalty of 4 years (Article 30.1)[37] and all other measures, which in principle are available according to national laws (Article 30.4). The EDPs in each MS will be competent to receive and execute the measures assigned by the handling EDP or by the EPPO itself.
97. The system of cross-border cooperation adopted in the Regulation seems to go one step further in the implementation of the principle of mutual recognition in the execution of cross-border evidence gathering: a request or an order will no longer be sent, but rather the handling EDP will simply assign the investigative measure. The "assignment" is not subject to any type of recognition procedure nor subject to conditions. Intentionally, the term "recognition" is ignored, most probably to make it clear that the authority providing the assistance does not carry out any oversight of the need, adequacy, or proportionality of the measure, nor of the *ne bis in idem* principle or any other formality.[38]
98. The Regulation also does not include grounds for refusal to execute the assignment. Any circumstance that might appear to affect the execution of the measure shall be communicated by the assisting EDP to his or her supervisor and to the handling EDP.
99. The approach is very clear: any problem arising with regard to the execution of the required (assigned) measure, shall be dealt with by both EDPs involved in order to try to find a solution by way of bilateral communication and together with the European Supervisory Prosecutor. In case a solution is not found within

[36] Precise functions and responsibilities will be regulated by the rules on the internal functioning of the EPPO to be adopted by the College, in accordance to Article 9 EPPO Regulation.

[37] See Article 30.1 EPPO Regulation.

[38] P. Csonka, C. Juszczak, E. Sason, "The establishment of the European Public Prosecutor's Office. The road from vision to reality", *eucrim* 2017/3, p. 129, call this as a *sui generis* system, away from the mutual legal assistance regime, as it entails the obligation to execute the assigned measure.

a period of 7 days "the matter will be referred to the competent Permanent Chamber" who will decide "in accordance with applicable national law as well as this Regulation" (Article 31.7 and 8 EPPO Regulation).

100. Once the assignment system has been briefly described, what has to be addressed here is the relationship between the provisions of the EPPO Regulation and the provisions of other "legal instruments of mutual recognition", in particular the EIO.

101. This relationship is precisely defined under Recital (73) of the EPPO Regulation, which reads[39]:

"The possibility foreseen in this Regulation to have recourse to legal instruments on mutual recognition or cross-border cooperation should not replace the specific rules on cross-border investigations under this Regulation. It should rather supplement them to ensure that, where a measure is necessary in a cross-border investigation but is not available in national law for a purely domestic situation, it can be used in accordance with national law implementing the relevant instrument, when conducting the investigation or prosecution."

102. The EPPO Directive clarifies that the rules on the assignment of cross-border investigative measures and the channels of communication foreseen in the EPPO are to be applied with preference to other mutual recognition instruments. That clarification is positive, although the second part of this Recital is difficult to understand.

103. As under Article 31.6 of the EPPO Regulation, it is stated that the instruments of mutual recognition will supplement the rules of this Regulation, in particular, with respect to measures not available in the national legislation of the assisting State for a purely domestic situation", but only for transnational proceedings. It should be understood that if such a measure has been foreseen in the executing (assigned) State for transnational criminal proceedings

[39] "The possibility foreseen in this Regulation to have recourse to legal instruments on mutual recognition or cross-border cooperation should not replace the specific rules on cross-border investigations under this Regulation. It should rather supplement them to ensure that, where a measure is necessary in a cross-border investigation but is not available in national law for a purely domestic situation, it can be used in accordance with national law implementing the relevant instrument, when conducting the investigation or prosecution."

according to the "national law implementing the relevant instrument", this measure as a rule should also be accessible for the EPPO investigations. Being regulated at the national level, it is not easy to determine how important it is that the measure is not accessible for exclusively national proceedings, taking into account that the competence of the EPPO will be exercised in cases that present transnational elements (Article 23 EPPO Regulation). The confusing wording of this rule does not allow proposing a clear interpretation for its future application.

104. On the other hand, the Regulation does not regulate EPPO cross-border investigations that will have to be carried out in a MS not participating in the enhanced cooperation,[40] or in a third State. Obviously in such cases the assignment system will not be applicable and the handling EDP will have to resort either to the rules of the EIO Directive or to international instruments of mutual legal assistance in criminal matters (with the two MSs to which the EIO is not applicable). In such cases the handling EDP shall act as the issuing or requesting authority of an EIO. The grounds for refusal will be those provided in such instruments[41].

105. It is too early to be able to determine how the EPPO assignment system and the EIO will interact in the future. Therefore at the present moment it is not possible to identify best practices in this field. However, what is clear is that the assignment system shall have preference to the EIO in the gathering of cross-border evidence in the criminal proceedings under the EPPO.

106. It is also possible to raise some questions that will need to be dealt in due time. First, as there are no grounds for refusal in the assignment system, it is difficult to assess how the assigned EDP will have to act when the requested

[40] See L. Salazar, "Definitivamente approvato il Regolamento istitutivo della Procura Europea (EPPO)", *Diritto Penale Contemporaneo*, 10/2017, p. 330; C. Di Francesco, "Repercussions of the establishment of the EPPO via enhanced cooperation. EPPO's added value and the possibility to extend its competence", *eucrim* 2017/3, p. 157 and 159.

[41] On the grounds for refusal under the EIO system see extensively, L. Bachmaier Winter, "The proposal for a Directive on the European Investigation Order and the grounds for refusal. A critical assessment", *in* S. Ruggeri (ed.), *Transnational evidence and multicultural inquiries in Europe*, Heidelberg, 2014, p. 71 ff.; A. Mangiaracina, "A new and controversial scenario in the gathering of evidence at the European level: the proposal for a Directive on the European Investigation Order", *Utrecht Law Rev*, 2014, 10, p. 116 ff.

measure is not foreseen in the executing MS, or would not be available for a similar domestic case. It seems clear that, such situation will be discussed with the handling EDP and the supervisor in order to substitute the measure or gather the evidence in a diverse way, always complying with the *lex loci.* The assignment system is designed to be more flexible and the fluent communication among the EDPs shall not make necessary the establishing of precise grounds for refusal.

107. On the other hand, while the EIO shall continue to be used with regard to the MS that are not participating in the enhanced cooperation, it should be determined whether the defendant in the EPPO proceedings would be allowed to request cross-border evidence via EIO.

**14) Proposed best practice:** As set out in the EPPO Regulation's Explanatory Memorandum, the assignment system does not replace the EIO, but supplements it. Therefore, in all other aspects not covered by the EPPO assignment system the EIO shall continue being applicable. Therefore, the defendant will be able to make use of it as provided under Article 1.3 DEIO.

**15) Proposed best practice:** Other rules provided in the DEIO for ensuring the fairness of the proceedings in the cross-border evidence proceedings, shall also be applicable to the EPPO assignment procedure. This applies specifically to the provision foreseen in Article 14.7 DEIO: "Without prejudice to national procedural rules MSs shall ensure that in criminal proceedings in the issuing State the rights of the defence and the fairness of the proceedings are respected when assessing evidence obtained through the EIO."

### 7.4. EIO and the future production and preservation order for e-evidence

108. On 17 April 2018 the EU adopted the proposal for a Regulation on e-evidence production and preservation orders (PR EPO).[42] This legislative

[42] Proposal for a Regulation of the European Parliament and the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM(2018) 225 final. On this Proposal see, among others, V. Mitsilegas, "The privatisation of mutual trust in Europe's area of criminal justice: The case of e-evidence", *Maastricht Journal of European and Comparative Law* 2018, Vol. 25(3), pp. 263–265; V. Franssen, "The European Commission's E-evidence Proposal: Toward an EU-wide Obligation for Service Providers to Cooperate with Law Enforcement?", *European Law Blog*, October 12, 2018, available at

initiative of the EU Commission tries to improve one of the problems in the access to e-evidence in the EU-USA transatlantic relationship. Only in 2014 there were 1700 MLA requests sent from EU MSs to USA, and 400 from USA to the EU MSs. Many of those MLA requests issued by authorities of the MS of the EU were related to e-data held by Internet Service Provider (ISP) companies. Due to this increasing number of requests for e-evidence, experts found that a new instrument that would allow the direct request/order to be sent directly to the ISP company could help in overcoming the complex judicial cooperation via MLA requests. It has to be noted also that many requests issued by authorities of EU MSs were refused on the basis that the standard for privacy encroachments according to US constitutional law, which requires probable cause, were not met.

109. The proposed Regulation seeks to reduce the level of complexity and fragmentation in obtaining e-evidence, reduce the costs of those proceedings for collecting evidence abroad, increase the effectiveness and expedite the judicial cooperation, while strengthening also the level of legal certainty.[43]

110. The proposed Regulation on the production/preservation order (EPO) is applicable only for the gathering of electronic stored data –data held by an ISP at the time of receipt of the order–, regardless where they are located. "It does not stipulate a general data retention obligation, nor does it authorise interception of data or obtaining to data stored at a future point in time from the receipt of a production or preservation order certificate."[44] A European Production Order Certificate (EPOC) is a binding decision issued or validated by a judicial authority of a MS compelling an ISP which offers its services in the EU

---

http://europeanlawblog.eu/2018/10/12/the-european-commissions-e-evidence-proposal-toward-an-eu-wide-obligation-for-service-providers-to-cooperate-with-law-enforcement/;
L. Buono, "The genesis of the European Union's new proposed legal instrument(s) on e-evidence Towards the EU Production and Preservation Orders," *ERA Forum,* 3.9. 2018, accesible at https://doi.org/10.1007/s12027-018-0525-4

[43] As stated in the Explanatory Memorandum, p.9: "The initiative is expected to enable more effective and efficient investigations and prosecutions while improving transparency and accountability and ensuring respect of fundamental rights. It is also expected to foster trust in the digital single market by improving security and reducing the perception of impunity for crimes committed on or through networked devices".

[44] See *Whereas* (19).

and is established or represented in another MS, to produce electronic evidence (Article 2.1 PR EPO). This EPOC requires –save when only subscriber data are requested– that it is issued within criminal proceedings or proceedings related to criminal offences of legal persons which are punished with more tan three years or crimes committed by means of an information system (Articles 5 and 6). This threshold, as stated already, does not apply to the request of subscriber data.

111. The main novelty of the cooperation system of this proposed Regulation, apart of course of the obligations established for the ISP to provide the requested data regardless where they are located, is that the order shall be sent directly by the issuing authority to the legal representative designated by the ISP for the purpose of gathering evidence in criminal proceedings (Article 7.1). The EPOC will thus circulate within the EU territory, without being subject to the prior recognition by the judicial authorities of the State where the representative of the ISP is located (or if no legal representative has been designated, where any establishment of the service provider in the EU is located). Upon receipt, the addressee of the EPOC shall provide the data requested directly to the issuing authority within the established deadline and can claim the reimbursement of the costs incurred. The judicial authorities of the State where the "executing" ISP is located, will play a role only when called upon by the ISP in the cases defined under Article 9.5 PR EPO: when it considers that the order manifestly violates the EU Charter of Fundamental Rights or is manifestly abusive.

112. The analysis of this judicial cooperation instrument in criminal matters lies beyond the aims of this CBP, and therefore, after this brief description of the proposed e-evidence production/preservation order, what is relevant here is to explain the relationship/interaction between the two instruments. Taking into account that at present there is only a Proposal for a Regulation and that its text may change along the legislative process, it is nevertheless worth to address some of the questions that might appear in the future once the PR EPO is adopted. The diverse impact and regulation of the grounds for refusal will not be discussed here, neither will the formal requirements be mentioned, not

being sensible to enter into those details, when there is no definitive text of the Regulation.

113. The PR EPO specifically addresses the relationship between the EPO and the EIO in Article 23 PR EPO, which reads:

114. "Member States' authorities may continue to issue European Investigation Orders in accordance with Directive 2014/41/EU for the gathering of evidence that would also fall within the scope of this Regulation."

115. Out of this provision, it is clear that the EPO will not replace the EIO, nor does the Regulation impose the use of the EPO over the EIO for gathering e-evidence. It could be understood that the issuing authority will be free to choose between the two instruments when there is need to request e-evidence held by an ISP, but this is not clear, as will be explained next.

***a) The EPOC vis a vis the EIO, interchangeable instruments or not?***

116. As stated earlier, the PR EPO seeks to overcome the MLA requests to the USA authorities to obtain e-data stored by US ISP companies. The most significant improvement is precisely obliging the ISP companies that offer services in the EU to provide the e-data stored by them when needed by a judicial authority for criminal proceedings, regardless where the data are located and where the seat of the company is located. This is the main advantage that the implementation of this proposed Regulation will represent: avoiding to have to go through the US courts and the complex MLA requirements to obtain data from ISP companies that operate in the EU. The fact that, in addition to such obligation, the request can be sent directly to the ISP company and that the company has to respond directly to a foreign judicial authority of an EU MS, is an innovation, but less meaningful than the obligation of those companies operating in the EU to provide the e-data. The possibility to handle the EPOC directly between the ISP and the requesting authority avoids the overloading of the judicial authorities of the relevant country where the legal representative of the ISP is located.

**16) Recommendation:** Once it is established that the ISP operating in the EU are obliged to produce e-data when requested by a EU judicial authority –regardless

the location of the data–, it is unclear whether such obligation shall apply only within the scope of application of the EPO Regulation or if it could be understood that it also should apply to any request of e-evidence, regardless if it is transmitted by way of an EIO or an EPOC. As for now, this aspect is not clear, and therefore, until the Regulation on the EPO is adopted, it would be unreasonable to try to set any guideline in this regard. At this moment it can only be proposed, that the future text of the Regulation, if finally adopted, clarifies this point.

***b) Once the compatibility of these two instruments has been explained, what shall be the criteria for the issuing authority to make the decision of choosing the EPO or the EIO? When should he/she make use of the EPO and when resort to the EIO?***

117. If the previous question is answered in the positive and the ISP company is obliged to produce the data independently where they are physically stored, in order to decide whether to issue an EIO or an EPO, the issuing authority shall first check if the offence falls within the scope of application of the EIO and/or the EPO. The type of proceedings covered are not the same, as under the EPO it is more restricted, as it does not cover the same administrative proceedings as covered by the DEIO (Article 3.2 PR EPO, in comparison to Article 4 DEIO).

118. Second, the offences for whose investigation an EPO can be issued are the ones listed under Article 5.3 PR EPO. If the offence is not included in that provision, the EIO will be the only choice. If there is the possibility to choose, the issuing authority shall take into consideration, if the e-evidence is the only evidence quested or not.

119. If only stored e-evidence held by ISP is needed by the issuing authority, it might be swifter to make use of the EPOC than issuing an EIO: the transfer of the request should be quicker as the process for recognition by an executing judicial authority of another EU MS would in principle be avoided.

**17) Proposed best practice:** For practical reasons, when the issuing authority only needs stored e-evidence for the purpose of the criminal proceedings, he/she should opt for the issuing of an EPOC, which should in principle be quicker and easier to handle. However, if the issuing authority is requesting to

the same MS also other types of evidence, it might not be worth to fragment the request, and it would be probably easier to issue an EIO for requesting jointly all the evidence requested from the same MS.

## 8. COMPETENT AUTHORITIES

### 8.1. Preliminary considerations

120. The designation of the authorities competent to issue an EIO, to recognise and to execute is a MS's task/duty. In this endeavour the wide margins provided for in Art. 2 DEIO shall be respected.

121. Using the possibility established in Art. 7 (3) DEIO, the MSs may also designate a central authority in order to assist the competent authorities in the framework of the EIO and to channel its administrative transmission and receipt. From the information sent by the MSs bound by the DEIO[45] to the Commission with regard to those authorities, it can be deduced what follows:

*«Issuing authorities»*

122. Most of the States have designated as issuing authorities the judge/judicial authority and/or the public prosecutor, as those are the authorities competent to order the gathering of evidence in domestic criminal investigations. Spain and Italy only recognise as issuing authorities judges and PPs[46], therefore in these two countries the validation procedure does not apply [Art. 2 (c) ii) DEIO].

123. In addition to the judge/judicial authority and/or the public prosecutor, some other MS have designated as issuing authorities certain administrative and law enforcement institutions or bodies competent to carry out investigations under their national law. This is the case, among others, of Poland, where the EIO may be issued by a court or by the public prosecutor

[45] Denmark and Ireland have not acceded to the DEIO. The United Kingdom, however, adapted its national law to the Directive, but due to the uncertain conditions of the Brexit, it is unclear how the EIO will be implemented after the date provided for the exit of the UK. On this issue, se below.

[46] Art. 187(1) LRM and Art. 27(1) LD n. 108/2017, 21 June 2017.

within their respective spheres of competence[47], but also by the police after validation by the public prosecutor[48].

*«Receiving, recognising and executing authorities»*

124. The States studied have opted for granting the same authorities the task of receiving the EIO and deciding over its recognition and execution, save certain exceptions.

125. In Poland the authority competent to receive the EIO and to proceed with its recognition and execution changes depending on the moment when the order has been issued. If the EIO is issued during the pre-trial stage, the competent authority to execute it as a rule will be the PP. However, if the EIO has been issued at the later stage of the proceedings, the authority competent to receive and execute it is the District Court.

126. In Italy the authority competent to receive the EIO and to proceed with its recognition and execution is the PP at the court in the capital of the district where the requested measures shall be carried out[49]. However, in the case that the requested measures are to be carried out in several places, the PP where the largest number of measures are to be executed; if the number of measures is equal, the competence will be of the PP's Office of the district where the more important investigative measure is be executed[50].

127. A tipping point in this context is represented by the cases where the issuing authority requests that a judge executes the EIO or cases where, according to the Italian law, the measure requested shall be executed by the judge (e.g. interception of communications, or any other measure which affects the fundamental rights guaranteed under the Constitution). In such cases, the PP will still be competent to receive and recognize the EIO, while the execution will lie with the Judge for the preliminary investigation (*giudice per le indagine preliminare*).[51] The judge, once the EIO has been transferred to him/her, can

[47] Art. 589w § 1 PCPC
[48] Art. 589w § 2 PCPC in relation with Art. 307, 311§2 y 312 PCPC.
[49] Art. 4(1) LD n. 108/2017, op. cit.
[50] Art. 4(5) LD n. 108/2017, op. cit.
[51] Art. 5(1) LD n. 108/2017, op. cit.

revise *ex officio* or upon request of the parties, the decision adopted by the PP recognising the EIO[52].

128. However this option poses problems in practice not only because at present, the authority in charge of the pre-trial criminal investigations is, as a rule, the Investigating Judge (*juez de instrucción*)[53].

129. Spanish law has designated the PP as receiving authority for any EIO. The PP is also the authority charged with holding the record of every received EIO, acknowledge its receipt and recognise the EIO. It will also directly proceed to its execution when: (1) the EIO does not refer to measures restricting fundamental rights or, even if it includes it, this measure can be substituted, according to the assessment of the PP, by another measure which does not restrict fundamental rights; and (2) when the issuing authority has not explicitly stated that the measure shall be executed by a judicial authority.

130. In all other cases, once the EIO has been received and registered, the judge will be competent to recognise and execute the EIO (measures restrictive of fundamental rights which the PP considers cannot be substituted by a non-coercive measure; or the issuing authority has explicitly stated that the measure shall be executed by a judge). The PP will hand over the EIO to the judge with material and territorial jurisdiction[54], together with an assessment on the possible grounds for refusal of the EIO, and the position of the PP regarding the lawfulness of the measures requested in the EIO according to the domestic law.

**18) Proposed best practice**: It is appropriate that the receiving authority is the one who has to execute the EIO. It is adequate that the receiving authority is in all three countries the PP, as they will also have competence to execute many of the EIOs. If the execution of the EIO requires to leave the execution in the hands of a judge –because this is required by domestic law of the executing state or

[52] Art. 13 (5) LD n. 108/2017, op. cit.

[53] Cfr. Report of the General Council of the Judiciary to the draft law modifying Law 23/2014, 20 November, "On Mutual Recognition of Criminal Sentencing in the European Union".

[54] The criteria for setting the subject-matter and territorial jurisdiction are included in Art. 187(3) LRM.

because the issuing authority specifically requests so–, the PP shall transfer the EIO to the competent court.

**19) Proposed best practice:** Keeping the reception of the EIOs in the hands of one single institution (the PP), can also facilitate the registering, the elaboration of statistics and the dissemination of best practices, for the action of the PPs is better coordinated, due to their hierarchical structure. It will also ensure uniformity in the handling and transfer of the EIOs. Moreover, in those cases where the PP is directly competent also for the execution, this solution is to be viewed as the most efficient.

**20) Proposed best practice:** identifying the PP office of the relevant territory where the measure/s are to be executed as the receiving authority is a good option for handling incoming EIOs.

131. Poland has opted for a diverse mechanism, depending at what the stage of the proceedings the EIO has been issued. Such division may be necessary to comply with the domestic rules on jurisdiction, nevertheless it does not seem to be justified in abstract nor to simplify the quick identification of the receiving authority.

### 8.2. Recognition when receiving authority is not competent for the execution

132. When the receiving authority is not competent for the execution of the measure, the question is: 1) should the receiving authority also decide on the recognition, before transferring the EIO to the judge competent for the execution?

**21) Proposed best practice:** Once the EIO has been received by the PP (not in Poland), and the PP considers that the EIO is to be carried out by a judge, the way to proceed for optimising the efficiency, is that the same PP decides on the recognition before transferring the EIO to the judge, although the judge can later revise such decision. This is the solution adopted by Italy.

In Spain, however, in such cases, the receiving authority will not recognise the EIO, but transfer it directly to the judicial authority, albeit with a not-binding report on the

grounds for recognition/not recognition. The judge will, before executing the EIO render a decision on the recognition.

133. Both systems are very similar, and either practice is acceptable, although the first one seems to be more efficient and promotes more the uniformity of the interpretation of the grounds for refusal. Important at this point is to underline that when receiving and executing authority are not the same, the recognition done by the first (the PP) should be subject to be revised by the second (the judge).

### 8.3. Request of several investigative measures under the same EIO

134. Should the execution of the EIO be divided so that those measures that can be directly carried out by the PP remain in its competence, so that the judge should only execute part of the EIO, the one precisely which requires his/her intervention?

135. Regarding this issue, when an EIO requests several measures, and some can be executed by the PP and others require the intervention of the judge. Should the receiving authority be allowed to fragment the EIO so that the requests that can be executed by the PP are not transferred to the judge? Or rather, should all the measures requested in the EIO be handed over to the judge? This second option is the one chosen by the Spanish law. Italian practice is unclear in this respect, because the LD n. 108/2017 does not contain a specific provision on this. In the light of EIO provisions as well as of the principles of the Italian criminal procedure, it can be concluded that the PP will transfer to the judge only measures that need to be executed by him. But this will need to be checked further in practice, as for now the information is not complete. Poland does not face this dilemma, because the competence of the receiving/executing authority is determined by the procedural stage and not by the type of measure.

136. Which would be the best way to proceed? To fragment or to not fragment the EIO? Both options present advantages and disadvantages. The fragmentation may allow the judges not be overloaded with requests which can be executed directly by the PP, so promote a more balanced division of work. However, this solution, may not be optimal for the communications with the

issuing authority, that would be forced to follow the execution of the measures before different authorities. A third practice could be: the same receiving authority (the PP) keeps the coordination of the execution of those "mixed-EIOs". This would allow the issuing authority to communicate only with one interlocutor, and at the same time, relieve judges from executing non-coercive measures.

**22) Proposed best practice:** The best solution will depend on the contextual elements: depending which authorities are best prepared, more experienced and less overloaded. As for the moment, Spanish law has opted for concentrating the execution of "mixed EIOs" in the hands of the judges. It will need time to see how efficient this is dealt with in practice.

### 8.4. The EIO received requires execution of several measures in different districts

137. This situation adds more difficulty as the EIO can fall not only within the competence of different type of authorities (PP and judges), but also authorities located in different territories. The fragmentation of the execution of the measures seems unavoidable in most cases, because the territorial limits of jurisdiction of the national authorities will not be altered just within the EIO enforcement proceedings. But the competence for dealing with the EIO can be still kept under one single authority.

**23) Proposed best practice:** while the competence for executing each of the measures requested in an EIO will need to be divided, the competence (and coordination) for the recognition, coordination of execution of measures and transfer of evidence, can still be kept under one single judge/authority.

138. This is the best practice to be adopted, in order not to scatter all measures requested in one EIO. The issue now, is which authority shall retain the competence. The Italian solution is to establish the territorial competence in the PP where the majority of the measures requested are to be executed, and if this criterion does not apply, then where the most important investigative measures are to be carried out.

139. This seems to be an adequate practice. In Spain the same rule could be applicable, to identify the territorial competence of the PP or the one of the judge, in case of several measures.

**24) Proposed best practice:** Questions and conflicts of competence among the executing authorities that would delay the whole procedure of the execution of the EIO should be avoided. To that end, certain flexibility should be applied so that the issues of territorial and material competence are solved in a swift manner: in gathering of evidence the principle of the legally pre-established judge is not to be interpreted in a strict way; therefore, issues of competence and jurisdiction should be addressed with flexibility, taking always into account the principle of efficiency in providing the requested judicial cooperation.

140. In cases of complex EIOs, where different authorities and districts are involved, it could also be considered if a coordination authority might not be appointed. In Spain such coordination could lie with the PP, as they are based on the province, which covers different judicial circuits. In Italy a role of coordination, at the stage of investigation, is performed by the National Anti-Mafia and Counter-Terrorism Prosecutor. But his function is limited to proceedings for crimes referred to in Art. 51 § 3-*bis* and 3-*quater* (mafia-type organisations, trafficking of drugs, sexual offences…), and for the application of mafia and terrorism prevention measure. Regarding "common" offences coordination could lie with the PP.

### *8.5.* Role of Central authority

141. Not all MSs bound by the EIO have opted for appointing a central authority as provided under Art. 7(3) DEIO, but Italy, Poland, and also Spain have done so. In Spain the Central Authority, according to the Law On mutual Recognition is the Ministry of Justice. However it is unclear what shall be its role with regard to the EIO, as the direct contact between issuing and receiving/executing authority is already provided within this mutual recognition instrument.

142. In Italy the Central Authority, according to Art. 2 lett. f) of LD no. 108/2017, is the Minister of Justice to whom the PP has to transmit a copy of

the EIO received (Art. 4 § 1). Is not specified in any provision which is the role of the Ministry of Justice. According to scholars his involvement could be useful where the execution of the EIO could prejudice national security that is a ground for refusal. In my opinion the communication is relevant in order to elaborate national statistics on the application of the new instrument.

**25) Proposed best practice**: It does not seem that the Central Authority is to be involved in any form in the procedure of issuing or executing an EIO. However, in case of non-compliance or a systematic infringement of the obligations set out in the EIO Directive, the Central Authority can play a crucial role in collecting complaints regarding the EIO implementation.

### 8.6. Issuing of the EIO

#### *a) Who may request the issuing of the EIO?*

143. Art. 1(3) DEIO provides that the issuing of the EIO may be requested by the suspect or accused person (or by a lawyer on his behalf) within the framework of applicable defence rights in conformity with national criminal procedure.

144. Poland and Spain extend the possibility of Art. 1(3) DEIO also to any person who is party to the proceedings: In Poland both the suspect and the victim may request the judicial authority to issue an EIO, although the judicial authority does not need to provide a formal response to this request (Art. 9.1 PCPC).

145. Spain provides that the EIO may be issued *ex officio* or at the request of a party (Art. 189 (1) LRM). The party entitled to request the EIO will depend on the proceedings where the issuing of an EIO is requested:

146. When the body conducting the investigations is the PP (those pre-judicial investigative measures that can be ordered and carried out by the PP without intervening the Investigating Judge[55]), the suspect (or the lawyer on his behalf) may request the PP to issue an EIO with a view to conducting

[55] Art. 773(2) LECrim and Art. 5 EOMF.

preliminary inquiries (not restrictive of fundamental rights) for gathering exculpatory evidence[56].

147. This request is not binding for the PP and its refusal does not need to be motivated and there is no appeal against it. No other parties are entitled to intervene in these preliminary investigative stage, thus only the defence could file the request to issue an EIO to the PP[57]. The same applies to juvenile proceedings –where the Public Prosecutor directs the pre-trial investigation[58] -, but in this case, both defence and victim can request an EIO to be issued. In this case, if the PP refuses to issue the EIO, the parties may file again the request before the Juvenile court[59].

148. In the pre-trial investigation led by the Investigating judge, in addition to the defendant, and the victim, all other parties intervening in the proceedings may request the issuing of an EIO (private and popular accuser). The judge must decide by way of an order (auto), explaining the reasons for its decision. This order is subject to appeal, as any other request for evidence filed by the parties[60].

149. In Italy the victim is not included among the persons entitled to request the issuing of an EIO. This does not mean that the victim may not ask for it, but that the PP can reject it without motivating the decision.

150. On the other hand, the EIO requested by the defence will only be admitted if it explains the reasons that justify such investigative measure (Art. 31 LD), which obliges to disclose the defence strategy. In the same vein, it is important to stress that, although the law provides that the decision to reject the request shall be motivated (and shall be adopted after hearing the parties if it comes from the judge), this decision may not be challenged by way of appeal.

---

[56] FGE, Circular 4/2013 of 30 December 2013 "sobre diligencias de investigación" ("Instructions of the Prosecutor's General Office on investigative measures"), op. cit., para. III.1.

[57] FGE, Circular 4/2013 of 30 December 2013 "sobre diligencias de investigación" ("Instructions of the Prosecutor's General Office on investigative measures"), op. cit., para. XI.

[58] Art. 16(1) LORPM.

[59] Art. 26(2) LORPM and FGE, Circular 1/2000 of 18 December regarding the application criteria of the Organic Law 5/2000 of 12 January, regulating the Minors' criminal liability, para. VI.3.C.

[60] See *infra* when addressing the national legal remedies.

151.

**26) Proposed best practice:** The decision rejecting the issuing of an EIO requested by the defence should be motivated. Victims and other parties should be entitled to request the issuing of an EIO, as long as this is not incompatible with the principles of the national criminal procedure.

**27) Proposed best practice:** It should also be possible, to hear the parties to the process/proceeding before taking a decision on the issuing of the EIO, if such hearing does not endanger the outcome of the proceedings.

**28) Proposed best practice:** In cases of several measures requested within the same EIO, the decision on the competence of the executing authority might be quicker if the whole procedure is coordinated by one single authority.

**29) Proposed best practice:** Direct contact between requesting and executing judicial authority is crucial. The communication channels should work equally regardless who is the receiving/executing authority. Where according to national laws, receiving authority in certain cases cannot execute the measure, coordination between both authorities is to be ensured.

### *b) Information that can be obtained by way of police cooperation*

152. In practice there are many EIOs issued requesting information on the domicile or residence of a certain person (suspect or witness). Such information can be obtained more easily and swifter via police cooperation, and that should be the preferred channel.

**30) Proposed best practice:** Before issuing an EIO, the issuing authority shall determine if the requested information can be provided by way of judicial cooperation or not.

### *c) The role of Eurojust with regard to the EIO*

153. The structure and forms of the EIO are mainly designed for cooperation in evidence gathering which involves two states (issuing and executing MS), and

single investigation measures. However, transnational cross-border criminality often entails great complexity, involves several MS (and non EU states), and only exceptionally one single investigative measure is needed. Especially when it comes to transnational organised crime (TOC), the EIO may not be completely suitable for tackling efficiently the cross-border criminal investigation. This is why, an early involvement of Eurojust is highly recommended, not only in giving support in the issuing and transfer of the EIOs, but also in taking the decision whether a JIT should not be a better option than the issuing of several EIOs.

154. Apart from those cases where there is a highly complex criminal investigation going on, in general, due to their particular structure and swift communication among the diverse MS's national desks, the role of Eurojust in helping in any cross-border criminal investigation, shall be highlighted. It is to be regretted that the role of Eurojust is not adequately reflected in all the domestic laws transposing the DEIO, and this is the reason why the role if Eurojust is especially underlined in this CBP in the cross-border criminal investigations.

**31) Proposed best practice:** Early involvement of Eurojust should be promoted, in particular with regard to EIOs that entail complexity of the investigation entails several measures and/or countries. Taking advantage of the support that Eurojust can give in the issuing of the EIO as well as in facilitating the execution, is to be promoted.

### *d) Is the form of the EIO enough to be sent to the executing authority or must the issuing authority attach to the form also the judicial resolution?*

155. The EIO is set out in a form (Annex A)[61]. As with other instruments based on the principle of mutual recognition this form, as a rule, does not need to be accompanied by a certified copy of the decision taken in the national proceedings with regard to the measures requested in the EIO[62]. The form shall be signed by the issuing authority (or validating authority) and shall be filled in

[61] For the interception of communications for which no technical assistance from the executing State is needed (Art. 31 DEIO), the form to be employed is Annex C.

[62] Art. 7 (I) LRM. Art. 30 LD no. 108/207, concerning the content of EIO where Italy is the issuing authority.

an official language of the executing State or in any other official language accepted by it[63].

**32) Proposed best practice:** As a general rule, the form is enough and there is no need to attach the judicial decision. However, as an exception, if the executing State needs more information which are not possible to obtain from the form, it may request the issuing authority to send the judicial decision. It is however recommended that the issuing authority include in the EIO certain additional data with a view to seek the admissibility of evidence and/or facilitate the role of the executing authority. Thus, it is desirable that in Section I, besides recording the formalities and procedures required for the execution of the EIO, there are set out the measures or actions which can not be carried out in a "in a similar domestic case".

***e) What other information shall be included in the form of the EIO?***

156. The form shall explain all the elements that justify the necessity and proportionality of the measure requested, in order to enable the executing authority to analyse if such a measure would be allowed in a similar domestic case in the executing state. Further, the issuing authority should also justify the elements that allow to determine that the measure shall serve to establish the facts investigated or to obtain the evidence sought.

**33) Proposed best practice:** If such information is missing, before refusing, the receiving/executing authority shall communicate with the issuing authority asking to complement the data required. In certain cases where a coercive measure that entails a serious encroachment of the fundamental rights is requested via EIO, the executing authority may ask the judicial decision upon which the EIO is based to be sent.

[63] The information on the languages accepted in the different States is available on the website of the EJN *Status of implementation of the Directive on the European Investigation Order*.

### *f) What other information should be included in the EIO?*

**34) Proposed best practice:** To contribute to ensuring the admissibility of evidence, the issuing authorities shall include in the EIO those requirements that will facilitate the admissibility of the evidence and which should be followed by the executing authority. The issuing authority shall specify which requested measures are to be adopted by a judge and also whether the issuing authority could carry out the requested investigative measure in a similar domestic case.

**35) Proposed best practice:** Establishing precise conditions on privileges and immunities when the EIO requests the interrogation of a witness is also crucial to ensure that the admissibility of such statements are not challenged later. In cases where the witness is to be protected or is already within a witness protection programme, the issuing authority shall inform exactly the executing authority what safeguards and confidentiality protections are to be adopted to shield the identity of the protected witness.

**36) Proposed best practice:** Within Section J (Legal remedies), it should be specified not only whether an appeal against the issuing of the EIO has been lodged, but also whether such an appeal is admissible according to the *lex fori*.

**37) Proposed best practice:** In order to avoid unnecessary translation costs, it is recommended to fill out the form of Annex A in *Word*, eliminating from the document the Sections and/or paragraphs not applicable to the specific EIO which is issued. In any event, the Italian and Spanish issuing authorities must not to fill Section L of Annex A DEIO.[64]

### *g) How to identify the authority to whom the EIO shall be sent?*

157. Once it has been checked that the relevant State has implemented the EIO[65], it is possible to identify the authority competent to receive the EIO

[64] Section L of the Annex XIII LRM, as regards Spain; and the Section L of the Annex A LD, as regards Italy.

[65] Information available on the website of the EJN *Status of implementation of the Directive on the European Investigation Order*.

through the EU ATLAS, which is also accessible from the website of the EJN. In any event, it is possible to request the help of the contact point of the EJN, Eurojust or the central authority, if this has been appointed.

158. Establishing a centralised receiving authority would facilitate the work of the requesting authority and its transmission. However this would run against the main principle that contact should be directly between issuing and executing authority in order to avoid delays and unnecessary intermediate steps. It is not recommended to establish a centralised receiving authority, although concentrating all the receiving in the PPs office, as a much structured and hierarchically organised institution might ensure a better coordination in the identification of the competent executing authority.

**38) Proposed best practice:** Before issuing the EIO authorities should check whether the EIO has to be sent/notified to other authorities of the executing State. In particular, in Italy the EIO shall be transmitted to the *Direzione Nazionale Antimafia e Antiterrorismo* when the investigations refer to some of the crimes mentioned in Art. 51 (3 and 3bis) ICPP[66]. Furthermore, copy of the issued EIO should be sent also to the *Ministero della Giustizia*[67].All MSs shall inform Eurojust (through its national member) of the transmission of an EIO, when the necessary conditions for the action of this body are met[68]. When such conditions exist, it is also possible to request the assistance of Eurojust in identifying the authorities competent to receive the EIO[69].

[66] Art. 27(2) DL

[67] See Eurojust, Italian Desk, "L'ordine di indagine europea. Cosa è utile sapere? Domande e risposte", p. 10, 12.

[68] In Spain this obligation is explicitly set out in Art. 9(3) LRM, as well as in Art. 24 of the Law 16/2015, of the 7 of July. In Italy, in Art. 7 of the Law 4/2005, núm. 41.

[69] Art. 3 of the consolidated version of the Council Decision on the strengthening of Eurojust and amending Council Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime.

***h) To which authority should the EIO be sent in cases where the investigative measure requested does not have a link to a certain territory within a MS? Which authority in the executing state should be competent?***

159. In those cases where the investigative measure requested does not have a specific link to a territory, as it occurs with the remote access to computers or other e-evidence, the MS shall identify clearly which is the receiving/executing authority. Spanish law has designated the National Court as the executing authority in such cases, while the German law has distributed the competence among the authorities of different Länder. Such an approach is to be followed, as it simplifies the identification of the competent authority from the very beginning and without having to resort to complex interpretations regarding which would be the authority with territorial competence to execute such measures.

160. The same criterion is to be applied in cases where the measure undertaken is an interception of telecommunications without technical assistance, in order to identify which is the authority in the "executing" state that shall be notified of such interception.

**39) Proposed best practice:** Each country shall identify clearly which is the authority to receive and execute those EIOs that relate to an investigative measure which is not linked to a precise territory. The same approach is to be done in order to identify the authorities that are to be notified following Art. 31 DEIO.

## 9. EXECUTION OF THE EIO

### 9.1. What are the actions to be taken when receiving an EIO?

161. General rule is to proceed to register such request, check its compliance with the legal requirements and proceed to execute it or transfer it to the authority competent for the execution if this is different from the receiving one. Important for the follow up reports on the implementation of the EIO is that there is an automated system for registering incoming and outcoming EIOs, the issuing authority, the type of measure requested, if the EIO was refused on what

grounds, the final outcome of the procedure for cooperation (which evidence was gathered, within which time it was sent, how was it transferred, and if the measure was challenged. In Spain, Italy and Poland, where the PP plays a relevant role as receiving and executing authority, these statistics should be elaborated by this authority, at least with regard to the incoming EIOs. As the issuing authorities may be different –in Spain it will be most often an Investigating Judge and not the PP who issues an EIO–, it is of utmost importance that a protocol for centralising such information is adopted, so that the statistical information is gathered following the same criteria and methodology.

**40) Proposed best practice:** It shall be ensured that all information regarding incoming and outgoing EIOs is centralised for statistical aims in one body.

### 9.2. Further effects of an EIO at the domestic level?

162. Once the EIO is received, registered and checked for recognition, the execution shall be carried out as soon as possible. A good practice that has been identified in Spain relates to the DNA information requests. This information has been centralised in the central cooperation unit of the PP, and has contributed to reduce significantly the time to provide such information to the requesting authorities. At present, in Spain it may take no longer than one day in providing such information, while before it took several weeks.

**41) Proposed best practice:** Certain information on DNA which is already kept in national data bases, can be provided by a central single unit. This practice is in conformity with the approach suggested below, regarding the identification of one single authority for executing EIOs that are not related to a certain territory. The practice in Spain allows to present this as best practice.

### 9.3. Can the information provided in an EIO be used as *notitia criminis* to trigger a national criminal investigation or other measures?

163. Further it has to be determined what shall the domestic receiving authority do with the information provided in the EIO. Some domestic provisions –this is the case of Spain– determine that upon receiving a *notitia*

*criminis*, a criminal procedure to investigate such allegedly criminal facts should be opened. Can the receiving authority trigger a criminal investigation upon the notice of the facts described in the EIO? The answer is no. An EIO shall not give rise to trigger a criminal investigation on the same facts in the executing state. However, it may raise questions regarding the jurisdiction, if the receiving authority considers that in application of the domestic rules on international jurisdiction, the receiving state should investigate and prosecute such offences.

164. As long as there are no specific rules on attribution of jurisdiction and the solving of conflicts of jurisdiction in criminal cases at the EU level, beyond the ones established in the FD 2009/498/JHA[70], the principles as expressed in such FD should be followed, in order to avoid infringements of *ne bis in idem* and parallel investigations.

**42) Proposed best practice:** The information obtained by way of EIO should not be used to trigger a national separate criminal investigation. If such information raises doubts on the jurisdiction, it has to be called upon the involvement of Eurojust.

### 9.4. How shall the executing authority proceed in cases when during the execution of an EIO, new information about another crime is found?

165. This is a complex question, and the practitioners interviewed have not given information in this. The answer is not easy and it will depend whether the evidence/information discovered is related to an offence that is connected to the one which triggered the investigative measure via EIO or not. If the newly discovered offence presents some kind of connection with the offence that has triggered the EIO, the issuing authority is to be consulted, in order to determine whether according to the rules of the requesting state, the connected offence falls within their jurisdiction.

[70] Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings. See, for example, P. Caeiro, "Jurisdiction in criminal matters in the EU: negative and positive conflicts, and beyond", *Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft (KritV),* vol. 93, No. 4, 2010, pp. 366-379.

**43) Proposed best practice:** If during the execution of the requested investigative measure evidence of a new offence is discovered which does not present any connection with the initial one, the executing authorities shall proceed with such evidence according to their national rules on accidental findings. Consultations with the requesting authority shall always take place to decide how to proceed with the newly accidentally discovered evidence, unless it is manifest that such evidence is completely unrelated to the case that triggered the EIO.

### 9.5. Shall the EIO issued or validated by the PP be refused when it includes measures restricting fundamental rights whose adoption in the executing State is reserved to the judge/judicial authority?

**44) Proposed best practice:** An EIO should not be refused on this ground. It would be contrary to the principle of mutual recognition, as well as to the principle of mutual trust which "requires, particularly with regard to the area of freedom, security and justice, each of those States, save in exceptional circumstances, to consider all the other MSs to be complying with EU law and particularly with the fundamental rights recognised by EU law".[71]

**45) Proposed best practice:** In addition, the executing authority has no legitimacy to question the competence of the issuing or validating authority, as long as such authorities according to their own domestic legal system, qualify as "judicial authority" in accordance with the criteria set forth by the DEIO [Art. 2 (c) i)] and by the CJEU itself[72]. Furthermore, it should be noted that neither Art. 9.3 and 11 DEIO, nor the corresponding implementing law envisage expressly this circumstance as a ground for refusal of the EIO.

[71] CJEU, C-404/15 and C-659/15 PPU, *Aranyosi and Căldăraru*, 5 April 2016, para. 78, and case law cited there.

[72] The case law of the CJEU on the concept "judicial authority", although adopted in the context of the EAW, may be applied to the EIO: "the words 'judicial authority' (…) are not limited to designating only the judges or courts of a Member State, but may extend, more broadly, to the authorities required to participate in administering justice in the legal system concerned". CJEU, C-477/PPU, *Kovalkovas*, 10 November 2016, para. 34; C-452/16 PPU, *Poltorak*, paras. 33, 38.

## 9.6. How to proceed if the EIO has not been issued by a judge or a PP, but by an authority which according to the domestic legal framework is labelled as a judicial authority.

166. If the domestic law of the issuing state defines an authority as "judicial" to the effects of the criminal investigation, even if it is not a judge or a PP. This has been the case in some EIOs issued by custom authorities in Germany, which according to the German law qualify –within the scope of their activities– as judicial authority. The requested authorities in the executing state (Netherlands), however, refused to execute the EIO, on the grounds that such an authority, to their view, did not fit into the definition of Art. 2 (c) 1 DEIO. Unless it was validated by a judge or a PP, it would not be accepted for execution in the Netherlands.

167. This case leads us to the following question. Shall the requested authority before granting the execution check if the authority identified in the EIO form as "judicial authority" can be considered in fact a judge or PP to the end of Art. 2 (c) (i) DEIO? In other words, if the issuing authority states that it is a "judicial authority", how shall the requested authority act? Check if it really is such an authority or according to the mutual recognition principle, take for valid the statement made in the form?

**46) Proposed best practice:** In general, the executing authority should NOT check whether the issuing authority has judicial nature under its national law. Only exceptionally when the executing authority has really grounds to believe/fear that the issuing authority might not be a judicial authority in the meaning of Art. 2 (c) (i) DEIO, may the executing State check it on the condition that coercive measures are concerned, and under its national law, according to fundamental constitutional principles, this authority can not be considered a judicial one. In this case, it can ask the issuing State to have the EIO validated by a judicial authority and if the latter does not validate it, it may refuse it or refer a preliminary question to the CJEU.

### 9.7. Can the defence lawyer and other parties to the proceedings take part in the execution of the EIO?

168. Art. 9(4) DEIO acknowledges that the issuing authority has the option of requesting that one or more authorities of the issuing State assist in the execution of the measure, participating in the taking of evidence together with the competent authorities of the executing State. According to this provision, the executing authority is obliged to accept such assistance, unless it considers it contrary to the fundamental principles of law of the executing State or it is perceived as harming its essential national security interests.

169. Obviously, having recourse to this option will be very positive in order to ensure the admission of the evidence in the issuing State. In practice however there are budgetary constraints that hinder the issuing authority to travel to the executing state to be present during the gathering of the evidence by way of the EIO.

170. It would have been positive to extend the participation in the execution of the EIO to the defence attorneys and the parties to the proceedings[73]: in the first place, because **(in)** this way the lawyers may first-hand ascertain whether the measure is being carried out lawfully and in accordance with the procedural safeguards; in the second place, because their presence during the execution of the measure would allow them to file complaints "*in situ*" and also to object to a supplementary EIO; and, lastly, according to the national law of the issuing State, respecting the adversarial principle at that investigatory stage may also have a decisive impact on the admissibility of the evidence obtained abroad[74].

171. However, neither the DEIO nor the national implementing laws mention the possible intervention of the defence lawyers in the execution of the EIO, but

[73] This was foreseen under Art. 4 of the European Convention on Mutual Assistance in Criminal Matters of 1959. In the same sense, see the Recommendation No. R (80) 8 of the Committee of Ministers to Member States concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters, of 27 June 1980.

[74] This is the case in Spain, for instance, with regard to the investigative measures which are impossible or very difficult to be practiced later at trial. Cfr. Art. 730, 777(2) y 797(2) LECrim.

only for the «authority» or the «officer». [75] Nevertheless, although not specifically foreseen, it should not be interpreted as a prohibition of the defence lawyers to intervene. Moreover the protection of the right of defence and the principle of equality of arms[76] would support such participation, as long as the investigations are not to be kept secret[77].

**47) Proposed best practice:** The participation of the lawyers in the execution of an EIO should be facilitated in order to protect the defence rights. Thus, as long as it is compatible with the investigations and those are not secret, intervention of the lawyers in the execution of the measures carried out in another MS should be promoted. To that end, the issuing authority should require that the defence lawyers are informed of the date scheduled for its practice.

## 10. REQUIREMENTS OF PROPORTIONALITY/NECESSITY OF THE EIO

172. The DEIO does not establish a minimum threshold for issuing an EIO, therefore any evidence that is required within the proceedings of Art. 4 DEIO, regardless the gravity could be requested via en EIO. This is coherent with the aim of establishing a single AFSJ, so that any evidence that could be requested within one country could also be requested via an EIO. Although this approach is to be supported and is also the way in which the DEIO is to be understood, in practice, however, this may lead to certain tensions, because it may lead to the overburdening of the executing authorities and can also cause costs that some countries may view as excessive or disproportionate.

173. As it was already experienced with regard to the EAW, although the impact of the proportionality principle has a different meaning in the realm of the gathering of evidence, a cost-benefit analysis should also be undertaken

[75] Art. 191 and 210 LRM; Art. 29 (1 y 2) LD; and Art. 589zi (§ 1 y 2) PCPC.

[76] It should be noted that, as consistently stated by the ECtHR, this principle is integrated in the right to a fair trial enshrined by Art. 6 CEDH. See, for all, judgment *Dombo Beheer v. The Netherlands*, App no 14448/88, 27 October 1993.

[77] This is requested also by the group of lawyers interviewed in the framework of this project.

before issuing an EIO. The practice in Spain has shown that there is a huge number of EIOs issued within administrative offences' proceedings in Germany, where the sanction imposed is less than 10 euros. The executing PPs in Spain feel overburdened by such requests and feel that some kind of cost-benefit analysis should be undertaken by the issuing authority. Similar problems can arise when costly investigative measures are requested for the prosecution of petty offences, specially stemming from MSs whose criminal justice system follows a strict application of the principle of legality. This issue shall be addressed at the domestic level, by imposing some kind of cost-benefit analysis in the prosecution of certain petty cross-border crimes, or considering the possibility of sharing costs if some of the executing MS become overloaded.

174. If the number of EIOs regarding evidence related to insignificant infringements or sanctions continues increasing, it is to be foreseen that some kind of proportionality threshold will be claimed or applied. If several MS cause a disproportionate increase of work and costs upon the authorities of other states, some re-balancing mechanism should be applied.

**48) Proposed best practice:** It is recommended that the issuing or validating authority undertakes some kind of proportionality test, before issuing an EIO, which is not only focused on the need for the evidence to prosecute the crime, but also with regard to the costs that it may entail faced with the gravity of the offence.

**10.1. How shall the issuing authority describe the facts of the investigated offence, the elements that trigger its investigation and the need for the requested investigative measure?**

175. The facts are to be described as precisely as possible, so that it is clear for the executing authority which is the offence under investigation and what is the relationship between the investigative measure requested and the facts that are to be proofed. However, being said this, the level of detail and precision of the factual basis of the criminal offence and the explanations on the necessity of

the investigative measure and the elements that point at a certain person/s as suspect/s, is not easy to determined. The practice is diverse, even within he same country: for some authorities it is enough to identify the main facts of the offence, other authorities require a precise description of the background information that has served to grant a certain investigative measure. Being this practice very diverse, it is impossible to identify here a proper guideline valid in every case.

**49) Proposed best practice:** One criterion is to be followed: the description of the facts have to be so precise as to allow the executing authority to identify the precise offence that is being investigated, and be able to exclude that the EIO is used for carrying out fishing expeditions.

### 10.2. How to proceed in cases where the collecting of evidence is requested via EIO, but the form of the EIO is a) not complete b) is incorrect; or c) it is not used?

176. The forms included in the Annex of the EIO are aimed at facilitating the whole procedure of issuing and executing the requests for cooperation. At the same time, in order to make the whole procedure easier and swifter the use of those forms is mandatory.

177. In case a): the issuing authority fills in the form, but this is not complete or is incorrect. The way to proceed is established under Art. 16.2 (a) DEIO: only if it is impossible to the executing authority to take a decision, the executing authority shall "immediately" inform the issuing authority.

178. Sensu contrario, this means that, even if the form is not complete or mistaken, if it is clear for the executing authority what is requested and how to proceed to gather the evidence identified in the EIO, it shall proceed without the need for prior information.

179. Defects in the forms, incomplete forms do not lead to a refusal, nor to a suspension of the execution, unless the lack of such information makes it impossible to proceed. In such, cases, the executing authority shall contact the issuing authority and clarify the content of the EIO (correct mistakes, fill in gaps).

**50) Proposed best practice:** Forms are aimed at facilitating, not at hindering the cooperation. In this sense, formalities are never to be invoked as a ground for refusal, as long as the issuing authority is one of the authorities listed in conformity with the DEIO.

180. In case b) the executing authority has received the request for collecting evidence by way of a letter rogatory instead of using the forms of the EIO. This situation can occur during the first months after entering into force the EIO legislation in the MSs, but should disappear once the "transition" phase is over and every practitioner masters the EIO procedure. At present (as of September 2018), several countries have reported that they continued receiving requests in the form of letters rogatory instead of the form of the EIO.

181. The appropriate way to proceed in such cases –where all the conditions and requirements for an EIO are met, but the form is not used– would be: initiate the execution of such measures under the EIO rules, and at the same time contact the issuing authority, pointing out to the mistake in not using the prescribed form and: 1) state that they will proceed to execute despite the error, but this practice should not continue in the next future; 2) state that they will proceed to execute despite the error, but ask the issuing authority to re-send the request in the correct form.

### 10.3. How shall the executing authority proceed in case the issuing authority requests a measure that is not covered by the EIO, but using the forms of the EIO?

182. The practice of the MS authorities varies greatly. Some practitioners deal with such requests not falling within the scope of the EIO, directly as if they were MLA requests (e.g. Czech Republic), others however refuse the EIO for falling out of its scope. It has to be recalled that the issuing authority shall use the appropriate channels to gather cross-border evidence. Nevertheless, flexibility –at least at the initial months– should be the rule.

**51) Proposed best practice:** If the request for an EIO is sent as a letter rogatory, or the other way round, an MLA request is transferred via an EIO form, in both cases, the executing authority shall promote the execution: proceed to execute under the applicable rules, and at the same time inform the issuing authority on the mistake detected.

### 10.4. Immunities/privileges

183. So far the practice observed in the three countries studied has not presented specific problems related to immunities and privileges in the execution of the EIO. Nevertheless, as the role played by the lawyers in prevention of money laundering is increasing, it has to be thought of establishing a common approach at the EU level on the lawyer-client privilege, so that EIOs requesting the lawyer to be interrogated as witness are treated in a uniform way. The same applies to auditors and auditing companies.

184. The issue of the protection of certain privileges and immunities is to be specifically addressed in the realm of the interception of communications and search of computers, as during the execution of such measures it is frequent that confidential information or communications is accessed. An agreement on how such privileges/immunities are to be protected in cross-border criminal proceedings is needed.

**52) Proposed best practice:** This is more than a proposal for practitioners, but rather a proposal for taking legislative action at the EU level on common rules on professional immunities/privileges.

### 10.5. Shall the EIO be executed directly upon the certificate or shall the executing authority request for the domestic order of the requesting authority?

185. As a rule the domestic order granting the investigative measure does not need to be attached to the EIO and the execution of an EIO cannot be made dependent on it: attaching the domestic order that underpins the EIO certificate is not a legal requirement for its recognition and execution, and therefore its

absence cannot be treated as a formal shortcoming. The practice shows however a diverse practice, some executing authorities wanting to see the domestic order that supports the EIO, others being satisfied with the complete certificate and forms of the EIO.

186. Despite these preferences of single judicial authorities, it has to be underlined that the certificate stands for itself, and is to be directly executed. Only if some information is missing or there is the need to check the underpinning judicial decision in order to check if it would be allowed in a "similar domestic" case, the executing authority could consult with the issuing authority and ask for clarifications and eventually for the domestic order granting the investigative measure. But this conduct should be accepted only in exceptional cases, as the rule that the certificate is to be executed directly.

187. From the point of view of the defence rights, when the defence plans to file a remedy against the execution of the EIO in the executing state, having access to the supporting judicial order might be convenient. But, as in the executing country the reasons for issuing the EIO –necessity and proportionality of the investigative measure–, cannot be challenged, accompanying the judicial order should not be required.

**53) Proposed best practice:** The rule is that the certificate "is" the judicial decision. Executing authority shall only exceptionally request the issuing authority for the judicial order granting the requested investigative measure. This should occur only very exceptionally, when the content of the EIO is unclear or open doubts on the legality of the execution of such measure in the executing state.

### 10.6. How to deal with the costs of the EIO?

188. Art. 21 DEIO establishes the rule that the executing authority shall bear the costs "related to the execution of the EIO", unless they are exceptionally high, in which case it may consult with the issuing authority "on how the costs could be shared or the EIO modified" (21.2 DEIO).

189. Problems related to costs are not very frequent, as the practice shows in the three analysed countries. Those investigations that are highly complex, and

therefore could entail exceptionally high costs, are often coordinate by Eurojust, and thus the problem does not appear in the execution of the EIO. Costs is a problematic not so much in the execution of a single EIO, but due to accumulation of high number of EIOs stemming out from petty offences –administrative or criminal–, which consume at the end a lot of resources. But this issue has been addressed already above.

190. An example of a case where the executing authority considered that the execution of the EIO caused "exceptionally high costs", appeared with regard to a search of computer, where a specific IT expert was needed. Executing authority (Luxembourg) estimated that the costs were too high, and consulted with the issuing authority in order to find an agreement on the sharing of the costs. In this example, the issuing authority renounced to the IT-expert evidence, following Art. 21.3 (a) DEIO.

191. This example shows how the executing authority has to proceed: consult with the issuing authority on the sharing of the costs. However, it is still difficult to establish what shall be considered as "exceptionally high costs", as this assessment will depend on many factors, among others, the budget the executing authorities have allocated for the international judicial cooperation, as well as the number of requests received, apart from the costs of the forensic evidence or others in a single case.

192. Not having any guidelines as to the definition of "exceptionally high costs" in the context of the execution of an EIO, the best practice is to stick to the general rule –executing authority shall bear the costs–, and only in really exceptional situations discuss with the requesting authority on the need to continue with the execution and the possibility of sharing costs.

**54) Proposed best practice:** When the costs appear to be exceptionally high the executing authority shall consult on the: 1) relevance of the evidence to the proceedings; 2) on the relevance to the criminal policy; and 3) on the relevance to the overall costs. The general social interest has to taken into account when the problem of exceptionally high costs of an investigative measure arises.

## 11. GROUNDS FOR REFUSAL

193. It is essential to have a close look on the rules regarding the conditions for issuing, refusing and executing an EIO as well as the rules on remedies to be able to assess if this instrument will facilitate the judicial cooperation in the gathering of evidence.[78] Moreover focusing on these rules will allow to verify if the EIO is consistent with the principles applicable in the state of execution, while providing at the same time enough protection of the fundamental rights of the defendant and the other parties affected during the criminal investigation.

### 11.1. Regulation of the grounds for refusal as Mandatory or as optional?

194. From the point of view of efficiency the transposition of the DEIO done by most MSs has clearly favoured the judicial cooperation in the gathering of cross-border evidence in criminal proceedings within the EU. Nevertheless, it still faces many obstacles, in particular due to the fact that while the DEIO provides for optional grounds for non-recognition or non-execution (Art. 11 DEIO), when transposed into domestic law most of the MSs have transformed those grounds for refusal into mandatory: the term "may be refused" has been transposed as " shall be denied". This has been the case in Spain, Italy and Poland, while Germany, for example, has established the Art. 11 DEIO ground for refusal as optional.

195. This transformation of optional grounds for refusal into mandatory grounds for refusal has been seen also within the implementation of the EAW, and has been widely criticised for it, as it does not promote the efficient cooperation within the EU AFSJ. While it is true that regulating all grounds for

[78] Generally on the grounds of refusal see L. Bachmaier Winter, "The role of the proportionality principle in cross-border investigations involving fundamental rights", *in* S. Ruggeri (ed), *Transnational inquiries and the protection of fundamental rights in criminal proceedings. A study in memory of Vittorio Grevi and Giovanni Tranchina*, Heidelberg, 2013, p. 100 ff; F. Jiménez-Villarejo Fernández, "Orden europea de investigación: ¿Adiós a las comisiones rogatorias?", *in* C. Arangüena (ed), *Cooperación judicial civil y penal en el nuevo escenario de Lisboa*, Granada, 2011, p. 194 ff.; M. Aguilera Morales, "El exhorto europeo de investigación: a la búsqueda de la eficacia y la protección de los derechos fundamentales en las investigaciones penales transfronterizas", *BIMJ*, 2012, 2145, p. 11 ff.

refusal to recognise or execute an EIO as mandatory, will contribute to a more uniform application of them by the executing judicial authorities in a given state, it runs counter the aims of the mutual recognition principle.

**55) Proposed best practice:** Domestic rules should regulate all grounds for refusal provided under the DEIO as optional grounds for refusal, allowing the domestic judicial authorities to assess if they exist or not in each single case.

### 11.2. The investigative measure would not be allowed in a similar domestic case

196. Art. 10(1) EIO –apart from regulating the cases where the requested measure could or should be substituted–, also includes a ground for refusal. In those cases where the requested measure is not available and its substitution is not possible or would not have the same results "the executing authority must notify the issuing authority that it has not been possible to provide the assistance requested," and thus refuse its execution.

197. This case of non-execution of the indicated measure would not pose any further problems save for the expression: "the investigative measure indicated in the EIO would not be available in a similar domestic case" (Art. 10(1)(b) EIO). How should this provision be interpreted? It can mean that the measure is expressly excluded for the offence indicated in the EIO, but it can also be interpreted in the sense that, even if there is no specific provision excluding the measure, according to the assessment of the principle of proportionality in the executing State the measure would not be in conformity with the constitutional principles of the executing state and thus should be refused. it seems that Art. 10(1)(b) allows the refusal of an EIO that does not fulfil the proportionality requirement according to the test applicable in the executing State.[79] However, the checking of the "similar case" should not lead the executing authority to undertake a revision on the grounds which led to the issuing of the EIO and the granting of the investigative measure.

[79] See L. Bachmaier Winter, "The role of the proportionality principle in cross-border investigations involving fundamental rights", *in* S. Ruggeri (ed), *Transnational inquiries and the protection of fundamental rights in criminal proceedings. A study in memory of Vittorio Grevi and Giovanni Tranchina*, op. cit., pp. 100-101.

**56) Proposed best practice:** Refusal grounds are to be interpreted in a restrictive way, so that the EIO execution is not checked under the whole domestic legal framework of the executing state.

### 11.3. Privileges/immunities

198. With regard to the existence of "an immunity or a privilege under the law of the executing State which makes it impossible to execute the EIO" (Art. 11.1 a DEIO), recital (20) of the Explanatory Memorandum of the DEIO recognizes that "there is no common definition of what constitutes an immunity or privilege in Union law; the precise definition of these terms is therefore left to national law." As examples, it cites "protections which apply to medical and legal professions" but explaining that these are not the only ones that could come into consideration and that this provision "should not be interpreted in a way to counter the obligation to abolish certain grounds for refusal as set out in the Protocol to the Convention on Mutual Assistance in Criminal Matters between the MSs of the European Union".

199. The mere existence of an immunity should not automatically hinder the execution of the request of evidence under the EIO.[80] Paragraph 3 of the same Art. 11 states that if the executing State has the power to waive the immunity "the executing authority shall request it to exercise that power forthwith." But, if the power to waive the immunity lies not within the executing State, it is the issuing authority the one competent to request the waiver.

200. It should be further analysed what are the practical implications of the existence of immunities in the international judicial cooperation and more precisely within the ambit of the European Union. Even if international law immunities and state immunities are not the most adduced reasons for refusing the judicial cooperation in cross-border gathering of evidence –in fact they are very exceptional– as such cases may be closely linked to the State sovereignty,

[80] On immunity of jurisdiction and execution of states, its scope, content and alternatives in Spain see the comprehensive analysis made by F. Gascón Inchausti, "Inmunidades procesales y tutela judicial frente a Estados extranjeros", Cizur Menor, 2008, pp. 97-106 and pp. 415 ff.; M. Kloth, "Immunities and the Right of Access to Court under Art. 6 of the European Convention on Human rights", Leiden, 2010, p. 88 ff.

they have to be properly regulated. We can think of a case where a judicial authority of a European MS issues an EIO to gather bank information of a representative of the Spanish State or the Head of State. But another type of immunity may play a relevant role in the execution of an EIO regarding the investigation of tax offences. The immunity, for example, enjoyed by auditors and tax counsels in the different MSs comes to mind[81].

**57) Proposed best practice:** The executing authority, following Art. 11(1)(a) EIO, before refusing the execution of the EIO on the basis of an immunity, it should seek to request the waiver of the immunity, which may be legally difficult, and also raise diplomatic concerns.

### 11.4. Protection of freedom of the press and freedom of expression: Art. 11(1)(a) EIO

201. After mentioning the existence of an immunity or privilege, the same recital Art. 11.1 a) makes reference to another ground of refusal, that does not seem to be linked to the previous one. The EIO might be refused when "*there are rules on determination and limitation of criminal liability relating to freedom of the press and freedom of expression in other media*." This ground of refusal, which was to be found already in the first draft of the DEIO, clearly seeks to protect the freedom of expression and the freedom of press, but its meaning is not clear: it may refer to the protection of the sources of information or it may deal with a specific double incrimination requirement that has to be checked when the EIO deals with an offence related to the freedom of press or freedom of expression. The Explanatory Memorandum of the DEIO does not shed light on how this ground for non-recognition and non-execution shall be interpreted and the practitioners interviewed have not informed about any experience in this regard.

[81] Although the "Ley 22/2015, de 20 de julio, de Auditoría de Cuentas" ("Law 22/2015, 20 July, Audit Of Accounts") provides in its Art. 31 for the obligation of secrecy of the auditors and auditing companies, no privilege to refuse to testify is regulated for these professionals in the Criminal Code of Procedure, whilst para. 53 (1).3 of the German *Strafprozessordnung* provides for their *Zeugnisverweigerungsrecht*.

**58) Proposed best practice:** the only best practice that could be proposed with regard to this ground of refusal, is the general guiding principle: before deciding on the non-execution of the EIO, the issuing authority shall be consulted (Art. 11(2) DEIO).

### 11.5. National security interests, protection of the source of the information and classified information (Art. 11(1)(b) DEIO)

202. The grounds of refusal set out under Art. 11(1)(b) DEIO are that the execution of the EIO "would harm essential national security interests, jeopardise the source of the information or involve the use of classified information relating to specific intelligence activities".

203. At this point the DEIO does not introduce any relevant innovation, but just adopts the causes already provided traditionally in the conventional rules.[82] Nevertheless the inclusion of these same non-execution grounds in an instrument based upon the principle of mutual recognition should make us rethink whether this implies any change to the treatment of these grounds of refusal. In strict application of the principle of mutual recognition, the mere allegation that the evidence requested affects national security interests or classified information, should not lead automatically to the non-execution of the EIO. The right of the State to keep certain information secrete and refrain from disclosing classified information should also be subject to control by the executing authority so that it would not lead to impunity of serious crimes.[83]

204. States are especially sensitive when it comes to protecting their national security interests and their intelligence activities. However, according to the

[82] This possible grounds for refusal are very similar to the one stated in the former Framework Decision 2008/978/JHA on the European Evidence Warrant (Art. 13(1)(g)), and are also to be found in Art. 2(b) of the EU Convention on MLA of 20 April 1959, applicable also to the EU Convention on MLA of 29 May 2000, although in the conventional rules the clause of *ordre public* and the exception of sovereignty are further mentioned.

[83] On the problems related to the use of state secrets and the access to classified information in judicial proceedings, albeit with regard to the US criminal justice system, see the interesting study of J.A.E. Vervaele, "Secreto de estado y "privilegios probatorios" en los procesos de terrorismo en los estados Unidos. ¿Control judicial de los arcana imperii?", *in* L. Bachmaier Winter (ed.), *Terrorismo, proceso penal y derechos fundamentales*, Madrid, 2012, pp. 229-261.

principle of mutual recognition, the executing authority should proceed in the same way as if it were handling a domestic case and such information were necessary for his/her own criminal investigation. The strict implementation of the principle of mutual recognition with regard to State secrecy and classified information is not a priority for the MSs or the European legislator. Nevertheless the interpretation here proposed would still be the most consistent with the principle of mutual recognition as established under Art. 1(2) and Art. 8(1) PD EIO where it says:

205. "The executing authority shall recognise an EIO (…) and ensure its execution in the same way and under the same modalities as if the investigative measure in question had been ordered by an authority of the executing State, unless that authority decides to invoke one of the grounds for non-recognition or non-execution or one of the grounds for postponement provided for in this Directive."

**59) Proposed best practice:** If the laws of the executing state would allow the executing judge to control the classified nature of the evidence requested or, if he/she would be authorised to require and obtain the declassification of classified documents, this should also the way to proceed when executing an EIO affecting such interests. And again, here applies also Art. 11(4) EIO: before deciding on the non-recognition or non-execution of the EIO, the executing judicial authority shall consult the issuing authority.

### *11.6.* The territoriality clause (Art. 11(1)(e) DEIO)

206. Art. 11(1)(e) DEIO regulates as a possible ground for refusal the so-called territoriality clause or exception of jurisdiction.[84] Four conditions have to be met to apply this ground of non-execution of the EIO: 1) the EIO relates to a criminal offence which is alleged to have been committed exclusively outside the territory of the issuing State; 2) the offence has been committed wholly or partially in the territory of the executing State; 3) the EIO requests a coercive

[84] The same clause was already included under Art. 13(1)(f) of the 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.

measure; and 4) the conduct the EIO refers to is not an offence in the executing State. This ground for refusal in principle seeks to prevent an abusive extraterritorial exercise of jurisdiction.[85] This is why it should be questioned if the possible problems deriving from the extraterritorial extension of the criminal jurisdiction and the solution of the conflicts of jurisdiction caused thereof is to be tackled by way of granting the possibility to refuse to cooperate in the evidence gathering requested through an EIO. Although it is admissible that each MS may refuse the cooperation in order to protect its own criminal jurisdiction –mainly linked to the territoriality principle–, from the viewpoint of the efficient prosecution of transnational crimes this ground for refusal is not to be seen as the adequate way.

**60) Proposed best practice:** This ground for refusal, if kept, should always have optional character. In those jurisdictions where the grounds for refusal have been regulated as mandatory, it shall be applied only in very exceptional occasions, and as a rule should not constitute an obstacle in the cooperation in the gathering of transnational evidence by way of an EIO.

### 11.7. The measures listed under Art. 10.2 DEIO

207. Measures listed under Art. 10. 2 DEIO –which are mostly non-coercive measures, but not only[86]–, are not subject to be substituted by a different

[85] F. Jiménez-Villarejo Fernández, "Orden europea de investigación: ¿Adiós a las comisiones rogatorias?", *in* C. Arangüena (ed), *Cooperación judicial civil y penal en el nuevo escenario de Lisboa*, op. cit., p. 189.

[86] Art. 10. 2 EIO: "Without prejudice to Article 11, paragraph (1) does not apply to the following investigative measures, which always have to be available under the law of the executing State:

(a) the obtaining of information or evidence which is already in the possession of the executing authority and the information or evidence could have been obtained, in accordance with the law of the executing State, in the framework of criminal proceedings or for the purposes of the EIO;

(b) the obtaining of information contained in databases held by police or judicial authorities and directly accessible by the executing authority in the framework of criminal proceedings;

(c) the hearing of a witness, expert, victim, suspected or accused person or third party in the territory of the executing State;

(d) any non-coercive investigative measure as defined under the law of the executing State;

(e) the identification of persons holding a subscription of a specified phone number or

investigative measure. As a rule, the measures listed under this recital are ordinary investigative measures foreseen in the criminal procedure of any of the EU MSs. This fact already would make it impossible to deny the execution of the EIO on the basis that such a measure does not. If such measures exist in all domestic legal systems of the MSs and are generally accessible for any criminal investigation, what is the purpose of this provision, just avoiding the substitution of the measure upon a proportionality test? Or the objective is to prohibit the refusal of the EIO on the grounds that although existing, the measure it would not be available for a similar domestic case?

208. The aim sought is that the execution of these measures are not subject to any kind of proportionality test, despite the diverse regulation under the laws of the issuing and executing State. These measures are to be made available to the requesting authority, provided that the EIO complies with all other formal requirements.

**61) Proposed best practice:** The measures listed under Art. 10.2 DEIO shall be granted execution without undergoing any proportionality test, provided that the other formal requirements are complied with.

### 11.8. Fundamental rights protection and Art. 11.1. (f) DEIO

209. Cooperation in criminal matters in the AFSJ is based on mutual trust, and this in turn requires a reliable system to ensure that the highest standards of human rights are respected and applied complying equivalent standards in all MSs[87]. In the DEIO a specific ground for refusal related to the protection of human rights has been included[88]. Having a clause based on the protection of

---

IP address."

[87] See M. Böse, "Human rights violations and mutual trust: recent case law on the European arrest warrant", in S. Ruggeri (ed.), *Human rights in European Criminal law. New Developments in European Legislation and case law after the Lisbon Treaty*, Heidelberg, 2015, pp. 135-145, pp. 137-139.

[88] Art. 11.1.f) DEIO. On this see L. Bachmaier Winter, "Transnational evidence: towards the transposition of the Directive 2014/41 regarding the European Investigation Order in criminal matters", *eucrim*, 2015/2, pp. 47-59, p. 54; I. Armada, "The European Investigation Order and the lack for European standards for gathering evidence. Is a fundamental rights-based refusal the solution?", *NJECL*, Vol 6, issue 1, 2005, pp. 8-31, pp. 22 ff.; C. Heard, D.

fundamental rights in the EIO is to be viewed as a very positive step. However, this ground for refusal needs to be interpreted in such a way that the effectiveness of the judicial cooperation as established in the EU law is not unduly hampered, while at the same time the level of protection of human rights is ensured in the process of gathering evidence in any MS.

210. In this regard, in the analysed countries, we have not found any established practice on the implementation of the ground for refusal provided under Art. 11.1 (f) DEIO. Nevertheless, despite this lack of practical application, it is worth making the effort to identify possible situations and try to set guidelines to be followed.

### 11.9. Request to interview a witness who according to the executing authority should be considered as a suspect

211. One of the problems that has been identified is the case when the issuing authority requests via EIO to interview a witness, but according to the executing authority and the evidence at hand, the person to be interviewed is to be considered as a suspect. How shall the executing authority proceed in such a case?

212. First it has to be clarified that the executing authority is not to undertake a control whether the witness to be interviewed is really a witness or not. Such check would run counter the principle of mutual recognition. Nevertheless, if it appears clear to the executing authority that the person identified as a witness is in fact to be considered as a suspect, the issue is whether they should disregard their own assessment and continue the interrogation as requested, or they should inform the relevant person of his/her rights as suspect.

213. If it is manifest for the executing authority that the witness is not such, and they do not inform him/her of his/her rights as suspect, "there are substantial grounds to believe that the execution of the investigative measure indicated in the EIO would be incompatible" with the fundamental rights and

---

Mansell, "The European Investigation Order: Changing the Face of Evidence-gathering in EU Cross-Border Cases", *NJECL*, Vol 2, Issue 4, 2011, pp.133-147, p. 142 ff.

procedural safeguards of the executing state, and thus would fall within the ground for refusal of Art. 11.1 (f) DEIO. Further, if the admissibility of evidence in the requesting state also requires compliance with the *lex loci* rules, there might be the risk that such statements are not admissible as evidence if not carried out following the principles of the interrogation of suspects.

214. In such cases, where it is evident that according to the rules of the executing state the person to be interviewed is to be treated as suspect, the executing authority shall explain the issuing authority the circumstances, and consult whether the interrogation shall continue as a suspect. The executing authority shall not change on its own the condition of the person to be interviewed and change the investigative measure requested; but it shall not infringe its own rules regarding the rights that are to be granted to suspects.

### 11.10. EIO requests to interview a witness who during the interrogation becomes a suspect

215. How shall the executing authority act when during the interrogation of a witness –not via videoconference– out of the questions provided, it appears that the person summoned as witness, should instead be held as suspect? This question is very much linked to the previous one, but the situation is slightly different and this is explains why it has been addressed separately.

216. Following the domestic law in Spain or Italy, in these cases the interrogation is to be stopped and the suspect is to be informed of his/her rights (right to be assisted by lawyer, right against self-incrimination, etc.). Once the interrogating authority faces this situation and decides to stop the interview, how shall it proceed? Inform the interviewed person of his new condition as suspect and his/her rights? Or before doing that, consult the requesting authority?

217. The right approach would be that the executing authority stops the interrogation and before changing the position of the interviewed person from witness to suspect, communicates with the issuing authority as whether they should finalize the interview at that moment, without informing the person of

the suspicions that his/her answers have raised; or continue the interrogation as a suspect.

**62) Proposed best practice:** The preferred way to carry out the witness interrogations is to request to do it via video-conference. This should be the preferred way in all cases.[89] When such a way for whatever reasons is not feasible, issuing and executing authority should keep connected while the interrogation is being carried out. This would allow deciding immediately how to proceed in the case where out of the answers the initial witness turns out to be a suspect. If such immediate communication is not possible, we are inclined to propose that the interview is suspended until the issuing authority can be consulted. In no case the interrogation should continue as a witness, when according to the executing authority the witness should be held as suspect.

### 11.11. What shall the executing authority do when the evidence requested would not be admissible as evidence in the executing state for having been obtained in violation of a fundamental right?

218. What should be the done in case the evidence was obtained legally but only fort he purpose of administrative proceedings and thus obtained against the right to self-incrimination? This issue does not deal with the admissibility of evidence in the issuing state, but rather on how the inadmissibility of such evidence in the executing state –for having been obtained against a fundamental right– would affect is transfer by way of an EIO.

219. It is known, that there is no harmonization on the exclusionary rules of evidence among the EU MSs and that this poses numerous problems in the circulation of evidence and therefore in the establishment of a single AFSJ in criminal matters.[90] As long as the evidentiary rules are not adequately harmonised among the different MSs, however, not only does such a transfer fail to contribute to ensuring the procedural safeguards of the defence, it also

[89] See also L. Bachmaier, *Transnational criminal proceedings, witness evidence and confrontation: lessons from the ECtHR's case law*, Utrecht Law Rev., special issue, 2013, September 2013, Volume 9, Issue 4 (September) 2013, pp. 126-148.

[90] On the need to establish general principles for transnational criminal proceedings, see J. Vervaele, S. Gless, "Law Should Govern: Aspiring General Principles for Transnational Criminal Justice", *Utrecht Law Rev.,* Vol 9, Issue 4, 2013, pp. 1-10: there is "need of rules that comprehensively deal with transnational criminal cases" (p.10).

creates a fragmented criminal procedure: the evidence is transplanted from one legal order to another[91]. This is a situation that is not originated by the EIO Directive, but exists ever since there is any international mutual legal assistance regarding to criminal evidence involving different legal systems. The fragmentation is not caused by the EIO, but should be addressed in a different way when implementing it in the European AFSJ.

220. The precise issue related to self-incrimination that will be addressed here is whether data obtained within administrative sanctioning proceedings are to be transferred for its use in criminal proceedings by way of an EIO, even if such data were obtained without respecting the right against self-incrimination. The problem appears frequently in criminal tax offence proceedings.

221. With regard to the right against self-incrimination in tax proceedings, the European Court of Human Rights has ruled, *inter alia*, in the cases *Saunders v. UK* of 17 December 1996[92], *IJL et al v. UK* of 19 September 2000[93], *Weh v. Austria* of 8 April 2004[94], or *Shannon v. United Kingdom* of 4 October 2005[95], that when the incriminating statement, in accordance with applicable law, was obtained under coercive means, this information cannot be admitted as evidence in the subsequent criminal procedure against the taxpayer concerned, even if such statements had been made before being charged. In particular, in those cases where the administrative procedure for establishing the tax due and the sanctioning procedure are not separated, the right to remain silent should also be granted during the inspection procedure. Otherwise, the sanctioning procedure would be based upon self-incriminating evidence, which is against the *nemo tenetur* principle[96].

---

[91] S. Gless, *Beweisgrundsätze einer grenzüberschreitende Rechtsverfolgung*, 2006, p. 142 ff.; I. Zerbes, "Fragmentiertes Strafverfahren. Beweiserhebung und Beweisverwertung nach dem Verordnungsentwurf zur Europäischen Staatsanwaltschaft", *ZIS* 3/2015, pp.145-155, although this last one refering specifically to the criminal proceedings under the EPPO.

[92] ECtHR, *Saunders v. UK*, App no 19187/91, 17 December 1996.

[93] ECtHR, *IJL et al v. UK,* App nos 29522/95, 30056/96, and 30574/96, 19 September 2000.

[94] ECtHR, *Weh v. Austria,* App no 38544/97, 8 April 2004, para. 44.

[95] ECtHR, *Shannon v. United Kingdom*, App no 6563/03, 4 October 2005.

[96] C. Palao Taboada, "El Derecho a no autoinculparse en el ámbito tributario: una revisión", *Revista española de Derecho Financiero,* num.159/2013, pp.1-25; J.A. Choclán

222. In the case *J.B. v. Switzerland*, of 3 May 2001[97] the ECtHR found a violation of the right against self-incrimination where it could not be excluded that the information requested from the taxpayer regarding his income –which he was obliged to provide under sanction–, could be used for charging him for the offense of tax evasion. This same doctrine was reiterated in the case *Chambaz v. Switzerland* of 5 July 2012[98].

223. The right against self-incrimination, is instrumental to the right of defence and must be respected *mutatis mutandis* also in administrative sanctioning proceedings. In this vein, the Spanish Constitutional Court has submitted "the essential values that are at the basis of Art. 24.2 SC would not be safeguarded if it were accepted that the administration could compel or force the taxpayer to confess –or testify about- the commission of acts that would serve for incriminating him/her"[99]. In another case the Spanish Constitutional Court, has granted full protection to the right against self-incrimination in administrative tax inspection proceedings also regarding the data obtained during an entry and search of premises, where the inspected person was not informed on the right to oppose to such entry and search.[100]

224. Applying the domestic rules of evidence, the data and objects obtained in infringement of fundamental rights cannot be assessed as evidence. In other

---

Montalvo**,** *La aplicación práctica del delito fiscal: cuestiones y soluciones,* Barcelona 2011, p. 465.

[97] ECtHR, *J.B. v. Switzerland*, App no 31827/96, 3 May 2001.

[98] ECtHR, *Chambaz v. Switzerland*, App no 11663/04, 5 July 2012. On the two separate opinions to this judgment see, C. Palao Taboada, "El Derecho a no autoinculparse en el ámbito tributario: una revisión", op. cit. pp. 4-5.

[99] Among others, STC 272/2006, of 25 September, para. 3; 70/2008 of 23 June, para. 4; and 142/2009, of 15 June, para. 4. Regarding the prior case law of the Spanish Constitutional Court on this issue, see C. García Novoa, "Una aproximación del Tribunal Constitucional al derecho a no autoinculparse ante la Inspección Tributaria en relación con los delitos contra la Hacienda Pública", *Jurisprudencia Tributaria Aranzadi*, 53/2005, pp. 1-9.

[100] Constitutional Court Judgment 54/2015 of 16 March: within a tax inspection regarding the infringement of the corporation tax law, VAT and other irregularities, the administrative authority ordered the entry and search of premises of the company investigated and the seizure of documents. The administrative authorization allowed the inspectors to carry out this measure, but only upon the consent of the owner or the administrator of the company. For the validity of the consent, the person affected –in this case the representative of the company- had to be informed of the existence of the administrative authorization as well as being made aware that the company could refuse to consent to the entry, search and seizure, unless there was a judicial warrant authorizing it

words, they have no evidentiary value. Nevertheless, following the wording of the DEIO, the objects, disks and data seized during the entry, despite being void, are "in possession of the executing authority". If the authority of another MS would issue an EIO requesting such information, shall the executing authority transfer the evidence already gathered even if such evidence would under domestic law be inadmissible for infringing a constitutional right? Could the requested authority invoke Art. 11.1. f DEIO as a ground for refusing to execute the EIO in the case described? Would the transfer of illegally obtained evidence –that would not have any evidentiary value under the law of the executing State– be contrary to the principles common to the MSs of "liberty, democracy, respect for human rights and fundamental freedoms, and the rule of law" (Art. 6.1 TUE)?

225. Transferring evidence that would not be admissible under the domestic laws of the executing state for having been obtained legally for the administrative sanctioning proceedings, but that would not comply with the protection granted under criminal procedure law and thus in violation of fundamental rights, would in principle not be against Art. 6 TUE or Art. 6 of the Charter. There are many EU MS where the exclusionary rules of evidence are not so strict as in the Spanish or the Italian legal system and a balancing test is applied for deciding on the admissibility of evidence[101]. In those States, the assessment of such evidence could be in conformity with Art. 6 TUE, despite not being in conformity with the *lex loci*.

226. The question is still, how shall the executing authority proceed? When receiving an EIO, the executing authority will have to face a difficult dilemma: either execute the EIO, assuming the risk that evidence that is tainted or even declared inadmissible in the executing State, may be used before a foreign court; or refuse the execution of the EIO because of the risk that the fundamental rights of the defendant might be infringed by the foreign trial court. The first alternative will promote the principle of mutual recognition and

[101] On the problems stemming from the lack of rules on admissibility of evidence obtained abroad, see the interesting contribution of S. Gless, "Transnational Cooperation in Criminal Matters and the Guarantee of a Fair Trial: Approaches to a General Principle", *Utrecht Law Rev.,* Vol. 9, Issue 4, 2013, pp. 90-108, 95-96.

the swift cooperation in the sphere of the cross-border evidence gathering. The second alternative tends to prioritize the protection of the fundamental rights of defendants, by keeping a double check on the respect of those rights, in the executing State as well as in the requesting State.

227. There is no identified practice on this issue in the legal framework of the countries studied, and Directive only states that the trial court should pay attention to the way the evidence was obtained in the foreign country when assessing the evidence obtained from abroad.

**63) Proposed best practice:** In the absence of a clear guideline, the proposed interpretation with regard to the use of evidence obtained under administrative proceedings without ensuring the right against self-incrimination in criminal proceedings, should always be in favour of the protection of human rights. Therefore if the evidence requested refers to data already in the possession of the executing authorities, but those data would not be admissible as evidence in the requested state, they should not be transferred to any other state.

### 11.12. Double criminality

#### *a) The lack of double incrimination as a possible ground of refusal*

228. The lack of double incrimination has been introduced as a possible ground for refusal under Art. 11(1) g DEIO albeit with certain limitations. First, this ground of refusal is not applicable to those cases where the requested measure is listed under Art. 10 (2) DEIO; and second, it cannot be invoked with regard to the EIO issued in relation of an offence listed in the Annex and such an offence is punishable with more than three years custodial penalty in the issuing State.

229. It seems appropriate that the lack of double incrimination might not be used to refuse the cooperation when it relates to an offence included in the Annex and it is considered a serious offence in the issuing State (penalty of more than three years), although with regard to the offences listed in the annex there hardly will appear any problems of lack of double incrimination. In practice the annex will facilitate the cooperation: if the issuing authority refers

in the requesting form that the offence is one of the 32 offences listed in the Annex, the requested authority will not need to check any double incrimination requirement and will not have to check if there would be a possible ground for refusal.

230. With regard to the requirement that the offence is punished with at least three years custodial penalty, it must be noted that this threshold might not be strictly necessary. In practice this case will not be frequent, as most of the 32 offences listed in the Annex are serious offences and are generally punished with more than three years. Moreover, in order to facilitate the cooperation, it should be enough that the offence is punishable in both States. Thus, if it is listed in the Annex, this should, as a rule be enough and the fact that the offence is punished with less than three years imprisonment in the executing State should not as a rule be a problem for executing an EIO as the principle of proportionality already appears protected under Art. 10 (1) b or Art. 11 (1) h DEIO: if the measure was not available for a similar domestic case or is restricted to offences of a minimum penalty.

231. The DEIO mentions expressly the offences connected to taxes or duties, stating that a EIO related to them shall not be refused on the basis that the executing State does not impose the same kind of tax or duty [Art. 10(1c) PD EIO]. This provision is a further clarification on the limits of the ground of refusal based on the absence of double incrimination.

**64) Proposed best practice:** The lack of double criminality should be interpreted in a very flexible way as a ground for refusal to cooperate with the requesting State. It has to be recalled that the grounds for refusal should as a rule have been regulated as optional and not mandatory. Those MSs whose legal framework have "transformed" the grounds for refusal into mandatory, when acting as executing State should not focus primarily in identifying grounds for refusal to avoid the cooperation, but rather in a flexible way.

### 11.13. Ne bis in idem

232. *Ne bis in idem* Art. is one of the optional grounds for refusal set out under 11(1) DEIO. This provision shall be interpreted in the light of recital 17 of

the DEIO, so that, in order to know whether in the framework of a specific case the *ne bis in idem* could be invoked. Consideration should be given to the European dimension of this principle as recognised by the Charter[102] and interpreted by the case-law of the Court of Justice of the European Union.

233. According to the CJEU case law the principle of *ne bis in idem* protest against a second criminal proceeding against the same person and for the same acts for which he/she has already been finally acquitted or convicted by a final judgment as well as from being punished twice fro the same facts. Furthermore, according to the CJEU, the principle of *ne bis in idem* applies both with regards to sanctions, preventing a duplication of sanctions (administrative/criminals) or with regard to proceedings (administrative/criminals), even though only in those cases where the administrative sanctions are "criminal in nature".[103]

234. Conversely, the CJEU has outlined the elements upon which the principle of *ne bis in idem* is based. Basically there are two conditions:

235. (a) The subjective and factual identity. That is, that the «same person»[104] is subject to a procedure or is sanctioned with a criminal penalty for the «same acts» (the *idem*)[105] for which he/she has already been

[102] Art. 50 of the Charter (2016/C 202/02) DO C202/389 (7.6.2016), as well as the Explanation to this provision, (Explanations relating to the Charter of Fundamental Rights, OJ C 303, 14.12.2007, p. 17-35), p. 31.

[103] According to the case-law of the Court there are three criteria to be considered in determining whether or not there is a "criminal charge": the legal classification of the offence under national law; the repressive nature of the offence; and the nature and degree of severity of the penalty that the person concerned risks incurring. In this regard, see the Engel criteria as set out in in the judgment of the ECtHR *Engel v. The Netherland*, App no 5100/71, 8 June 1976. See also CJEU, C-489/10, *Åklagaren Bonda*, 5 June 2012; CJEU, C-617/10, *Łukasz Marcin Fransson,* 26 February 2013; CJEU, C-596/16 and 597/16, *Enzo di Puma y Commissione Nazionale per la Società e la Borsa (Consob)*, 20 March 2018. In some cases, however, the CJEU has allowed certain limitations to the principle of *non bis in idem* or, what is the same, admitted the duplication of proceedings and sanctions classified as "criminal charge". In this sense, see CJEU, C-129/14 PPU, *Spasic*, 27 May 2014; CJEU, C-524/15, *Luca Menci*, 20 March 2018; CJEU, C-537/16, *Garlsson Real Estate and others*, 20 March 2018.

[104] CJEU, C-150/05, *Van Straaten*, 28 September 2006; CJEU, C-217/15 and C-350/15, *Orsi y Baldetti*, 5 April 2017.

[105] In the opinion of the CJEU, the expression «the same acts» is an autonomous concept of European Union law. CJEU, C-261/09, *Mantello*, 16 November 2010. On this concept, see also CJEU, C-436/04, *Van Esbroek*, 9 March 2006; CJEU, C-367/05, *Kraaijenbrink*,

convicted (or acquitted) in a previous procedure; and

236. (b) The existence of a final criminal decision, which includes any decision[106] – acquittal or conviction – that, according to the law of the State in which it was rendered, implies the definitive closing of the case[107] and has been adopted after an examination of the merits[108]. With reference to this second condition, it is also important to take into account that the CJEU finds to be compatible with Art. 50 Charter the so-called «execution condition»[109]. This condition – which applies in respect of the final judgments imposing a criminal conviction – implies that, in order for the *non bis in idem* to apply in respect of this kind of judgment, it is necessary that «…if a penalty has been imposed, it has been enforced, is actually in the process of being enforced or can no longer be enforced under the laws of the sentencing (State)» (Art. 54 CAAS)[110].

237. In the Italian, Spanish and Polish legislation implementing the EIO Directive the *ne bis in idem* has been regulated as a mandatory ground for refusal of the EIO[111]. However, to give this ground for refusal a practical meaning, it will need for the executing authority to know whether it applies or not. Unless this is notorious or the defendant invokes such ground for refusal, it will be difficult for the executing authority to take it into account.

***a) Cases where the ne bis in idem does not necessarily lead to the refusal of recognition and execution of the EIO?***

238. There are two circumstances where the EIO may not be refused on

18 July 2007; CJEU, C-150/05, *Van Straaten*, 28 September 2006; CJEU, C-467/04, *Gasparini and others*, 28 September 2006; CJEU, C-288/05, *Kretzinger*, 18 July 2007.

[106] That is to say also for the decisions which do not take the form of sentence or come from the public prosecutor and not from the judge. See CJEU**,** C-187/01 and C-385/01, *Gözütok y Brügge*, 11 February 2003.

[107] CJEU, C-491/07, *Turanský,* 22 December 2008; CJEU, C-261/09, *Mantello*, op. cit.; CJEU, C-398/12, *M*, 5 June 2014; CJEU, C-486/14, *Kossowski*, 29 June 2016.

[108] CJEU, C-496/03, *Miraglia*, 10 March 2005; CJEU, C-467/04, *Gasparini and others*, 28 September 2006; CJEU, C-398/12, *M,* op. cit.; CJEU, C-486/14, *Kossowski*, op. cit.

[109] CJEU, C-129/14 PPU, *Spasic*, op. cit. .

[110] CJEU, C-288/05, *Kretzinger*, op. cit.; CJEU, C-297/07, *Bourquain*, 11 December 2008; CJEU, C-129/14 PPU, *Spasic*, op. cit..

[111] Art. 10 (1) (d)LD, as regards Italy; Art. 32 (1) (a) LRM, as regards Spain; and Art. 589zj § 1 (“) PCPC, as regards Poland.

this ground, despite being regulated as a mandatory ground for refusal under domestic law[112]:

239. When the EIO is aimed at establishing if there is possible conflict with the *ne bis in idem* principle. In other words, when the EIO has been issued in order to clarify whether in respect of the same acts and against the same person a final irrevocable decision has been rendered.

240. The second circumstance or exception is that the issuing authority «has provided assurances that the evidence transferred as a result of the execution of the EIO would not be used to prosecute or impose a sanction on a person whose case has been finally disposed of in another MS for the same acts».

**65) Proposed best practice:** When the EIO aims to determine whether the acts and persons suspected by the issuing authority have already been judged, this should be explicitly indicated in Annex A DEIO (preferably in Section G). Similarly, when the issuing authority fears that the EIO may be refused in the executing State for this reason, it should specify in Annex A (and preferably in its Section G) that the evidence obtained would not be used to prosecute or impose a sanction on a person whose can already been finally disposed in another MSs for the same acts.

***b) How should the executing authority proceed when it has doubts that the acts which motivate the issuing of the EIO might have been subject to a final judgment in a third State?***

241. It is highly unusual that the executing authority is aware of the possible infringement of the principle of *ne bis in idem* when requested to execute an EIO.

242. In order to facilitate to check whether this ground for refusal may exist, it would be perhaps adequate to notify all the parties to the proceedings in the forum state of the issuing of the EIO. And at the same time, the executing authority should notify the parties affected by the

[112] See Recital 17 DEIO.

execution of the investigative measure,[113] so that they could put forward the possible ne bis in idem infringement.

243. In any case, the executing authority may not reject out of hand the execution of the EIO for this reason: before adopting a decision in this respect, it shall consult the issuing authority [Art. 11(4) DEIO], and involve also the authorities of the state where the decision that triggers the *ne bis in idem* was rendered (if it is different from the executing state).

**66) Proposed best practice:** In order to effectively enforce the *ne bis in idem* principle, issuing and executing authorities should ensure that, as far as possible, the parties to the process are aware of the issuing and/or receipt of the EIO and can oppose to it. If the executing authority considers that an EIO might be against the principle of the *ne bis in idem*, before taking a decision in this regard, it will initiate a consultation process with issuing authority and, where necessary, with the judicial authority which rendered the final decision on the same acts (if it is a third state).

***c) Is it possible to refuse an EIO on the basis of the principle non bis in idem because of litis pendens?***

244. Contrary to what happens in the domestic legal framework of some States, the European concept of *ne bis in idem* does not protect against the international *litis pendens*. Nor does the DEIO consider the pending of another criminal proceeding on the same facts against the same individual in another country as a ground for refusal – mandatory or optional – of the EIO[114]. If, on the occasion of an EIO, the executing authority acknowledges the existence of two or more parallel criminal proceedings on the same acts, it will proceed in the manner contemplated by the corresponding national law implementing the FD 2009/948/JAI, of the Council, of the 30 November,

[113] It should be recalled that Art. 22.1 LRM considers as compulsory such a notification in cases where the person concerned by the measure is resident or domiciled in Spain. However, an exception to this principle is made for the cases where the activities of the proceeding in whose framework the EIO has been issued are secret or in the cases where the notification may undermine the objectives pursued with the EIO.

[114] In this respect the DEIO is different from other instruments of mutual recognition. See Art. 4(2) FD EAW.

on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings[115].

**67) Proposed best practice:** Upon the receipt of an EIO the receiving or executing authority realize that the same facts are being investigated/prosecured in the requested State, the relevant authority shall notify this to the requesting authority and also involve Eurojust to address the issue on the jurisdiction, or eventually the setting up of a joint investigation team.

### 11.14. The meaning of Art. 6 (3) DEIO

245. The issuing authority has to assess the proportionality of the measure 'for the purpose of the proceedings' (Art. 6(1)(a) DEIO), and although the executing authority shall not check if such requirements are complied with, it can consult the issuing authority where 'it has reason to believe' that the EIO does not meet the required conditions of necessity and proportionality. Art. 6(3) of the Directive reads:

246. 'Where the executing authority has reason to believe that the conditions referred to in paragraph 1 have not been met, it may consult the issuing authority on the importance of executing the EIO. After that consultation the issuing authority may decide to withdraw the EIO.

247. Literally this provision it allows the executing authority to 'consult' the issuing one, when there are doubts as to the compliance of the requested measure with the conditions of proportionality and necessity. But, does this mean that the executing authority can question the assessment made by the issuing authority on the necessity of the measure? Having a look to the Explanatory Memorandum, it seems that this interpretation should be excluded. Should then the 'consultation' be limited to questioning the proportionality of the EIO? In such case, which criteria of proportionality could be subject to consultation: only the proportionality of the costs, or also the proportionality of

[115] DOUE L 328/42 (15.12.2009).

the intrusive measure in relation to the offence investigated? The way Art. 6(3) DEIO is drafted admits none of these interpretations.

248. Under a strict application of the mutual recognition principle, the executing authority should not check the proportionality and necessity of the measure requested and therefore, the justification of why such measure is needed and proportional for the investigation should not need to appear in the EIO. However, as was mentioned earlier, the DEIO has not gone so far as to provide for the automatic recognition and execution of the EIO in a blind way; rather it provides for the possibility to substitute the measure requested and even to refuse it when it does not meet the proportionality test applicable in the executing state. In particular, the executing authority shall have recourse to an investigative measure other than the one indicated in the EIO where the investigative measures selected by the executing authority would achieve the same result by less intrusive means than the investigative measures indicated in the EIO (Art. 10(3) DEIO).

### *a) Proportionality and costs*

249. The Directive does not further determine what shall happen once the executing state has made use of the possibility provided under Art. 6(3) DEIO. This provision only states: "After that consultation, the issuing authority may decide to withdraw the EIO". I already pointed out in previous papers that the meaning and aim of this sentence is unclear.[116] It could refer to the sharing of costs, in case the execution of the EIO would entail disproportionate efforts for the executing authority, and thus this provision should be read in conjunction with Art. 21 DEIO.[117] But, if it is not directly linked to the costs, once the consultation is done, what will be the consequence?

---

[116] Ibid, p. 52.

[117] Art. 21. Costs.

'1. Unless otherwise provided in this Directive, the executing State shall bear all costs undertaken on the territory of the executing State which are related to the execution of an EIO.

2. Where the executing authority considers that the costs for the execution of the EIO may be deemed exceptionally high, it may consult with the issuing authority on whether and how the costs could be shared or the EIO modified.

The executing authority shall inform the issuing authority in advance of the detailed

**68) Proposed best practice:** Article 6 (3) DEIO shall be interpreted in the sense that it requires to consult the issuing authority in all cases where there are questions related to the proportionality of the measure in terms of encroachment of fundamental rights as well as questions of the proportionality of the costs of the measure (related to the seriousness of the crime). Although Article 6 (3) DEIO states that the executing authority "may" consult, it should be advocated to consult in any event these doubts arise.

***b) Substitution of the requested measure***

250. Before resorting to another measure different from the requested one, the executing authority should inform the issuing authority, as provided under Art. 10(4) DEIO. The cooperation in the gathering of evidence under the DEIO is based on the fluent communication between the relevant authorities involved in the international cooperation, and thus any questions or problems arising in the process of executing an EIO should be dealt with by first consulting the issuing authority. Establishing a channel of consultations and reciprocal information should allow for finding the best possible solution in the process of cross-border evidence gathering for both the issuing and the executing authority.

251. In practice it has been seen that the EIO requesting the measure of entry and search of the bank premises to obtain certain financial information, is being substituted in Spain by the less coercive measure of issuing a production order. As in Spain, banks are obliged to provide such information in the context of a criminal investigation, the requested entry and search, is substituted in accordance with Art. 10.3 DEIO. This practice is not only very positive from the point of view of the efficiency, for reducing timeframes and costs, but also from the perspective of the proportionality principle. On the other hand, as such

specifications of the part of the costs deemed exceptionally high.
3. In exceptional situations where no agreement can be reached with regard to the costs referred to in paragraph 2, the issuing authority may decide to:
(a) withdraw the EIO in whole or in part; or
(b) keep the EIO, and bear the part of the costs deemed exceptionally high.'

measures do not require the judge to be involved, the judiciary is freed from being overburdened by such EIOs.

**69) Proposed best practice:** When receiving an EIO the executing authority shall substitute the requested measure by a less intrusive on, if such a measure would allow gathering the evidence requested. This practice has been observed frequently in the context of the request for bank data, where the requested measure of entry, search and seizure is being substituted by production orders. It would be possible that all MSs would provide for the possibility of accessing to bank information without the need to resort to a measure of entry and search.

## 12. LEGAL REMEDIES AT NATIONAL LEVEL

### 12.1. General considerations

252. Art. 14 DEIO deals with the legal remedies against the EIO, which can be challenged both in the issuing and in the executing State. More specifically:

253. States shall ensure that the decisions on the recognition and the execution of the investigative measures of the EIO, can be challenged in the executing State by way of "legal remedies equivalent to those available in a similar domestic case" (Art. 14.1 DEIO).

254. However, as a rule substantive grounds for issuing the EIO can be challenged *only* in the issuing State[118]. Despite the precise wording of Art. 14 (2) DEIO, interested parties should also be allowed to put forward challenges regarding the issuing of the EIO before the courts of the executing state, if this is provided within the domestic legislation: the DEIO itself recognises this possibility.[119] Moreover, it will be the only way to challenge the EIO when there is no other legal remedy in the issuing State.

255. The specific type of remedy and all the conditions to file it will be determined by the national legislation. What the DEIO requires as that such remedies are at least equivalent to those provided for similar national investigative measures [Art.. 14(2) and 6 DEIO]. Such challenge as a rule shall

[118] Art. 14 (2), in relation to Art. 6.1 DEIO.
[119] Art. 14 (2) DEIO, and recital 22 *in fine.*

not suspend the execution of the investigative measure, *unless it is provided in similar domestic cases*» [Art. 14 (6)].

256. The DEIO does not ultimately oblige the MSs to establish legal remedies against the EIO[120], nor can from this provision be inferred that the parties shall have a right to challenge the EIO.[121]

257. Another important aspect concerning legal remedies refers to the information that must be provided on them; or, rather, to the obligations that are imposed on the issuing and executing authorities in this regard. On the one hand the issuing and executing authorities have the duty to ensure that the parties promptly know the legal remedies applicable in each case (i.e., in due time «to ensure that they can be exercised effectively»). This obligation does not apply in the cases where the information may compromise the confidentiality of the investigation [Art. 14 (3) DEIO]. On the other hand issuing and executing authorities shall inform each other about the legal remedies sought against the issuing, the recognition or the execution of an EIO [Art. 14 (5) DEIO].

258. The success of the action brought in the executing state against the decision to recognise or execute the EIO, will be also of great importance, due to the fact that evidence obtained in violation of the *lex loci* will not automatically be excluded in the proceedings. Exclusion or admissibility of such evidence will depend on the laws of the forum state [Art. 14 (7) DEIO].

### 12.2. Legal remedies at the national level

#### *a) Spain*

259. Art. 14 DEIO has not been specifically implemented in the Spanish legislation.

---

[120] It should be recalled that the Council Framework Decision 2003/577/JAI (Art. 11 (1) y 5) obliged the MSs to establish such remedies for cases where the EEW contained coercive measures.

[121] It does not seem, thus, that Art. 14 DEIO provides directly a right to challenge a decision on the EIO. Nor it seems that the impossibility to challenge the EIO at the national level is contrary to the mentioned Art. 14 DEIO. It is nevertheless necessary to wait for the CJEU decision on the preliminary ruling, C-324/17, *Gavanozov*, filed on the 31 May 2017 (OJEU C 256/16).

260. LRM [122] provides that against the EIO the same legal remedies as provided in a similar domestic case will be applicable. Following this rule the identification of legal remedies against the EIO –taking into account the diverse factors that apply– results in the following:

| **Issuing of the EIO** | **Public prosecutor** (Prior to the opening of the criminal trial) | **Investigating judge (*)** (When a criminal proceeding has been initiated, but prior to the judgment) | **Trial Court** (Trial) |
|---|---|---|---|
| **Pre-trial investigations by the prosecutors** | There is no appeal (Art. 13.4 LRM). | | |
| Pre-trial phase of the criminal proceeding against minors | No direct appeal is provided, but the parties may challenge it before the Juvenile Judge (Art. 26.2 LORPM). | | |
| Proceeding for crime punishable with imprisonment of more than 9 years Proceedings for grave crimes (Procedimiento ordinario) | | Reforma/appeal (Art. 216 y ss. LECrim).<br>***<br>Annulment of the proceedings/ acts (240.2 LOPJ) | No direct appeal is permitted, but it is possible to lodge complaint. It is necessary to lodge complaint in order to appeal the judgment (Art. 659 LECrim). |

[122] Art. 13 LRM, with regard to appeals against decisions concerning the issuing of the EIO; and Art. 24 LRM, with regard to the appeals against the decisions concerning the recognition and execution of the EIO.

| | | | |
|---|---|---|---|
| | | | *** Annulment of the proceedings/acts) (240.2 LOPJ) |
| Proceedings for crimes punishable with imprisonment up to 9 years (Procedimiento abreviado) | | Reforma/appeal (Art. 766 LECrim). *** Annulment of the proceedings/acts (240.2 LOPJ) | No direct appeal is permitted, but the part that requested the issuing of the EIO and whose request was rejected may reproduce its request at the beginning of the trial (Art. 785.1º II LECrim). Against the decisions adopted at the beginning of the trial on the issuing of the EIO there is no direct appeal, but it is possible to lodge complains. The lodging of such a complain is necessary in order to appeal |

| | | | |
|---|---|---|---|
| | | | the judgment (Art. 786.2º LECrim).<br>***<br>Annulment of the proceedings/acts (240.2 LOPJ) |

* The same system of appeals applies in cases where the EIO is issued by a Court for Violence against Women (*Juzgado de Violencia sobre la Mujer*) or by a Central Investigating Court (*Juzgado Central de Instrucción*). If the EIO is issued by a Juvenile Judge (measures restricting of fundamental rights), there is a right to reform and to appeal the decision (Art. 41.2 LORPM).

** The Courts and Tribunals of this kind are, among other, the Criminal Courts, the Provincial Court (*Audiencia Provincial*), the Central Criminal Courts, the Criminal division of the National High Court (*Sala de lo Penal de la Audiencia Nacional*), the Juvenile Courts; and the civil and criminal divisions of the High Court of Justice and the Criminal Division of the Supreme Court (the latter two courts are competent to adjudicate the cases against persons with a special personal jurisdiction).

| **Recognition and execution EIO** | **Public Prosecutor** | **Investigating Judge (*)** | **Juvenile Judge (**)** |
|---|---|---|---|
| Measures not restricting the fundamental rights | There is no appeal (Art. 24.4 LRM) | *a) Proceeding for crimes punishable with imprisonment of more than 9 years* (Proceedings for grave crimes (Procedimiento ordinario)<br>Appeal (Art. 216 ff. LECrim).<br>***<br>Annulment of the proceedings/ acts (240.2 LOPJ)<br>*b) Proceeding for crime punishable with imprisonment up to 9 years (Procedimiento abreviado)*<br>Appeal (Art. 766 LECrim)<br>***<br>Annulment of the proceedings/acts (240.2 LOPJ) | Appeal (Art. 41.2 LORPM).<br>***<br>Annulment of the proceedings/ acts (240.2 LOPJ) |
| Measures restricting the fundamental rights or EIO in which the issuing authority requires the intervention of the judge | | | |

* The same system of appeals applies in cases where the authority competent to the recognition and execution is a "Juez Central de Instrucción" or a "Juez Central de lo Penal".
** The same system of appeals applies in cases where the authority competent to the recognition and execution is the Central Juvenile Judge (Juez Central de Menores).

261. In accordance with Art. 14 (6) DEIO, the lodging of an appeal against the EIO does not suspend the execution of the measures there included. However, and as an exception, it is possible to suspend the execution of the order when, in carrying it out, may be created «irreversible situations or may cause injury that will be impossible or difficult to redress». In those cases, the suspension may be accompanied by the provisional measures necessary to ensure the effectiveness of the measure (Art. 24.1.II LRM).

262.

***b) Italy***

263. The Italian legislation does not foresee the possibility of **appealing against** investigative measures agreed at the national level. On this premise, and given that the LD also omit any reference to the possibility of challenging the EIO when it is issued in Italy it shall be concluded that it is not possible to challenge the decisions taken in this regard by the Public prosecutor (decreto) or the judge (ordinanza). Are exempted from this rule the cases when the EIO is to be regarded as a *seizure aimed at evidence*[123].

264. The LD, on the contrary, provides for a system of "opposition" against the decree of recognition of the EIO by the Public prosecutor (Art. 13 § 1 a 6 LD). This "remedy" – which should be brought within five days before the judge for preliminary investigations – shows some shortcomings[124]:

265. The first is that only the suspected person and his/her lawyer may use it. It is, thus, not possible the "opposition" by third parties. In other cases, the

[123] Cfr. Art. 28 LD and Art. 368 and Art. 324 ICPC.

[124] Particularly in comparison with the other "*remedy*" envisaged against the decree concerning the execution of a *seizure aimed at evidence* (Art. 13 § 7 LD). See extensively, A. Mangiaracina, "L'acquisizione "europea" della prova cambia volto: l'Italia attua la Direttiva relativa all'ordine europeo di indagine penale*", Diritto penale e processo*, 2/2018 p. 169 ff.

resolution (decreto) of recognition is communicated to the defence, which prevents *de facto* its "opposition".

266. Furthermore, it should be noted that if the "opposition" is successful, the decree of recognition of the EIO is annulled. Such an outcome may cause problems in the issuing State in respect of the evaluation of the evidence obtained.

267. The filing of the "opposition" in no case suspend the execution of the investigative measure. The only decision that may be taken by the Public prosecutor is to suspend the transmission of the evidence to the issuing State when such a transmission may cause a serious and irreparable harm to the suspected person (Art. 13§4 LD).

268.

| **Issuing state EIO** | **Public Prosecutor** (Pre-trial) | **Judge for the preliminary hearing** (Pre-trial) | **Judge** (Trial) |
|---|---|---|---|
| Criminal proceedings | a) In general Remedies?<br>b) Seizure aimed at evidence<br>Request for a review (Art. 28 LD and Art. 324 ICPC) + Appeal and Cassation (Art. 322 bis and 325 ICPC) | a) In general Remedies?<br>b) Seizure aimed at evidence<br>Request for a review (Art. 28 LD and Art. 324 ICPC) + Appeal and Cassation (Art. 322 bis and 325 ICPC) | a) In general Remedies?<br>b) Seizure aimed at evidence<br>Request for a review (Art. 28 LD y Art. 324 ICPC) + Appeal and Cassation (Art. 322 bis y 325 ICPC) |
| Proceedings for the application of | Seizure aimed | Remedies? | Remedies? |

| | | | |
|---|---|---|---|
| financial preventive measures (“Anti-Mafia Code) | at evidence Request for a review (Art. 28 LD and Art. 324 ICPC) + Appeal and Cassation (Art. 322 bis and 325 ICPC) | | |

**(To be reviewed and completed)**

| **Executing state EIO (Art. 13 LD)** | **Public prosecutor** | **Judge** |
|---|---|---|
| | *a) In general:*<br>Opposition to the judge for the preliminary investigations within five days since the communication of the decree which recognise the EIO<br>(Art. 13.1 LD)<br><br>b) Seizure aimed at evidence:<br>Opposition to the judge for the preliminary investigations within five days since the communication of the decree which recognise the EIO + recourse to the Supreme Court<br>(Art. 23.7 LD and 127 ICPC) | *a) In general:*<br>Opposition to the judge for the preliminary investigations within five days since the communication of the decree which recognise the EIO<br>(Art. 13.1 LD)<br><br>b) Seizure aimed at evidence:<br>Opposition to the judge for the preliminary investigations within five days since the communication of the decree which recognise the EIO + recourse to the Supreme Court<br>(Art. 23.7 LD and 127 ICPC) |

### 2.3. *Poland*

269. As in Spain, in Poland the system of appeals applicable to the issuing and execution of the EIO is the one foreseen at the national level to challenge those decisions concerning the adoption of certain investigative measures or decisions to secure evidence which do not have a cross-border nature.

270. So, it is possible to lodge an interlocutory appeal against the decision to issue the EIO, but only when the order includes certain measures as, i.e., domicile enquiries or tracking of the location of a person holding and opening of correspondence the seizure of property or the monitoring and interception of telephone and electronic telecommunications (Art. 589w § 4, in connection with Art. 236, 240 y 241 PCPC). With regard to the latter sort of measures (i.e., the surveillance and wiretapping and the interception of e-communications including the e-mails), it is important to take into account that Polish law provides that the parties will not be informed of the decision granting this measure when it is necessary to protect the successful outcome of the investigations. This notification should in any event be done prior to the ending of the pre-trial stage (Art. 589ze § 4, in relation with Art. 239 PCPC).

271. According to Polish law, not only the defence, but any person affected by the investigative measures mentioned above is entitled to challenge is lawfulness.

272. The polish report points out that "the decision of execution of the EIO cannot be challenged in Poland". Does this mean that there is no recourse against the decision to recognize or execute an EIO? In Poland, does the remedy suspend the application of the measures?

## 12.3. Who may challenge the issuing/execution/deferral of the EIO? The term "parties concerned"

273. The term "parties concerned" used in Art. 14(4) DEIO casts doubt on

who can appeal the decisions adopted in relation to the EIO[125]. However a systematic interpretation of this expression,[126] allows to conclude that it encompasses also the third parties affected by the investigative measure or the provisional measure provided in the order. Concerend party is anyone affected by the order or the measure.[127]

**70) Proposed best practice:** The effective legal remedies against the EIO must be available for the parties to the criminal proceeding and for the third parties affected by the EIO. Consequently, when the respective national laws provide for an appeal in a similar domestic case, will be considered part of the process those third parties, at least for the purposes of challenging the decision or measure which affects them. This, of course, this is possible if the information about the possibility to use these legal remedies is given to the third persons as soon as this information does not undermine the successful outcome of the investigations[128].

[125] The already mentioned reference for a preliminary ruling C-324/17, *Gavanozov*, op. cit., can be taken as an example of these doubts. In this case, the questions referred to the CJEU concern the search on residential and business premises, the seizure of specific items and the examination of a witness; all measures included in an EIO issued by Bulgaria. The first question is whether the holder of the domicile or a person who is to be examined as a witness are considered as «person concerned» for the purpose of Art. 14(4) DEIO. The second question asked is whether in the case that the investigative measure is directed to a third person, the suspected or accused person may be considered as «person concerned» with a view to challenge the EIO.

[126] It should be noted that Art. 13.2 DEIO establishes the compulsory suspension of the transfer of the evidence to the issuing State if such a transfer «would cause serious and irreversible damage to the person concerned». This provision clearly shows the balancing of the interests of the criminal investigation and the rights and legitimate interests of the person concerned by the measure, regardless whether the latter is a party or a third party.

It should also be reminded that both the FD 2003/577/JHA (Art. 11) as well as the FD 2008/978/JHA (Art. 18) use the term "party concerned", although both instruments specified explicitly that the term comprised also the "bona fide third parties".

[127] This is the interpretation in compliance with ECtHR, *MN and Others v. San Marino*, App no 28005/12, 7 July 2015 and ECtHR*, Brito Ferrinho Bexiga Villa-Nova v. Portugal*, App no 69436/10, 1 December 2015.

[128] In Spain this notification represents a legal obligation in the cases where the person concerned by the measure is resident or domiciled in this State. See Art. 22 (1) LRM.

## 13. TRANSFER OF DATA AND SPECIALITY PRINCIPLE

274. An issue that in practice may raise problems is the one related to the data protection of the information obtained by a MS ("A") from the executing State ("B") in execution of an EIO. In this case, a problem concerns how the information obtained by the State A in execution of the EIO may be used. May they only be used for the specific purpose and in the framework of the specific criminal proceeding in relation to which the EIO has been issued (principle of speciality in data protection law), or may this information be used in other proceedings, for other reasons than those indicated in the EIO? Even more, may this information be forwarded from MS A to another MS ("C"), without the consent of the executing MS B that transmitted these information for the specific purpose indicated in the EIO?

275. These questions arise, in particular, because of the principle of speciality, or principle of "purpose limitation", according to which personal data shall be collected for specified, explicit and legitimate purposes and not further transmitted to others, nor can they be used for purposes other than those for which they were transmitted to the recipient. According to this principle, thus, apparently State A could not transmit to a third State C the data obtained from a State B for the specific purpose indicated in the EIO; in fact, every time that State A would like to transmit the information obtained via the EIO to another MS C or every time that it would like to use them for another purpose or in another proceeding, it should ask State B for consent or authorisation to use or forward these information for a purpose other than this indicated in the EIO.

276. However, at the same time, allowing State A to forward the information obtained in execution of the EIO to another MS C requesting them for the purposes of another investigation without asking for the consent of the executing MS B would ensure to the maximum extent possible the free circulation of evidence and information between national competent authorities within the area of freedom, security and justice and the effective investigation and prosecution of the perpetrators of crimes having a cross-border dimension.

277. It is, thus, fundamental to find a balance between these two different needs: the need to ensure the protection of the data transmitted from State B to State A and the need to ensure the free circulation of evidence between the MSs in order to ensure the effective prosecution of the perpetrators of the crimes committed on, or otherwise connected to, the territory of more than one MS. The solution proposed as a guideline is, thus, the one that in our opinion allows to the largest extent possible to reconcile these two different needs.

### 13.1. Possible interpretations

278. In the first instance, it should be highlighted that the DEIO, differently from the 2000 MLA Convention, does not expressly regulate this rule. Thus, in this respect, three different interpretations are possible.

279. **1)** According to a first interpretation, the MS A which received the information in execution of an EIO can not use these information in another proceeding, at least if it is not strictly and directly connected to the one in relation to which the EIO has been issued, nor can it forward these information to another MS C requesting them through an EIO without the consent of the executing State B which gave it the information. This interpretation has been adopted by some national implementing laws, such as Art. 193 of the Spanish implementing law, which says that the Spanish authority can not use the information obtained in execution of an EIO for other purposes than those explicitly indicated in the EIO without the consent of the executing authority or the data subject. According to this interpretation, therefore, the issuing authority which received the information in execution of an EIO must ask for the consent/authorisation of the executing authority every time that it wants to use the data for other purposes than those indicated in the EIO. Such a strict interpretation of the data protection principle of speciality was also adopted by Art. 23 of the 2000 MLA Convention.

280. According to the Directive, the personal data communicated could be used by the MS to which they have been transferred only “for the purpose of proceedings to which this Convention applies, for other judicial and administrative proceedings directly related to proceedings referred to under

point (a), for preventing immediate and serious threat to public security" or "for any other purpose, only with the prior consent of the communicating MS, unless the MS concerned has obtained the consent of the data subject". However, the 2000 MLA Convention has been replaced by the DEIO.

281. According to Art. 34 DEIO, the DEIO "replaces, as from 22 May 2017, the corresponding provisions of the […] (c) Convention on Mutual Assistance in Criminal Matters between the MSs of the European Union and its protocol". In this respect, the corresponding provision[129] of Art. 23 MLA is Art. 20 DEIO, which concerns the protection of personal data. Thus, according to a literal interpretation, Art. 20 DEIO replaces Art. 23 of the 2000 MLA Convention. In this regard, it has nevertheless been argued that the verb used in the DEIO is "replace" and not "derogate". The provision on data protection of the 2000 MLA Convention, i.e. Art. 23, would therefore be still applicable, as far as it is not explicitly derogated by the DEIO. If such an interpretation is retained, the use of the data for other purposes than those indicated in the EIO would thus be possible only with the consent of the data subject or of the executing State according to Art. 23 of the 2000 MLA Convention.

282. **2)** According to a different interpretation, on the contrary, Art. 20 DEIO fully applies and, thus, the data communicated in execution of an EIO is to be processed in accordance with Directive (EU) 2016/680 "on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA", which repeals the Council Framework Decision 2008/977/JHA mentioned in Art. 20 DEIO. In this regard, Directive 2016/680 provides that "MSs shall provide for personal data to be: processed lawfully and fairly;

[129] On the controversial concept of "corresponding provisions", see also Council Document, "Note on the meaning of "corresponding provisions" and the applicable legal regime in case of delayed transposition of the EIO Directive", doc 9936/17 LIMITE, 13 June 2017, Annex II. Council Document, "Extracts from Conclusions of Plenary meetings of the EJN concerning the practical application of the EIO", 15210/17, 8 December 2017, p. 3, let. b), p. 8, point 1.

collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes; adequate, relevant and not excessive in relation to the purposes for which they are processed; […] kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed."[130]

283. Thus, according to the 2016/680 Directive, the data obtained in execution of an EIO may be processed for any other purposes concerning the prevention, investigation detection or prosecution of criminal offences other than that for which the personal data were collected, if such a use is allowed in accordance with Union or MS law and if the processing of data is necessary and proportionate to that other purpose in accordance with Union or MS law. It seems therefore that the processing of data for a purpose other than that for which the information were collected is allowed if it results from a case by case assessment that the use of the information is "proportionate and necessary to that other purpose" in accordance with national or European law; an evaluation of the proportionality and necessity of the use of the data concerned for the other purpose for which they are to be used is thus necessary. From a combined reading of Art. 20 DEIO and Art. 4(2) of the 2016/680 Directive, it seems, thus, that MS A does not have to ask for the consent/authorisation of the executing State every time that the data received in execution of an EIO should be used in another proceeding for purposes other than those for which they were requested or when they are requested through an EIO by another MS C. MS A may, in fact, use this data for another purpose or forward them to another MS C, as far as it is allowed to do so according to its national law and as far as this processing is necessary and proportionate for that other purpose in accordance with Union or MS law. In this regard, it should therefore be mentioned that Art.

[130] See Art. 4, par. 1 of the 2016/680 Directive. Furthermore, Art. 4(2) provides that "processing by the same or another controller for any of the purposes [of 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] other than that for which the personal data are collected shall be permitted in so far as: (a) the controller is authorised to process such personal data for such a purpose in accordance with Union or MS law; (b) processing is necessary and proportionate to that other purpose in accordance with Union or MS law".

193 of the Spanish implementing law could be an obstacle for the Spanish authority in forwarding these information without the prior consent of the executing State, which is expressly required under the Spanish national law[131].

284. The same result, i.e. the necessity to ask for the consent of the executing authority, may also be derived from a systematic interpretation of a given national legal system, such as the Italian one, where there is no specific rule in this regard. In this case, in the absence of a specific provision, the general rules apply and thus, by a coherent interpretation of Art. 729 of the Italian code of criminal procedure, the use of a forwarded investigatory act could be limited to a specific proceeding.

285. **3)** According to another interpretation, on the contrary, the "speciality rule" does not apply in relation to the transfer of evidence, as there is no specific legal basis in the DEIO on the applicability of the speciality rule. If such an interpretation is accepted, in those national legal system, as the Polish one, where there is no provision ensuring the respect of the principle of speciality with regard to the transfer of evidence, there is no warranty that the evidence obtained by MS A in execution of an EIO will not be forwarded to MS C, provided that is possible according to the Polish national legal system. This interpretation is in line with the wording of another provision of the DEIO, namely Art. 10(2)(a), according to which there are some investigative measures which must always be available under the law of the executing State, such as "the obtaining of information or evidence which is already in the possession of the executing authority and the information or evidence could have been obtained, in accordance with the law of the executing State, in the framework of criminal proceedings or for the purposes of the EIO". Thus, according to this provision, MS A has to forward to the requesting MS C the information received

[131] However, see in this regard the report on the evaluation of the practice in relation to the Spanish system, where we read that "some of the Magistrates have answered they transfer data obtained in a criminal investigation to other proceedings, even if those data have not been obtained in the specific case for which the judicial cooperation was requested. In their opinion, the prosecution of crime prevails over the principle of specialty in evidence matters, prevailing the principle of availability. Any information that has been obtained can be provided on the basis of the lack of prohibition of the spontaneous exchange of information. Limitations on an exchange of date are considered an inadequate barrier to international judicial cooperation" (p. 27 of the Report).

in execution of an EIO from MS B that are now in its possession. According to this provision, MS A would not only be allowed, but even obliged to forward this information to the requesting MS C. Thus, if one considers that once they have been received by MS A, this information is in its possession, Art. 10(2) DEIO would apply. The consequence would be that, as in this case, the European legislator decided to make sure that the need to ensure the free circulation of evidence prevails over the need to ask every time for the consent/authorisation of the executing State, and MS A could forward the information to MS C without the need to ask for the previous consent of MS B.

286. **4)** According to another interpretation of the silence of the Directive on the applicability of the speciality rule, in the "Conclusions of the 49th Plenary meeting of EJN", which took place in Tallinn, November 2017, and particularly in the Workshop III on the "practical implementation of the European Investigation Order in criminal matters", some argued in favour of an interpretation according to which the evidence obtained in execution of an EIO are subject to the speciality principle and may, thus, be transferred to another MS, only if the requirement of double criminality is fulfilled.

287. **5)** Finally, according to another interpretation, Art. 19 of the Directive, which concerns the duty of confidentiality, can be considered as an argument for the rule of speciality to be applied. As stated by Art. 19 DEIO, the executing authority "shall, in accordance with its national law, guarantee the confidentiality of the facts and the substance of the EIO, except to the extent necessary to execute the investigative measure" and "the issuing authority shall, in accordance with its national law and unless otherwise indicated by the executing authority, not disclose any evidence or information provided by the executing authority, except to the extent that its disclosure is necessary for the investigations or proceedings described in the EIO." Finally, Art. 19(4) DEIO, which concerns the disclosure of bank information, obliges the MSs to take the necessary measures to ensure that the bank does not disclose to the bank customer concerned or to other third persons that information has been transmitted to the issuing State or that investigation is being carried out in execution of an EIO.

288. At first sight, it seems, thus, that pursuant to Art. 19 DEIO, MS A cannot forward the information to MS C without the consent of MS B. According to this provision, the issuing authority, i.e. in the example MS A, must, "unless otherwise indicated by the executing authority", not disclose any evidence or information provided by the executing authority, "except to the extent that its disclosure is necessary for the investigations or proceedings described in the EIO". Thus, MS A, according to this provision, must not disclose the information obtained in execution of an EIO, except in two cases: in the first place, in case there is an express consent or indication to that effect from MS B, and, in the second place, if that disclosure is necessary for the investigations or proceedings described in the EIO. Consequently, it seems that if the disclosure of the information is not necessary for the investigations or proceedings described in the EIO, but it is necessary for another investigation, the consent of the executing State is needed.

289. However, on closer examination, from the analysis of the rationale behind Art. 19 DEIO, one infers that the aim pursued by the legislator with Art. 19 DEIO is different from the objective sought by the legislator when requiring the respect of the speciality principle in the transferring of evidence, as it was the case, for example under the 2000 MLA Convention. In fact, unlike the principle of "purpose limitation" or speciality principle, which aims at protecting the personal and confidential data of the data subject, the duty of confidentiality referred to in Art. 19 DEIO aims at ensuring that the competent authorities can carry out effective investigations.

290. This is patently clear from paragraph 4 of Art. 19 DEIO, but can also be inferred from a closer examination of paragraphs 1-3 of Art. 19 DEIO. According to Art. 19 DEIO, the person to whom information must not be disclosed is in fact the suspect or the data subject and not other judicial authorities; the aim of the provision is not to damage the investigation. The consent of State B is thus required in this case in order to ensure the confidentiality of the investigation, so that the competent authorities may effectively carry out their investigation. On the contrary, the principle of speciality aims at ensuring that the confidential data concerning the data subject are not forwarded to another authority to

ensure an adequate data protection of the data of the data subject. That is completely different from the case of Art. 19 DEIO, according to which the judicial authority may decide not to disclose the information known to it to the data subject in order to ensure that investigations are carried out effectively.

291. It follows *a contrario* that **the information may be disclosed to carry out investigation having a different purpose than the one for which they were obtained through the EIO if this does not damage the investigation in relation to which the EIO was issued.** The different objectives pursued, thus, change the way of interpreting the need of confidentiality and secrecy of the information and the consequent possibility to use this information in other criminal proceedings. In this respect, it should be noted that, even if it is true that in some cases are the same information which are not disclosed to judicial authorities of another MS in order to ensure the respect of both the principle of speciality and the duty of confidentiality, this is not always the case; thus, one can not derive the need to ensure the respect for the principle of speciality from Art. 19 DEIO, which protects a different interest, i.e. the confidentiality of the investigations.

292. **6)** In conclusion, however, from an overall interpretation of the European legal framework, i.e. of the whole DEIO and the Directive 2016/680, it seems that the interpretation under point 3) is possible only in relation to the so-called non-coercive investigative measures, namely those measures which do not restrict the fundamental rights of the individuals concerned. In fact, in case of coercive measures affecting the fundamental rights of the persons concerned, an interpretation according to which MS A must obtain the consent of MS B or of the data subject or, if the interpretation under point 2) is retained, must evaluate whether the processing of the information in its possession is necessary and proportionate to that other purpose in accordance with national and European law, seems the more suitable solution in order for the right to data protection of the subjects concerned to be fully respected.

**71) Proposed best practice:** In case that MS A is requested to forward to MS C via an EIO the information obtained from MS B in execution of an EIO, it is recommended that, in case of non-coercive measures MS A forwards the

information without needing to ask for the consent/authorisation of MS B from which it obtained the information. On the contrary, in case of coercive measures, it is recommended that MS A, either ask for the consent of MS B or of the data subject, or assess itself whether the processing of the information for this other purpose is necessary and proportionate for this other purpose in accordance with national and European law.

## 14. TRANSFER OF THE EVIDENCE

293. There is no uniform practice on this. First, the channel to transfer the evidence gathered in the executing State will depend on what kind of evidence it is. If the evidence can be transmitted via mail –because it is documented evidence, documents, or any kind of e-evidence or images, it should be transferred via secured channels. However, not all countries have implemented those secured channels. The existing channels are: 1) the EJN STN; 2) via Eurojust; 3) the COM Secure Online Portal; 4) via Interpol through the e-MLA support; 5) and finally by way of the Schengen Information System.

294. Depending on the type of proceedings and the competent authority issuing/executing the EIO, one of those channels will be chosen. Practitioners generally claim that having a secured communications channel accessible from their own office (be it the PP office or the court), would speed up the transfer of the evidence gathered, as well as ensure the confidentiality of the procedure and the security of the data transferred.

295. In those cases where the evidence to be transferred cannot be done by way of IT communications systems, the channel for sending the pieces of evidence to the issuing State will also depend on the type of object to be sent (a vessel, and the measures needed to ensure the preservation of the object (blood samples, chemicals, etc.) as well as the security measures that need to be implemented (e.g. samples of explosives, arms, money, etc.). In the countries studied practice shows that it is very frequent that law enforcement agents serving in the judicial police and in the cooperation units, travel to the relevant country either to bring or to collect the objects of evidence. In general no

problems are reported. The issue is still to rethink if such system is the optimal one from the point of view of securing the evidence and also from the perspective of the costs.

296. Other MSs have started outsourcing such transportation services, so that they hire a specialised company for carrying out the transfers of evidence.

**72) Proposed best practice:** The best practice for transfer of evidence that can be transmitted via internet communication, is to implement the secured communications channel in each MS and if possible in each judicial district. While this is not implemented, the authorities should use any of the reliable existing channels (via EJN, Eurojust, SIS, COM Secure Online Portal, or e-MLA), which enable to establish the identity of the sender, the recipient, the content of the message + attachments and the date and time of the transfer, without possibilities of being manipulated. For other objects, it would be positive to adopt a common protocol on how the evidence should be transported, in order to ensure the authenticity and integrity of such evidence. The aspects of the costs should also be further studied.

## 15. SPECIFIC INVESTIGATIVE MEASURES

### 15.1. Entry and search of premises: the seizure of computer stored data. How should the executing authority act when the EIO requests the measure of entry and search, but does not specify which objects or data shall be seized?

297. The question to be addressed is how to deal with EIO request the measure of search and entry, but does not specify which objects or precise data are to be seized. This is in particular problematic when Spain is receiving authority, because the legal reform introduced in 2015 require a specific justification for the seizure of computer data. This means that a judicial warrant authorizing the entry, search and seizure does not cover the searching of computers in Spain. Without a specific authorization, the law enforcement officers carrying out the entry and search will be allowed to seize the computer but not to access the data stored in it. The search of a computer requires a specific motivation and is not covered by the general search and seizure warrant.

298. Therefore, when it is foreseeable in advance that during the entry and search, the seizure of computers, telephone or electronic communications instruments, mass storage digital information devices, or the access to electronic data repositories will take place, the judicial warrant authorizing the search of dwellings shall extend its reasoning to express the reasons, if any, that authorize the agents to access the information contained in such devices.

299. 2. The simple seizure of any of the devices mentioned in the preceding paragraph, carried out during the home search, does not authorize to access to its content, notwithstanding the possibility that such access could be authorized later by the judge.

**73) Proposed best practice:** If the issuing authority requests to seize data stored in a computer, in order to comply with the *lex loci* in Spain a specific justification is needed, in addition to the ordinary search and seizure. The receiving authority should make aware the issuing authority of such requirement and consult whether the seizure of computer data is also requested. If this is the case, the issuing authority should complement the previous EIO, and add the specific motivation for searching the computer and seizing the stored data.

### 15.2. Interception of communications

300. Following the wording of Art. 17 to 20 of the Convention on Mutual Assistance in Criminal Matters between the MSs of the European Union of 29 May 2000,[132] the Directive 2014/41 has also included special provisions regarding the interception of telecommunications. In fact, several provisions of Art. 30 DEIO resemble, or are practically identical to, those already established in the EU MLA Convention.

#### *a) The problem of defining "interception of telecommunications"*

301. There is no common understanding what should be included within the concept of "interception of telecommunications" to the aim of the EIO. It is not our purpose here to establish a common definition that is valid for all kinds of

[132] 2000/C 197/01.

interceptions and for all domestic legal systems nor to delve in complex conceptual issues. To the aim of this CBP all the investigative measures that use a telecommunication connection will be dealt with under "interception of telecommunications", regardless if it affects meta-data, content data, conversations, access to stored data or interception on real time, or geo-location data. Traffic data and IP-address identification would fall outside the regulation of "interception of communications.

302. Of course, each of these measures is regulated differently in each of the MS and subject to diverse conditions, depending of the intrusiveness in the fundamental rights of the persons affected. But to the aim of the EIO, all of them would fall within the concept of "coercive" measure, as long as these measures can imply an encroachment –less severe or more severe– of the right to privacy and/or data protection or secrecy of communications. Being aware of the simplification this may entail, it is probably the more logical way to address the rules on the EIO.

***b) What is the degree of suspicion that would allow the interception of communications? Should the executing authority be able to check it in order to ensure that the measure would be allowed in a "similar domestic case"?***

303. In the Spanish system, law enforcement agents cannot resort to measures that restrict fundamental rights for preventive or intelligence purposes[133]. The use of electronic investigative measures in a proactive setting is prohibited expressly by Art. 588 bis (a) (2) LECRIM[134], seeking to prevent a

[133] On the contrary, Germany has regulated the remote search of computers in the preventive sphere, both for intelligence (*Verfassungsschutz*) as well as for law enforcement preventive purposes (*Polizeirecht*), but up to now not as an investigative measure within the criminal code of procedure. See T. Böckenförde, "Auf dem Weg zur elektronischen Privatsphäre", *Juristenzeitung,* 19/2008, pp. 932-933.

[134] Art. 588 bis (a) (2) LECRIM: "The principle of specificity requires that the electronic investigative measure is related to the investigation of a specific criminal offence. No electronic investigative measures shall be authorized which are aimed at preventing or discovering crimes or to confirm suspicions that do not have an objective basis."

general investigation or *inquisitio generalis* on the citizens.[135]. Such was the dictum of the Constitutional Court in its judgment 253/2006 of 11 September: investigative measures that restrict the right to privacy (in that case interception of communications) are valid only if authorized on the basis of precise objective indications of a crime and not mere subjective hypothesis or general suspicions.[136] Naturally, determining which is the required level of specificity is linked to the degree of suspicion that justifies granting a concrete measure.[137]

304. Mere suspicion, conjectures or guesses are not enough to grant the interception of communications but in practice it is not easy to differentiate between "reasonable suspicion" and "probable cause" in order to qualify the degree of suspicion[138]. The Spanish Supreme Court has repeatedly held that "the mere affirmation of the police about the existence of certain suspicions is not enough to order the interception of the communications".[139] And the Spanish Constitutional Court has stated that "the relationship between the person under investigation and the crime committed has to be supported by objective data: these data shall be susceptible to be assessed by third persons, and thus cannot be only based on subjective conclusions or a hunch; secondly, they have to be based on facts that allow to infer that a crime has been

[135] On the limits and safeguards of the criminal procedure to avoid it becoming a tool for carrying out an *inquisitio generalis* see M. Aguilera Morales, *Proceso penal y causa general,* Madrid 2008.

[136] In the same sense, STC 197/2009 o 219/2009.

[137] See *United States v. Hunter,* a search of computers that was considered disproportionate (*overbreath of the search and seizure*), because the warrant did not specify the computer to be searched neither the reasonable suspicion that justified the measure. The judgment is quoted by C. Rhoden, "Challenging Searches and Seizures of Computers at Home or in the Office: From reasonable Expectation of Privacy to Fruit of the Poisonous Tree Doctrine", *American Criminal Law Journal,* 30, 2002-2003, pp. 107-134, p. 115.

[138] The requirement of probable cause in the US Fourth Amendment is related to the likelihood of finding evidence. When applying for a search warrant, officers have to demonstrate probable cause that they will find evidence of a crime, and they must describe that evidence with particularity. Of course particularity links the probable cause to a specific crime, but the probable cause is directly referred to the evidence, not to the probability that a crime has been committed, as in the Spanish system. Although in theory "probable cause" entails a higher probability than mere "reasonable suspicion" and the latter is lower than "justified grounds", in practice tracing a difference between these different degrees on the probability of finding evidence is difficult.

[139] Spanish Supreme Court Decision of 18 June 1992, which is one of the landmark decisions defining the requirements for the interception of communications.

committed or will be committed, but they may not involve judgments about the person. These suspicions must be based on factual evidence or indications that suggest that someone attempts to commit, is committing or has committed a serious crime".[140]

305. In such a context, what shall the executing authority do when receiving an EIO requesting the interception of communications, but where the degree of suspicion is not clarified, or even it reflects that the request is based upon unclear intelligence information? Can the executing authority refuse the execution of such EIO on the grounds that it would not be allowed in a "similar domestic case"?

306. The answer is not clear. Nevertheless, following the principle of mutual recognition, the position to be supported is the one most favourable to the cooperation.

**74) Proposed best practice:** As a rule the executing authority shall not check the grounds that led to the issuing of the EIO by the issuing authority, nor compare the degree of suspicion required for a precise investigative measure in the issuing State and in the executing State. The rule is to trust the assessment made by the issuing authority on the legality, need and proportionality of the measure. Nevertheless, exceptionally, when the executing authority considers that there is a manifest lack of grounds for the issuing of an EIO or the reasons to issue it are not sufficiently described, it may refer to the issuing authority and ask for further clarifications.

### *c) Duration of the interception: which timeframe is to be applied?*

307. An EIO requesting the interception of telecommunications shall express the "desired duration of the interception" (Art. 30.2 DEIO). The expression "desired" has not been used by chance, as the executing authority is not bound

[140] STC 253/2006 of 11 September, quoting also judgments of the European Court of Human Rights, precisely ECtHR, *Klass and others v Germany*, App no 5029/71, 6 September 1978, and *Lüdi v Switzerland*, App no 12433/86, 15 June 1992. See also, T. Sánchez Núñez, "La jurisprudencia del Tribunal Constitucional sobre el uso de las nuevas tecnologías en la investigación penal", in *Los nuevos medios de investigación en el proceso penal. Especial referencia a la vídeovigilancia, CGPJ, Cuadernos de Derecho Judicial,* Madrid, 2007, pp. 251-299.

by the duration requested by the issuing authority The duration of the interception will need to comply with the timeframe established under the law of the issuing state, and also the ones of the executing state. The regulation of the maximum length for interception of telecommunications shows great variations among the EU MSs. While the maximum length of the interception order is one month in Belgium, the Netherlands or Sweden, it can be granted for up to three months in Germany and Spain, and for four months in France and the Czech Republic.[141]

308. As long as there is no legal harmonisation in this respect, it is clear that the only way to avoid clashes of the legal systems, when carrying out measures in the exercise of international cooperation and to prevent the infringement of executing state's own national rules, is to try to adapt the duration of the measure to the time requested, but always within the timeframes set out in the national laws.

309. Further to the necessary compliance with the *lex loci*, while trying to adapt to the *lex fori* in this regard, it is unclear if the executing authority can decide on the duration of the interception, applying national proportionality standards. For example, if the EIO expresses two months as the "desired" duration of the interception of telecommunications of the targeted subject, and this duration is within the timeframe established in the laws of the executing state, could the executing authority nevertheless establish a shorter duration, based on a proportionality assessment?

**75) Proposed best practice:** In establishing the duration of the interception of communications in the executing state, the executing authority should try to respect the principle of mutual recognition in so far as this does not collide with its own laws and constitutional principles. In that vein, as long as the "desired" duration expressed in the EIO is not contrary to the national provisions, the executing authority should not apply its own criteria to limit such duration.

[141] See the excellent 'Comparative analysis' by T. Tropina, in U. Sieber and N. von zur Mühlen (eds), *Access to Telecommunication Data in Criminal Justice*, Berlin, 2016, pp. 13–117.

### *d) How to decide on the extension of the duration of the interception?*

310. There is another point that shall be addressed in practice while executing an EIO. National laws allow for extending the duration of the interception of communications, beyond the initial maximum length.[142]

311. Regarding the prolongation of the initial authorisation contained in the EIO, most national laws subject such time extensions to a periodical assessment on the need of the measure, thus requiring that the judge checks the results obtained so far, and takes a decision whether the requisites of necessity and proportionality are still fulfilled. This periodical review for granting the prolongation of the measure should also be carried out when the interception of communications is executed in a foreign country by way of an EIO. To that end, the executing authority should transmit to the issuing authority the communications intercepted within the time periods set out by it – or immediately, if possible – and the issuing authority should decide on granting the extension or not. Such a prolongation should not exceed the maximum timeframe accepted in the national law of the executing state.

**76) Proposed best practice:** For taking the decision on the possible extension of the interception of communications, issuing and executing authority shall agree on the periodicity of the transfer of the results of the interception. Fluent communication between the issuing and executing authorities should be promoted for swiftly addressing these issues, as well as other possible incidents that may appear during the execution of the interception of telecommunications. The control by the issuing authority over the execution of the measure in order to decide over the possible prolongation would be clearly facilitated if there were an immediate transmission of the intercepted communications.

### *e) Interception of telecommunications without technical assistance*

312. Art. 31 DEIO regulates how to proceed in cases where the interception of the telecommunications in another MS does not require the technical

[142] See T. Tropina, op. cit., pp. 78–79.

assistance of such state. The main obligation for the "intercepting" state is to notify the relevant state affected by the interception measure.[143]

313. This provision is almost identical to Art. 20 EU MLA Convention, also establishing the obligation to notify the relevant state and the possibility of the latter to require the termination of such interception if it would not be allowed in a similar domestic case. Furthermore, the notified MS can also "where necessary" communicate to the "intercepting State" that the intercepted material cannot be used or that it can be used only under certain conditions (Art. 31.2 DEIO and Art. 20.4 EU MLA Convention).

314. As the EIO Directive replaces the EU MLA Convention of 2000 as of 22 May 2017 (Art. 34.1 (a) DEIO), it has taken over several of the provision contained in the MLA Convention. While the provisions of Art. 31.1 DEIO stem from a type of international cooperation governed by the principles of reciprocity, comity and international relations under public international law, it should be reconsidered if they have a different meaning in the context of the EU AFSJ and the principle of mutual recognition that governs the judicial cooperation in civil and criminal matters in the EU.

315. Yet Article 31 DEIO constitutes a provision not related to a request for assistance, as this is not needed for executing the investigative measure, and there is no need for an EIO. However, the notification is positive for the aim of keeping mutual trust among the MSs, for the respect to their sovereign powers, and for promoting the exchange of information among the MSs.[144]

316. That being said, it might be appropriate to address some questions

[143] The exact terms of Art. 31.1 DEIO read as follows:
"Where, for the purpose of carrying out an investigative measure, the interception of telecommunications is authorised by the competent authority of one MS (the 'intercepting MS') and the communication address of the subject of the interception specified in the interception order is being used on the territory of another MS (the 'notified MS') from which no technical assistance is needed to carry out the interception, the intercepting MS shall notify the competent authority of the notified MS of the interception.
Such notification shall be done either prior to the interception if the location of the subject is known, or during or after the interception when the authority issuing the interception order did not previously know of it."

[144] It is somewhat surprising that the extensive Explanatory memorandum does not make any reference to this provision.

regarding the interpretation and implementation of this provision.

### *f) Concept of sovereignty in the digital space*

317. Accessing the telecommunications of subjects located in another country – or data stored in another country – is an action that raises issues on sovereignty principles and international comity.[145] The fact that technology allows to access telecommunications regardless of territorial borders does not mean that it should be automatically considered lawful.

318. However, in the global digital world, it has become increasingly accepted that it is not feasible to apply territorial concepts to the cyberspace, and that physical boundaries and geographical frontiers are not relevant anymore in the virtual world. In this field, further discussions and studies are needed in order to consider how to overcome the traditional concepts on jurisdiction linked to the concept of territoriality and State sovereignty, which may no longer fit the globalised digital environment. Linking the issues of jurisdiction to the locality of the person whose communications are intercepted or to the place where the digital data are physically stored, does not seem to be a valid approach anymore.

319. For example, since telephone or internet communications can also be established – and also intercepted – while flying on an aircraft, would it be sensible to apply the traditional notions of territory to such interceptions, and oblige the requesting State to notify the State where the aircraft is registered or the States whose airspace is being overflown? The notions of physical location are even less important regarding electronic data stored in the cloud, where the intercepting authority might not even be aware where those servers are located.

320. Although it goes beyond the content of a Code of Best Practices, it is highly advisable to take some action in order to agree at the EU level on a common concept of sovereignty in this context, in order to facilitate a common approach on the remote access to telecommunications and e-data: there is a

[145] See J.L. Goldsmith, "The internet and the legitimacy of the remote cross-border searches", *University of Chicago Legal Forum,* 2001, pp. 103–18.

clear need to revise the concept of sovereignty in cyberspace and in the digital environment within the EU cross-border criminal investigations. This is why we dare here to make a recommendation that is not strictly based on a best practice.

**77) Recommendation:** EU should strive to agree on a common understanding of the concept of sovereignty in connection to the digital space in order to clarify and establish common principles and standards of protection when digital evidence is gathered without technical assistance of any other EU MS. This endeavour is crucial for ensuring the admissibility of evidence, and the EU would have legislative competence on this subject, according to Article 82.2 (a) TFEU.

### *g) Obligation of the "intercepting authority" to notify the affected MS: Who shall be notified?*

321. Article 31.1 (a) DEIO establishes the obligation to notify the relevant State prior to the interception of the telecommunications if the competent authority knows that "the subject of the interception is or will be on the territory of the notified MS." If the authority does not know beforehand where the subject is or will be the notification shall be made to the MS where he/she was at the moment of the interceptions, once this is known.

322. Several questions arise here. First, whom shall the competent authority notify of the fact of the interception? Some MS have identified a judicial authority that shall act as receiving authority of such notifications and shall also check the conformity of the measure with the principles/rules of the domestic legal framework. If such authority for notifications is not identified, it shall be assumed that the notification should be made to the central authority of the relevant MS(s). It is difficult to think of another recipient of such notification, especially in those cases where the person has no permanent domicile in that State, or is travelling across several EU countries.

**78) Proposed best practice:** As done in Spain, Italy or Germany, for notification purposes under Article 31.1 DEIO, a specific judicial authority should be

identified. This authority or authorities (in the case of Germany it is divided due to its federal structure), shall receive the incoming notification, register it for the aims of statistics, and communicate with the "intercepting authority" on the authorization or refusal to continue with the interception. In case such authority is not identified in a relevant MS, the notification should be sent to the central authority. Where several authorities are appointed as receiving authorities of the notification provided under 31.1 DEIO, those authorities shall establish a uniform interpretation and approach, so that the standards applied are consistent.

### *h) Whom to notify in case the subject of the interception is moving across several countries?*

323. The second question is whether the competent "intercepting" authority shall notify all MSs in which the subject has been located while his/her communications were intercepted. For comity reasons, mutual trust and swift information exchange, it goes without saying that this should be the best practice: notifications should be sent to each and every State where it turned out that the subject was located while his/her communications where intercepted. This will only be possible *ex post*, and usually not beforehand.

324. However, from the point of view of facilitating the circulation and admissibility of evidence it would be really complicated that the *forum* State would have to notify numerous countries where the subject was travelling through, in order to comply with Article 31.1. DEIO and face the risk that one of them denies the use of such communications as evidence. It seems that some kind of re-balancing approach would be reasonable. The actual practice regarding these notifications is diverse, because while some MSs regularly comply with the obligation to notify, others don't.[146]

**79) Proposed best practice:** "Intercepting" State shall always notify the States that have been affected by the interception measure, because the subject was

[146] Information obtained from Spanish practitioners.

located in its territory. If the subject is moving from one country to another, all of them should receive the notification.

***i) What shall be the stance of the "notified" authorities towards the interception measure?***

325. What is the role of the 'notified authority', taking into account that in these cases it is not the "executing authority"? Or should the "notified" authority be considered as "executing authority" as defined under Article 2 (d) DEIO in this context? Is the notification a mere formality or should the "notified State" check in every case the proportionality and lawfulness of the interception?

326. In use of this power, the notified State could, for example, ban the remote search of computers in its territory if such measure is not regulated in its national laws; it could also prohibit the use of the materials intercepted. If the measure is foreseen in the laws of the relevant State, in order to assess whether such measure could be adopted in a similar domestic case, the notified State shall check all the data related to the criminal investigation and see if any of the grounds for refusal would apply.

327. Once the notification is made in accordance with the procedure foreseen in the DEIO, it is for the notified State to decide whether it applies the prohibition of the investigative measure and/or the use of the materials obtained by way of the telecommunications interception.

328. In accordance with Article 31.3 DEIO, the "notified State" **may** prohibit the interception where the "interception would not be authorised in a similar domestic case". It is important to underline that the Directive has provided for the **possibility** of the notified State to prohibit the carrying out of such measure in its territory, and therefore the affected State could trigger an optional ground for refusing to accept such interception to take place in its territory. However, as with other grounds for refusal, the transposing laws –as in Spain and Italy– have regulated this optional ground as a mandatory ground for refusal, so that the "notified" authority shall prohibit the interception if it would not be allowed in a similar domestic case.

329. This means that in practice any interception of communications –with or without any technical assistance of the executing/notified State–, shall undergo the same requirements and necessity and proportionality test.

330. This seems to be coherent from the point of view of the executing/notified State –so that all investigative measures, regardless if they do or don't need any support of the relevant State– are subject to the same standards. This should allow keeping the same level of protection to all the subjects while they are physically located in the relevant territory.

331. However, such approach may not be so coherent if viewed from the point of view of establishing of a single AFSJ, where the mutual recognition and free circulation of evidence should be the principles to strive for. While in the execution of investigative measures that require the technical support of the executing State, obliging the executing authority to carry out measures that would violate their own legal framework does not seem to be acceptable, in the cases where the executing authority does not execute any measure the approach could be less stringent. In this case, it does not seem completely coherent to prohibit the execution of a measure by authorities who are not executing such measure, simply because the "intercepted subject" is moving to a different territory.

332. From the point of view of the subject whose communications are intercepted and then travels abroad, it is questionable if his/her reasonable expectation of privacy of those conversations is infringed if the interception can continue also once he/she has crossed the internal borders within the EU. In other words, it does not seem to be reasonable that the movement of the suspect is not subject to frontier controls, while the interception measure, which is available in the digital space without the need for any support from another MS, is limited to such territorial limits.

333. In order to protect the rights of the persons affected by an interception of communications, if it is legally foreseeable for them that the interception will continue even if they cross State borders within the EU, the measure should not be prohibited by any MS on the basis that it would not be allowed in a similar domestic case. The applicable law to the interception would not be dependent

of the physical location of the suspect, but to the laws of the forum where the person has become a suspect and is being investigated. Only if such measures would be considered as completely disproportionate from an objective point of view –and not only from the stand of the domestic law, there should be the possibility of refusing to continue the interception in the "notified" State and prohibit its use as evidence in the forum. However, this should be the exception, and not the rule.

334. Firstly if the use of the materials obtained through such interceptions is frequently prohibited, this can lead to the practice that MSs avoid complying with the requirement of notification, which, as stated earlier, would also run counter to mutual trust. Furthermore, the general obligation of the MSs to protect their citizens in their territory from encroachment of their rights through foreign interception of communications is hardly applicable anymore in the cyber-world.

**80) Proposed best practice:** Notified States should take a flexible approach towards the interceptions of telecommunications carried out in their territory without their technical support, when it affects a person who is travelling. They should not apply the possibilities provided under Article 31.3 DEIO in a strict way. This provision should not operate as a validity check of the interception according to the national standards applicable to the measure in a similar domestic case. A too strict approach might case the undesired effect that the intercepting authorities would skip the obligation to notify the affected State and use such evidence according their own standards on admissibility of evidence, and thus contribute to creating more distrust. In any event, the best approach should be to take action at the EU level on the concept of sovereignty in the digital space, as expressed above.

**81) Proposed best practice:** Until a common agreement on the rules applicable to the digital space are adopted, the case of the interception of communications carried out from abroad using remote interception devices to intercept the communications of physical or legal persons that are resident in a foreign country, should undergo the same standards as to the interceptions of

communications with technical assistance via EIO.

### *j) What should be the consequences for the admissibility of evidence in the forum/intercepting State if the 'notified State' prohibits the use of the intercepted communications?*

335. Would the "intercepting State" be bound by such a decision? Would such a decision render the evidence obtained in the foreign State inadmissible in the *forum* State? These are questions that will need to be faced by the courts in practice and again, certain uniform guidelines would help in implementing adequately this provision of the Directive. As for now, no practice has been identified in the studied countries, and defence lawyers as a rule do not question the admissibility of evidence obtained via international judicial cooperation. The principle of non-inquiry has been applied for long in these States, so that defence lawyers continue to accept that such is the principle that should continue to be applied.

336. In absence of more precise practice and/or case-law in the countries studied, in those cases where technical assistance is not needed for the interception of communications, and in conformity with the position stated above in favour of not trying to exercise territorial boundaries and old concepts of sovereignty in cyberspace–, the admissibility of such evidence is governed by the rules of the forum State.

337. This means that regardless of the position of the "notified State", if the measure was unlawful in the State of "execution", the admissibility of evidence could be questioned in the intercepting State for infringing the *lex loci*. This topic, however, is to be dealt with by each national court, which shall ensure that the principle set out under Article 14.7 DEIO is complied with.[147]

**82) Proposed best practice:** As long as there are no common EU rules on admissibility of evidence, the domestic procedural rules on evidence will apply, and as long as these rules are in conformity with the general principles set out

[147] Article 14.7 DEIO: "Without prejudice to national procedural rules Member States shall ensure that in criminal proceedings in the issuing State the rights of the defence and the fairness of the proceedings are respected when assessing evidence obtained through the EIO."

by the ECtHR, the MS enjoy a broad leeway. Compliance with *lex loci*, is not required as a pre-requisite for admissibility of cross-border evidence in every MS. Nevertheless, the best practice would be that the trial court in the forum State, in conformity with Article 14.7 DEIO, shall check if the infringement of the *lex loci* in the gathering of evidence would violate the procedural rights of the defendant.

***k) What should be the consequences for the* forum *State for infringing the prohibition to use the evidence gathered in another EU MS ex Article 31.3 b DEIO?***

338. What would be the consequences if the "intercepting State" would not comply with the prohibition to use the evidence gathered in the "notified" State?

339. If the "notified" State makes use of the possibility set out under Article 31.3 (b) DEIO and against the recommendation to use this power very sparsely, prohibits the use as evidence of the communications intercepted in its territory, the consequences would be: first, those as provided within the domestic legal framework of the forum, regarding the exclusion of evidence or the possible filing of a remedy for not complying *lex loci,* or nullity for infringing a legal provision. Further, it should be questioned if the EU should take action if such conduct is repeated and it turns out that there is a continuous violation of the obligations stemming out of the DEIO (ex Article 31.3 and ex Article 14.7 DEIO).

340. No best practice can be identified regarding this issue, but the following recommendation might be worth to be stated:

**83) Recommendation:** In order to promote the free circulation of evidence and to avoid that the diverse standards of admissibility of evidence end up in lowering the defence rights on the one hand, or represent an obstacle in the cooperation on the other hand, it would be advisable to advance in establishing common standards on admissibility of criminal evidence in cross-border criminal proceedings.

***l) What would be the consequences of infringing the obligation to notify the State where the subject of the interception was located?***

341. Would this lack of notification affect the validity of the evidence obtained through the 'non-notified' interception of telecommunications? This issue is closely related to the previous one. If admissibility of evidence is an issue to be counterbalanced in the forum/intercepting State, the absence of notification to the authorities in the "executing" State would not only affect the principle of international comity, but also imply a breach of complying with EU law, namely Article 31.1 DEIO. In addition, if in the forum/intercepting State, such notification is considered an essential element for the lawfulness of the measure and the admissibility of the evidence, in such case the defendant could move for the exclusion of such evidence. As stated earlier, the admissibility of evidence in cases of non-compliance with the obligation to notify the MS where it was obtained, will depend on the domestic rules in each MS. This situation might lead to a great diversity, and in this regard a common approach on admissibility of evidence would be desirable.

**84) Proposed best practice:** Each MS should ensure that the relevant judicial authorities comply with the obligation set out under Article 31.1 DEIO. Non-compliance with such an obligation should trigger consequences for infringement of EU law. Further, it would be advisable that the EU continues advancing in building up the AFSJ and makes use of the legislative process as provided under Article 82.2 (a) TFEU.

***m) Does the EIO cover cross-border surveillance and the tracking of objects?***

342. One of the rules not replaced by the DEIO is Article 40 CISA. Recital 9 of the DEIO states precisely that: "This Directive does not apply to cross-border surveillance as referred to in the Convention implementing the Schengen Agreement." The rules on this measure together with the hot pursuit (Article 41 CISA) have not been replaced[148], but only as long as they are police surveillance

[148] See Eurojust and the EJN, Joint Note of 2.5.2017, "Note on the meaning of corresponding provisions and the applicable legal regime in case of delayed transposition of the EIO Directive", Council doc. 9936/17.

measures. If the cross-border surveillance is ordered by a judicial authority within a criminal procedure, then such measure could be considered as an investigative measures aiming at gathering evidence, and thus would be covered by the DEIO, and the relevant authority would need to issue an EIO. The cross-border surveillance will be addressed again later. So far, we have mentioned this measure here for clarifying the meaning of "replaced corresponding rules": if it consists of police surveillance the CISA regulation it is not "replaced" by the EIO.

***n) The content of the notification ex Article 31 DEIO***

343. The 'intercepting State' shall notify the interception of the telecommunications – to be carried out or already executed – using the form set out in Annex C (Article 31.2 DEIO). The text provides expressly that the notification shall include all information necessary, including a description of the case, legal classification of the offence(s) and the applicable statutory provision/code, in order to enable the notified authority to assess, whether the interception would be authorised in a similar domestic case; and whether the material obtained can be used in legal proceedings (Annex C, para. V).

344. The information requested under the form of Annex C is very detailed, however, those data, as the form specifies, shall be provided "as far as they are known". The problem may arise when those data are not known, but are relevant for the "notified" State to decide if such an interception would be allowed in a similar domestic case. For example, if the date of birth of a physical person is not given, and the measure would not be allowed for a minor; or if the registered seat of a legal person is not indicated, but it would have its seat in the executing State, and the "notified" State applies diverse standards for domestic legal persons and others. In such cases, the notifying authority shall be consulted for completing the information, and if it is not possible to complete, the interpretation pro cooperation should be applied.

345. On the other hand, once the notification ex Article 31 DEIO has been received, under Annex C it is stated that: "any objection to the interception or the use of already intercepted material must be made no later than 96 hours

after the reception of this notification". It is curious that this provision is included in the Annex, because due to its impact it should have been included in the text of Article 31 DEIO. Therefore, it is unclear if not showing any objection within those 96 hours will amount to a tacit authorisation to continue the interception and use the evidence gathered; or rather it is only a formal timeframe but the objection could be filed also afterwards.

**85) Proposed best practice:** The lack of certain data to be specified in Annex C should not lead to the prohibition to continue the interception or to use the gathered elements as evidence. The notified authority shall consult the intercepting authority before taking any decision. In any event, the interpretation shall always be pro cooperation. The timeframe of 96 hours (4 days) shall preclude the possibility to exercise the objection under Article 31.2 DEIO.

### *o) Systems for transferring data of interception of communications*

346. Article 30.6 DEIO provides for a specific rule on the execution of the EIO issued for the interception of telecommunications. It precisely states:

"An EIO referred to in paragraph 1 may be executed by:

(a) transmitting telecommunications immediately to the issuing State; or

(b) intercepting, recording and subsequently transmitting the outcome of interception of telecommunications to the issuing State.

347. The issuing authority and the executing authority shall consult each other with a view to agreeing on whether the interception is carried out in accordance with point (a) or (b)."

348. This Article follows almost exactly, albeit with another wording, Article 18.1 of the EU MLA Convention of 2000, where the immediate transmission of the intercepted telecommunications and the recording and subsequent transmission are also foreseen as possible means of executing the request and transferring the results to the issuing authority. The Directive states expressly that both issuing and executing authorities must agree on how the execution of the interception of communications shall be carried out.

349. It may thus be expected that the direct access and immediate transmission of the intercepted telecommunications to the issuing authority will gain increasing importance in the AFSJ, although at present the direct data transfer obtained through the interception of communications is hardly used in practice.[149]

350. The present law and practice on the execution of requests on interception of telecommunications and the transfer of those data in the different MSs is quite diverse. In Belgium[150] and in Sweden,[151] for instance, the real-time transfer of communication data is not possible, while in Germany the real-time transfer of data is possible, both on the basis of an international Convention (such as Article 18 EU MLA Convention), as well as upon bilateral agreements.[152] In such cases, however, the German authorities must ensure that the German national rules are complied with and that they are respected by the requesting State. To that end, the German authorities, when acting as executing authorities, will subject the transfer of the real-time data to conditions, so that the privileges and immunities applicable under German law are safeguarded by the issuing authority directly accessing the communications data.

351. In Spain, there are no legal provisions on how the transfer of the information obtained through the interception of communications to the issuing authority is to be carried out, nor on the filtering of incoming data or of outgoing data.[153] In practice, the transfer takes place in different ways: when Spain is executing authority it may transfer the recorded communications as an

[149] See T. Tropina, p. 116.

[150] See G. Boulet, P. De Hert, "Access to Telecommunication Data in Criminal Justice: Belgium", *in* U. Sieber and N. von zur Mühlen (eds.), *Access to Telecommunication Data in Criminal Justice,* Berlin, 2016, pp. 123–246, 238–39.

[151] See I. Cameron, "Access to Telecommunication Data in Criminal Justice: Sweden", in U Sieber, N. von zur Mühlen (eds.), *Access to Telecommunication Data in Criminal Justice,* Berlin, 2016, pp. 611–44, 642–44.

[152] T. Wahl (with B. Vogel and P. Köppen) "Access to Telecommunication Data in Criminal Justice: Germany" in U. Sieber, N. von zur Mühlen (eds.), *Access to Telecommunication Data in Criminal Justice,* Berlin, 2016, pp. 499–610, 594–95.

[153] See L. Bachmaier Winter, "Access to Telecommunication Data in Criminal Justice: Spain", in U. Sieber, N. von zur Mühlen (eds.), *Access to Telecommunication Data in Criminal Justice* Berlin, 2016, pp. 647–704, 701–2.

attachment in e-communications; in case of being requesting State, it is not infrequent that a member of the judicial police, or even a member of the public prosecution, travels abroad to collect the disks with the recorded communications and bring them to the Spanish Investigating Judge. This is often done when the Spanish officers have already travelled to the relevant country for the purposes of the investigation, but there are also cases where the travel takes place only for bringing the disks with the intercepted communications. However, this is not the only practice. For example, when it comes to judicial cooperation with France, the transfer of data is often done through the *liaison* magistrates.

352. Members of the National Court report of cases where the data have been transferred through diplomatic personnel.[154] In investigations where several EU countries are involved and joint investigation teams have been set up, the disks sometimes are transferred through the heads of the respective joint investigation teams. In other cases, the disk is attached to the documents related to the request, and sent by ordinary channels. In sum, there is no uniform practice. But, as far as we know, at present neither the current legal framework nor the technical setting allows for the judge from another EU MS to have direct access to the data resulting from the telecommunications interception.

353. In view of these diverse systems and taking into account the different scope of privileges and immunities in the laws of each MS, it can be expected that the execution of the EIO, through an immediate transmission of the data, will not be generally implemented in the near future, although such a system of transmission could considerably improve the admissibility of the evidence.

354. The ways to grant direct access to the system for interception of communications could, once the EIO has been "recognised" in the executing State (following the check that there are no grounds for refusal), should be further explored and implemented. As the issuing authority would have direct access to the content data or the conversations that are being recorded, the

[154] This information has been obtained by interviewing several Investigating Judges of the National Court, but it refers mainly to evidence collected outside the EU.

control of the proportionality and necessity of the measure could also be done immediately according to national standards of the issuing State. Similarly, the decision on the prolongation or the suspension of the interception could also be adopted right away, and more importantly, the filtering of the communications would be done by the authorities of the forum State, respecting the immunities and privileges applicable to the criminal proceedings. Implementing this system will require the intercepting authority to agree to comply also with the *lex loci*, as such control would not be done by the authorities of the "executing" State.

355. Advancing in this direction should be one of the objectives of the EU MSs, as direct access would not only eliminate risks related to the admissibility of the evidence in the forum State, but would also allow implementing the principle of proportionality according to the national parameters. But most important, such direct access would also be beneficial to the right of defence of the defendants, who would be subject to the same legal provisions in cross-border interception of communications as in strictly domestic ones. There would be no need to be aware of the rules applicable in the executing State with regard to the filtering of data or the protection of immunities, or requirements for prolongation, as the law of the forum/the law of the issuing State would govern all these issues. The need for remedies for challenging the lawfulness of the measure in the executing State would not be necessary either, as in practice, except for the initial authorisation to connect to the interception system and the time-limits, once the EIO is recognised, the execution would be done in accordance to the national rules of the issuing State. In fact, once the EIO is recognised, the issuing State would become the 'intercepting State'.

356. Allowing the issuing authority to connect directly to the system of interception of telecommunications of the executing State, once the requirements of the EIO have been duly checked by the executing authority, would also increase the safeguards regarding the confidentiality of the information obtained. The executing State would, in principle, not have any knowledge of the content of the communications intercepted, but would only be responsible for the technical execution of the measure, and thus the risks of leaks of the intercepted data might also be reduced.

357. It goes without saying that such a system would clearly improve the cooperation in the gathering of evidence, and provide for swifter transmission of the results to the investigating authority in the issuing State. It would also be consistent with the principles of a single AFSJ, as the issuing authority would have access to the communications directly as if those communications had been intercepted in its own country.

358. However, the direct transmission will not only require a prior situation of mutual trust between the MSs, but also a certain harmonisation of the immunities and privileges in the issuing and executing States (precisely the lawyer–client privilege), or precise agreements setting out the conditions to be respected in the execution of such investigative measure.

359. As stated earlier, experience has shown that the direct transmission has hardly had any impact in practice. If things are to change in the execution of the EIOs, it is something that is difficult to affirm now. What is sure is that reaching the point where another EU MS obtains direct access to the telecommunications interception system in the executing country will require not only continuous efforts towards improving the mutual trust, but also the development of adequate software to be able to filter those communications that are not covered by the authorising order and/or are subject to a privileged protection. Moreover, this swifter cooperation will require specific agreements in each case, defining the scope of the interception in a clear way and the safeguards to be put in place for respecting both the *lex loci* and the *lex fori* / the laws of the issuing and executing States.

**86) Proposed best practice**: Even if the difficulties might appear to be insurmountable, both from technical and legal points of view, the ASFJ needs to advance towards the direct access to the interception of communications, developing the needed software and technical support, as well as by harmonising the regulation on immunities and privileges.

### *p) Specific analysis of the remote search of computers*

360. The use of spyware to access remotely to computers is a measure that is still highly controversial, due to its intrusiveness in the privacy of the

individuals.[155] Differently from the search of premises and the direct search of a computer, in the remote search of computers the suspect remains unaware of the access to his/her data[156]. The clandestine access obviously offers the law enforcement agents a very powerful tool to investigate the data stored in the computer, but at the same time, increases the encroachment upon the privacy.

361. Together with France and Italy, Spain also regulates the remote search of computers by way of using spyware as a criminal investigative measure. If the remote search of computers is done without the technical assistance of the State where the computer is located, the rules provided under Article 31 DEIO, which have already been analysed would apply. However, if the issuing authority requests via EIO the executing State to carry out such measure, Article 30 DEIO would apply. What has been already expressed with regard to these two forms of interception of telecommunications, would apply mutatis mutandis to the remote search of computers. At this point what will be analysed is the difficulty regarding the assessment of the proportionality of the measure.

***q) How shall the executing authority assess the principle of proportionality of the measure of the remote search of computers?***

362. 1) One of the main difficulties for judges when deciding on whether an investigative measure is to be authorized or not, is to determine if such measure is proportionate or not, if the sacrifice in the sphere of the fundamental rights is justified for prosecuting a crime. In case of very serious crimes, such assessment is much easier, provided that the degree of suspicion is sufficiently shown. It is accepted that in prosecuting transnational organized crime and terrorism, and even crimes against minors, the restriction of the suspect's privacy is generally legitimate, even by way of searching his/her computer with the help of forensic

[155] An interesting analysis on the rights affected through on-line searches, was carried out by the German Constitutional Court in its judgment of 27 February 2008, available under http://www.bundesverfassungsgericht.de,1 BvR 370/07,1 BvR 595/07. On this judgment see, among others T. Böckenförde, "Auf dem Weg zur elektronischen Privatsphäre", *Juristenzeitung,* 19/2008, pp. 925-939.

[156] See, for example, W. Abel, "Agents, Trojans and tags: The next generation of investigators", *International Rev. of Law Computers & Technology,* vol. 23, 2009, pp. 99-108, p. 103.

tools. However, the assessment on the proportionality of this investigative measure may represent a difficult challenge, when the law allows in general carrying out a search of a computer in the investigation of criminal offences committed through computer technology. In these cases the damage infringed to society might not be so evident, the penalty may remain low and therefore the seriousness of the offence is not a sufficient ground to justify the sacrifice of the fundamental right to privacy. But in domestic criminal procedure codes, like the Spanish CPC, the legislator opened the possibility to authorize a measure like the "hacking" of a computer by the police for prosecuting crimes that are not even considered as grave crimes. This is explained in the Budapest Convention: if these IT investigative measures are not provided, most of the crimes committed through computer technology will remain undetected. In order to avoid that the Internet becomes an "outlaw place", citizens will have to take into account that their privacy in the digital environment might be encroached, even for investigating minor crimes. The perils the global citizen is facing might render such approach reasonable, but it is not without controversy.

363. As there is no common regulation on the remote search of computers among the EU MS, it remains questionable when such measure will be allowed for investigating "offences committed through computer systems". In these cases, the seriousness of the crime and the penalty threshold should not be decisive for assessing the proportionality, but also the need for the deterrence effect of enforcing the criminal law, and the damage that such behaviours are causing to society or to the relevant individual. However, as long as each of the MS apply their own criteria for determining the proportionality of this measure, it may occur that the EIO dealing with the remote search of computers will be refused. This poses a huge challenge for the prosecution of cybercrime at the national level, as most of these cases entail the need to carry out investigations in the digital space, and thus affecting other MSs. If such investigations are hindered by the diverse concept of proportionality in each of the countries where the computer to be searched is located or the data to be accessed are stored, regardless the fact that the data or bots being used for the criminal offences are located elsewhere, cybercrime may at the end become an area of

impunity. Establishing a link with the territory where the computer or the subject using it is located might not be reasonable for fighting crime that is committed out of that territory, namely in the digital space, and has consequences in numerous places. As well as the jurisdiction to prosecute such crimes is not determined by the place where the data or the computer are physically located, the authorisation to use the evidence gathered by way of an interception without technical assistance of a relevant country, shall not determine the effective prosecution of such offences.

**87) Proposed best practice:** The regulation of the remote search of computers requires a common approach at the EU level in order to prevent that diverse requirements and criteria for assessing the proportionality of this measure, end up making the investigations in the digital space subject to a cumbersome fragmentation, not justified by technical issues but by a somewhat artificial territorial concept of the cyberspace. As long as this common rules are not implemented, MSs should make use of Article 31.3 DEIO very sparsely, and prohibit the use of evidence gathered without technical support only in very exceptional cases.

### 15.3. Exchange of information on bank accounts and banking and other financial operations

364. The issuing of an EIO in order to obtain information concerning bank accounts or other financial accounts, banking or other financial operations or for the monitoring of banking or other financial operations is regulated in Chapter IV, entitled "Specific provisions for certain investigative measures", and specifically in articles 26, 27 and 28(1)(a) of the DEIO.

365. As regards the implementation of the DEIO, it should firstly be noted that only few MSs provide for specific rules and investigative measures in order to obtain bank data; as a result, there is not a uniform procedure to obtain them, but as many different procedures as there are MSs. The countries studied have implemented these provisions into their domestic legal framework following the wording of the Directive.

366. In Italy two provisions of the Criminal Procedure Code, specifically Article 255 and 256 CPC, apply in case of gathering of information and documents in banks and other financial institutions. Furthermore a specific provision applies for the gathering of evidence in banks within the special proceedings for the application of a preventive measure[157]. In this case, the investigations on assets may be carried out directly by those bodies who have the power to request it or by the Italian Finance Police (i.e. *Guardia di Finanza*) if there is delegation. The investigating police authority delegated by the Public Prosecutor has the power to seize documentation only if authorised by the Public Prosecutor or the judge[158].

367. However, in general, Articles 255 and 256 CPC apply. According to the first article, it is possible to seize not only the documents, amount of money and securities deposited in current accounts held by the suspect or accused person, but also those held by persons other than the suspected or accused person if there are justifiable grounds to believe that they relate to the offence. As it has been highlighted in the national report, according to case law, in such case "it is not necessary to serve the notice relevant to the right to defence (Article 369 bis of the CPC) to persons who hold the seized document".[159] Article 256 CPC, on the other hand, regulates the case when these documents are held by a person subject to professional or public service secret.

368. In this regard, it is provided that they shall immediately deliver the documents and the documentary evidence to the requesting judicial authority, as well as data, information and software, and anything else they possess by virtue of their function, job, service, profession or art. They are exempted from doing so if they declare in writing that this information is covered by State, public service, or professional secret. In the last two cases, nevertheless, the judicial authority has the power to assess the legitimacy of the statement if it has well-founded reasons to doubt about it and it believes that it can not proceed without the gathering of these documents, documentary evidence or

[157] In this regard, article 19 of the Anti-Mafia code applies.
[158] See in this sense articles 253, 254 and 255 of the CPC.
[159] Cass. I, 7 July 1992, n. 3272.

objects. In case that it found the statement not justified, the judicial authority could consequently order its seizure. On the contrary, in case of State secrecy, if the evidence is essential to decide the case, the Court shall issue a judgment of non-prosecution due to the existence of the State secret.

369. As regards, the gathering of electronic flow in real time from or towards banks and financial institutions, the provisions concerning the interception of communications apply, i.e. article 266 and ff. CPC. In particular, the gathering of electronic flow of data is executed by the Public Prosecutor, upon request, if it is necessary, to the judge for preliminary investigations. In this case, thus, the Italian judicial authority shall verify whether there are specific conditions on admissibility, provided at the national level, for the interception of communications.

370. Furthermore, Article 20 of the Legislative Decree 108 of 2017 provides that, when the EIO does not specify the reasons why the acts are relevant in the criminal proceeding, the Public Prosecutor, before executing it, shall consult with the issuing authority to provide additional information needed for the quick and effective execution of the requested measure[160].

371. In Spain, articles 26 and 27 DEIO are respectively implemented by articles 198 and 199 of the law 3/2018, of 11th June, modifying law 23/2014 of 20th November, implementing the DEIO, which reproduce in both cases faithfully the text of the Directive. Article 28 DEIO, as far as the monitoring of bank transactions are concerned, is implemented by article 200 of law 3/2018. This Article states that the Spanish competent issuing authority should in these cases clearly indicate the reasons why it considers the information requested relevant (in Spanish, literally, “pertinente”) for the purpose of the criminal proceedings concerned.

372. Articles 217, 218 and 219 of the same law 3/2018 concern, on the other hand, the applicable regime to recognition and execution of the EIO concerning the exchange of bank information.

[160] Article 20, par. 3 of Legislative Decree n. 108 of 21 June 2017, “Norme di attuazione della direttiva 2014/41/UE del Parlamento europeo e del Consiglio, del 3 aprile 2014, relativa all'ordine europeo di indagine penale”.

373. Articles 217 and 218 of law 3/2018, dealing with request for bank information specify that, the Spanish relevant authorities may refute the execution of the EIO also in the cases where the investigative measure concerned would not be authorised in a similar domestic case. In this sense, the Spanish law has extended this ground for refusal to any request for bank information and not for the single cases provided in the DEIO (Articles 26.6, 27.5 and 28 DEIO), although this has not caused any practical problems.

374. Article 217 of Law 3/2018 provides also for the confidentiality of the investigations. In this sense, implementing article 19 of the DEIO, it provides that the Spanish competent authority shall take the necessary measures to ensure that banks do not disclose to the bank customer concerned or to other third persons that information has been transmitted to the issuing State in accordance with Article 26 or 27 or that an investigation has been carried out. The same provision nevertheless provides that the Spanish authority may use for this purpose the information existing in the "Financial title File"[161], provided that investigations of money laundering crime or financing terrorism are concerned.

***a) Whose bank information can be requested under Article 26 DEIO?***

375. The Explanatory Memorandum[162] says that the basis of the provisions included in Chapter IV concerning the exchange of information on bank accounts and banking operations are articles 1 to 3 of the 2001 EU MLA Protocol.[163] It defines that "accounts that are controlled *by* the person under

[161] Created by Order ECC/2503/2014, of 29 December, BOE n. 316, 31.12.2014, p. 107641 ff. ("Orden ECC/2503/2014, de 29 de diciembre, por la que se crea el fichero de datos de carácter personal denominado «Fichero de Titularidades Financieras»"), available at https://www.boe.es/buscar/doc.php?id=BOE-A-2014-13713.

[162] Council Document, Initiative of the Kingdom of Belgium, the Republic of Bulgaria, the Republic of Estonia, the Kingdom of Spain, the Republic of Austria, the Republic of Slovenia and the Kingdom of Sweden for a Directive of the European Parliament and of the Council regarding the European Investigation Order in criminal matters - Explanatory Memorandum, 9288/10 ADD 1, 3 June 2010, p. 17.

[163] In particular, article 26.1 DEIO, where an EIO is issued to determine "whether any natural or legal person subject to the criminal proceedings concerned holds or controls one or more accounts, of whatever nature, in any bank located in the territory of the executing State, and if so, to obtain all the details of the identified accounts" is based on article 1 of the 2001

investigation include accounts of which that person is the beneficial owner and this applies irrespective of whether those accounts are held by a natural person, a legal person or a body acting in the form of, or on behalf of, trust funds or other instruments for administering special purpose funds, the identity of the settlers or beneficiaries of which is unknown".[164]This measure covers "not only suspected or accused persons but also any other person in respect of whom such information is found necessary by the competent authorities in the course of criminal proceedings".[165]

376. Furthermore, Article 26.3 specifies that the information requested can also include accounts for which the person subject to the criminal proceedings concerned has power of attorney.[166] The fact that this clarification is made means that the executing authority is in fact not automatically bound to verify these accounts if not explicitly requested.

377. The identification of the subjects is not easy as there is the lack of company registers "allowing for the identification of hidden beneficiaries of opaque structures, benefiting from anonymity".[167] The difficulty in identifying the beneficial owner of complex legal persons is mainly due to the lack of transparency of information relating to legal ownership. In this respect the adoption of the fourth and fifth EU Anti-money laundering Directives, which provide for the establishment of European public registries of legal structures

---

MLA Protocol.

[164] See Explanatory Memorandum, p. 24 where we read also that "the concept of beneficial owner is defined in Article 3.6 of Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (OJ L 309, 25 November 2005, p. 15)".

[165] Recital 27.

[166] Article 26 (3) DEIO.

[167] See M. Simonato, M. Lassalle, "A fragmented approach to asset recovery and financial investigations: a threat to effective international cooperation?", *in* Z. Durdevic, E. Ivicevic Karas, (eds.), *European Criminal Procedure Law in Service of Protection of European Union Financial Interests: State of Play and Challenges*, 2016, p. 148; E. van der Does de Willebois et al., "The Puppet Masters: How the Corrupt Use Legal Structures to Hide Stolen Assets and What to Do About It", World Bank, 2011, p. 17 et seq.; M.G. Findley, D.L. Nielson, J.C. Sharman, "Global Shell Games: Experiments in Transnational Relations, Crime, and Terrorism", Cambridge, 2014, p. 29 ff.; M.E. Schulz, "Beneficial ownership: The private sector perspective", *in* G. Fenner Zinkernagel, C. Monteith, P. Gomes Pereira, *Emerging Trends in Asset Recovery*, Bern, 2013, p. 75 ff.

such as trust and companies[168] has been of great importance.

378. Finally, the last paragraph of article 26 provides that an EIO could be issued also to determine whether any natural or legal person subject to the criminal proceedings concerned holds one or more accounts in any non-bank financial institution located on the territory of the executing State. In this case, however, it is explicitly stated that, in addition to the grounds for non-recognition and non-execution referred to in Article 11, the execution of the EIO may also be refused if the execution of the investigative measure would not be authorised in a similar domestic case.

**88) Proposed best practice:** The information whether a person "holds or controls one or more accounts" is to be defined in the broad sense as expressed in the EU MLA Convention, Recital 27 DEIO, and Article 26.3 DEIO. It should be ensured that the practice in all MSs regarding the definition of legal or physical person who "holds or controls" an account is applied uniformly. Following Article 26.6 DEIO, and regardless how this measure is labelled in the domestic legal framework, the execution of this measure related to non-bank financial institutions, could also be refused if it were not available in a similar domestic case. However, not being a coercive measure, this ground for refusal should be applied in a restrictive way.

### *b) Article 27 DEIO: What information can be requested? The impact of this provision upon the subjects whose accounts can be investigated*

379. Article 27 DEIO regulates the possibility of issuing an EIO "in order to obtain the details of specified bank accounts and of banking operations which have been carried out during a defined period through one or more accounts specified therein, including the details of any sending or recipient account".[169] The term "details" should be understood to include at least the name and

[168] See article 30 of the fourth money laundering Directive and article of the fifth money laundering Directive.

[169] Article 27.1 DEIO.

address of the account holder, details of any powers of attorney held over the account, and any other details or documents provided by the account holder when the account was opened and that are still held by the bank".[170]

380. While article 26 provides for the possibility to issue an EIO to find out whether a person owns/controls, directly or indirectly, any bank account without any further inquiry into the transactions conducted by the account's holder, Article 27 provides for the possibility to discover what transactions the account holder has conducted during a specific period of time.

381. In the first paragraph of Article 27 there is no reference to the fact that the accounts in regard of which an EIO is issued should be linked with a criminal proceedings. An indirect reference to it is mentioned only in paragraph 4 of the same article, where it is explicitly stated that in the EIO "the issuing authority shall indicate the reasons why it considers the requested information relevant for the purpose of the criminal proceedings concerned".[171] From a combined reading of these two paragraphs and the explanatory memorandum,[172] it is thus clear that the EIO may also cover accounts held by third persons who are not themselves subject to any criminal proceedings but whose accounts are linked to a criminal investigation.[173]

382. Furthermore, the fact that the Article specifies that the information to be transmitted in the execution of such EIO includes also "the details of any sending or recipient account" means that the executing authority could be requested not only to provide information as regards the amount of money sent to/from the account or from/to another account on a certain date, but also to provide the requesting authority with information relating to the recipient/sending account, so that the issuing authority may trace the movements of money from account to account and, if necessary, proceed with

[170] Recital 29 DEIO.

[171] Article 27.4 DEIO.

[172] Explanatory Memorandum, p. 26.

[173] See the Explanatory Memorandum: "A practical example is the situation where the bank account of an innocent, and totally unaware, person is used as a 'means of transport' between two accounts, which are held by the suspect, in order to confuse and hide the transaction. Article 24 (now 27) allows the issuing authority to get information on any transactions to or from such an account".

an EIO in respect of the other account.

383. Article 27.3, similarly to article 26.3 specifies that each MS shall take the measures necessary to enable it to provide the information referred to in the first paragraph and that the obligation set out in IT "shall apply only to the extent that the information is in the possession of the bank in which the account is held".[174] The remarks made with reference to Article 26 are therefore also valid in respect of article 27.

384. Similarly to the last paragraph of Article 26, Article 27.5 DEIO states that an EIO may be issued in respect of the information concerning the financial operations conducted by non-banking financial institutions. The definition of financial institutions is given in recital 28: the term "financial institutions" should be understood "according to the relevant definition of Article 3 of Directive 2005/60/EC of the European Parliament and the Council". [175] Considering that that Directive has been replaced by Directive 2015/849, the term "financial institution" should thus be given the meaning referred to in Article 3 of Directive 2015/849.[176] The same additional ground for refusal applies in case of Article 27, as in respect of Article 26, and the same proposed best practice would apply here.

**89) Proposed best practice:** It follows from Article 27 paragraph 1 in conjunction with Article 27.4 DEIO and the Explanatory Memorandum that the EIO may also cover accounts held by third persons who are not themselves subject to any criminal proceedings, but whose accounts are linked to a criminal investigation. The issuing authority shall refer to the facts that allow to establish such a link in order to protect the rights of third persons that are not related to the criminal acts investigated, and that are unaware of the use that is being

[174] Article 27(3) of the DEIO.

[175] Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, OJ L 309, 25.11.2005, p. 15.

[176] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, OJ L 141, 5.6.2015, p. 73-117.

made of their bank accounts.

### c) *Execution of the EIOs related to bank accounts information: relationship with the Proposal for a Directive of 17 April 2018*

385. As far as the execution of the EIO is concerned, article 26 does not require the MSs to set up a centralised register of bank account holders, leaving to each MS the decision on how to comply in an effective way with article 26. Besides, the latter specifies only that the executing authority is obliged to give to the issuing authority all the details of the identified accounts only as far as the information is in the possession of the bank keeping the account.[177] "The result is that in many countries access to information on bank account holders is limited to judicial authorities, which need to officially request the information from every bank in their territory, without the possibility of consulting a single database including all the available information collected from all the banks in that territory".[178]

386. In this regard, the Proposal for a Directive of 17 April 2018 is set to play an important role in providing the competent authorities, including tax authorities, Asset Recovery Offices and anti-corruption authorities when carrying out criminal investigations under national law with direct access to the national centralised bank account registries or data retrieval systems.[179] The proposed Directive, based on Article 87(2) TFEU, is in fact aimed at facilitating the use of financial information to prevent, detect, investigate or prosecute serious crime and to improve access to information by Financial Intelligence Units and public authorities responsible for the prevention, detection, investigation or prosecution of serious forms of crime, to enhance their ability to conduct financial investigations and to improve cooperation between them.

[177] Article 26.4 DEIO.

[178] M. Simonato, M. Lassalle, "A fragmented approach to asset recovery and financial investigations: a threat to effective international cooperation?", in Z. Durdevic, E. Ivicevic Karas, (eds.), *European Criminal Procedure Law in Service of Protection of European Union Financial Interests: State of Play and Challenges*, op. cit., p. 148.

[179] Proposal for a Directive of the European Parliament and of the Council laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences and repealing Council Decision 2000/642/JHA, Strasbourg, 17.4.2018, COM(2018) 213 final.

387. Thus, the proposed directive, in order to reduce the recourse by competent authorities to blanket requests sent to all financial institutions in a certain MS, gives to the competent authorities direct access to the information of bank account holders held in centralised bank account registries or data retrieval systems. The latter, currently operational in 15 MSs, are in fact accessible by specific competent authorities in only 6 of them.

388. As regards the relationship with the DEIO, recital 11 of the proposed Directive provides, in particular, that "[t]he information acquired by competent authorities from the national centralised bank account registries can be exchanged with competent authorities located in a different MS, in accordance with Council Framework Decision 2006/960/JHA and Directive 2014/41/EU of the European Parliament and the Council".

389. The scope of the proposed Directive is therefore to give the competent authorities access to the information included in the national centralised account registries, but not to regulate the exchange of this information between the MSs. To that end, the DEIO still remains the essential instrument. However, the connection between the two Directives is evident, because the possibility granted to the executing authorities to have direct access to the national centralised bank account registries or data retrieval system will undoubtedly facilitate the gathering of information requested by way of an EIO and enable the executing authority to send the issuing authority the information referred to in articles 26 and 27 DEIO in a more accurate and swifter way. The proposed Directive is, thus, complementary to articles 26, 27 and 28 DEIO.

**90) Proposed best practice:** The adoption and implementation of the Proposal for a Directive of 17 April 2018 will enable a swifter and more effective execution of the EIOs. From the point of view of the cross-border gathering of evidence in criminal proceedings, its adoption should be seen as very positive. It would reduce timeframes and costs in the execution of EIOs related to the financial information covered by it.

### *d) Monitoring of banking or other financial operations that are being carried out through one or more specified accounts*

390. While Article 26 and 27 DEIO concern the acquisition of information on previous activities which should be already in the bank's possession, Article 28 concerns with the monitoring of banking or other financial operations in real time, continuously and over a certain period of time. It therefore implies a higher level of intrusion upon fundamental rights and requires more active cooperation with banks.[180]

391. This provision is very similar to Article 3 of the 2001 Protocol to the MLA Convention. However, Article 28 DEIO represent an improvement as regards the effectiveness of the cooperation between national authorities in comparison to the previous provision: Article 3 of the 2001 Protocol to the MLA Convention only obliged MSs to set up mechanisms which make them able to monitor the banking operations carried out through one or more accounts specified in the request, but MSs were free to decide whether and under which conditions to give the assistance in a specific case, "with due regard for the national law of that MS".[181] The MSs were therefore left with a wide margin of manoeuvre, which hampered the effective cooperation between them.[182]

**91) Proposed best practice:** As with other investigative measures that are very intrusive in the fundamental rights of the persons affected by them, the issuing authority shall specify very clearly what are the accounts to be monitored and give specific grounds when the holder of the account is a person not linked to the criminal acts and the criminal investigation. As at present bank information can provide a vast amount of information affecting the privacy of the users (not only financial aspects, but others as e.g. what has been purchased, at what time, where, etc.), the issuing authority shall scrutinize thoroughly the requirements

[180] And this explains why the EIO can also be refused "if the execution of the investigative measure concerned would not be authorised in a similar domestic case" (Article 28.1 DEIO).

[181] Article 3.3 of the 2001 Protocol of the MLA Convention.

[182] See in this regard, M. Simonato, M. Lassalle, "A fragmented approach to asset recovery and financial investigations: a threat to effective international cooperation?", in Z. Durdevic, E. Ivicevic Karas, (eds.), *European Criminal Procedure Law in Service of Protection of European Union Financial Interests: State of Play and Challenges*, op. cit., p. 145 ff.

of proportionality and necessity of the measure. The development of common criteria/thresholds for authorizing this investigative measure within the EU would be very positive.

### *e) Grounds for refusal of the EIOs regarding to bank information. Which rules apply?*

392. Does the fact that the legal framework concerning the exchange of information on bank accounts and banking operations is regulated in a specific Chapter with specific provisions imply that a different legal regime applies in respect of the exchange of bank information? More precisely do the rules referred to in Articles 10 and 11 DEIO, which regulate the recourse to a different type of investigative measure and set forth the grounds for non-recognition or non-execution of an EIO, apply to the measures regulated in Articles 26, 27 and 28 DEIO?

393. The issue might be important in practice considering that among the most requested activities in the field of judicial cooperation in criminal matters in the countries object of this study there is the request of information on bank accounts.[183]

394. The most plausible interpretation seems to be that articles 26, 27 and 28 are to be considered *lex specialis*; they therefore prevail over the general provisions of the directive, which have to be considered *lex generalis* (and the maxim *lex specialis derogat generali* applies). However, it should be highlighted that, even if this interpretation is accepted, the general regime would apply in the cases not specifically regulated by the special provisions.

395. This means that Article 10.1 (5) of the DEIO –which provides that the executing authority is to notify the issuing authority that it has not been possible to provide the assistance requested if the measure indicated in the EIO does not exist under the law of the executing State or it would not be available in a similar domestic case and where there is no other investigative measure which would have the same result as the investigative measure requested–,

[183] See p. 12 of the report on the evaluation of the practice in Italy and p. 20 of the Spain's report on the evaluation of the practice in this Country.

does not apply in respect of articles 26 and 27 DEIO.

396. The latter, in fact, specifically provides that each MS "shall take the measures necessary to enable it to provide the information referred to in paragraph 1 in accordance with the conditions" under those provisions. Each MS would, in fact, be obliged to ensure that the measures necessary to provide the information specified in paragraphs 1 of Articles 26 and 27 of the DEIO are available.[184] However some MSs –not the ones object of this study– do not provide for a specific measure to obtain information on bank accounts, banking and financial operations, but resort to the general provisions on search an seizure of documentary evidence or interception of telecommunications (for the monitoring of bank accounts).[185] Could these countries refuse the execution of measures requesting bank information because such measure would not be provided in a similar domestic case?

397. Applying the criterion according to which *lex specialis derogat generali*, it seems that the answer should be in the negative. In articles 26 and 27 DEIO it is, in fact, specifically provided that the each MS "shall" take the necessary measures to enable the gathering of the information on bank accounts and on the details of banking and financial operations. It seems therefore that the MSs cannot refuse to execute the EIO only because the punishment by which the given offence in the EIO is punishable does not reach the threshold provided for under its national law.[186]

398. However, a different reasoning and different legal regime applies with

[184] In similar terms, M. Panzavolta, "Ordine di indagine europeo e indagini bancarie: spunti di riflessione sul concetto di caso interno analogo e atto di indagine alternativo", *in* A. Di Pietro, M. Caianiello (eds.), *Indagini penali e amministrative in materia di frodi IVA e di imposte doganali. L'impatto dell'European Investigation Order sulla cooperazione transnazionale*, Bari, 2016, p. 379.

[185] In practice several EIOs received in Spain requested to carry out an entry of the bank and the search and seizure for obtaining bank information. In those cases the Spanish executing authority has applied Article 10.3 DEIO, and has substituted the requested measure by a less intrusive one: the order requesting those bank data, which the banks are obliged to produce. But Article 10.5 DEIO would not be applicable to refuse to provide bank information.

[186] This is interpretation is proposed also by M. Panzavolta, "Ordine di indagine europeo e indagini bancarie: spunti di riflessione sul concetto di caso interno analogo e atto di indagine alternativo", *in* A. Di Pietro, M. Caianiello (eds.), *Indagini penali e amministrative in materia di frodi IVA e di imposte doganali. L'impatto dell'European Investigation Order sulla cooperazione transnazionale*, op. cit., p. 378.

regard to Article 28.1(a) DEIO concerning the monitoring in real time, continuously and over a certain period of time of banking or other financial operations. In this case there is no specific provision obliging the MSs to adopt the necessary measures to enable the monitoring of banking and other financial operations.

399. This obviously does not mean that the MSs shall not adopt the measures necessary to implement this provision, but it means that no special regime applies in this regard; thus, all the grounds for non-recognition and non-execution apply, as well as article 10 DEIO, and specifically paragraphs 1 and 5, of the DEIO.

400. Furthermore, as specified in the same first paragraph of article 28, in addition to the grounds for non-recognition and non-execution referred to in article 11, the execution of the EIO may be refused "if the execution of the investigative measure concerned would not be authorised in a similar domestic case". The different regulation on this investigative measures at the domestic level creates many obstacles in practice. In this regard, it should be noted that in Italy, for instance, the legal framework applicable to the monitoring of bank transactions is the same as the one applicable to the interception of communications. There are no specific provisions regulating it and thus all the conditions regulating the interception of communications, which are rather stringent, apply.

401. These conditions could be stricter than those provided for in another MS and therefore the execution of the EIO could be refused on this ground. As far as the additional ground for refusal mentioned in Article 28.1 DEIO is concerned, it is also important to determine the relationship between this provision and the rules provided for in article 10 DEIO. Article 28.1 is a special provision with regard to Article 10.5 DEIO and therefore in case that the investigative measure were not authorised in a similar domestic case, the executing authority could directly refuse the execution of the EIO, instead of resorting to another investigative measure.[187]

[187] See in similar terms, M. Panzavolta, "Ordine di indagine europeo e indagini bancarie: spunti di riflessione sul concetto di caso interno analogo e atto di indagine

**92) Proposed best practice: a) Relationship between art. 26 (2), 27 (2) and 10 (1)(5) DEIO:** If the information requested via the EIO concerns a bank, the ground for non-execution referred to in article 10.1 (5) of the EIO does not apply. MSs shall comply with articles 26.2 and 27.2 DEIO. There is no possibility to refuse the measure because it does not exist or would not be available to a similar domestic case. This is specially important in those cases where the executing State executes these requests for bank information under the rules of search and seizure and/or interception of communications. The request for bank data cannot be refused because the search and seizure or the interception of communications is limited to offences with a minimum threshold of penalty. **b) Relationship between articles 26, 27, 28 DEIO and article 11 DEIO:** The general grounds for refusal under article 11 DEIO apply also in respect of articles 26 and 27 DEIO.

### *f) What reasons are to be justified for the issuing of an EIO related to bank information?*

402. All the three provisions concerning the obtaining of information on bank accounts and banking and financial operations as well as the monitoring of banking and financial operations (Articles 26, 27 and 28 DEIO), establish that the issuing authority must indicate the reasons justifying its EIO's request. The wording of the three provisions concerned is slightly different: Article 26.5 DEIO provides that the issuing authority "shall indicate the reasons why it considers that the requested information **is likely to be of substantial value** for the purpose of the criminal proceedings concerned", while Article 27.4 and 28.3 DEIO refer to the reasons why the issuing authority **considers the information requested relevant** for the purpose of the criminal proceedings"

403. The expressions "of substantial value" or "relevant" for the purpose of the criminal proceedings are not easy to define and can in fact be subject to a

alternativo", *in* A. Di Pietro, M. Caianiello (eds.), *Indagini penali e amministrative in materia di frodi IVA e di imposte doganali. L'impatto dell'European Investigation Order sulla cooperazione transnazionale*, op. cit., p. 379.

very broad interpretation, including many diverse types of information. In this regard, the Explanatory Memorandum specifies that "this paragraph implies that the issuing authority may not use this measure as a mean to "fish" information from just any – or all – MSs but that it must direct the EIO to a MS which is likely to be able to provide the requested information". The objective to avoid fishing requests is more than legitimate, however the absence of a common understanding on what shall be the level of detail given as reasons justifying the EIO, can cause a diverse approach by the different executing authorities, as has been seen already in the execution of MLA requests. While it might not be possible to define more precisely what shall be considered as "valuable" or "relevant" for the purpose of the criminal investigation, it is certain that the executing State, by being too strict, could hinder the smooth cooperation.

404. In addition, under Article 26 DEIO the issuing authority shall also explain the "on what grounds it presumes that banks in the executing State hold the account and, to the extent available, which banks may be involved".[188] How should the requesting authority explain that there are grounds to presume the existence of a certain bank account of a person?

405. There are multiple and very different reasons which can justify a presumption, but the same explanations can be deemed sufficient for one MS and insufficient for another State. In some cases, the issuing authority might be able to provide properly founded elements or even evidence supporting the request, while in other cases a mere suspicion could be enough to request the data under Article 26 DEIO. This diverse practice is known for long within the MLA judicial cooperation system, and at the end it is for the executing authority to assess whether the request is duly justified or not. There are no clear parameters to determine in advance which requests will be refused due to a lack of sufficient justification and which ones would, on the contrary, will be accepted as duly justified.

406. For obtaining the information under Article 26 DEIO elements that

[188]Article 26.5 DEIO. In the same provision it is stated that the issuing authority "shall also include in the EIO any information available which may facilitate its execution".

would justify the presumption are enough for issuing and executing the EIO for determining if a person holds an account in a certain MS. Excluding completely the adoption of this measure for prospective investigations is not possible, but on the other hand, not being a measure that is intrusive in the fundamental rights of the person concerned, a flexible approach that enables the execution is to be promoted.

**93) Proposed best practice:** While it is impossible to define in abstract what level of detail shall have the reasons given by the issuing authority on the value or relevance of the information requested for the purposes of the criminal investigation concerned, the issuing authority shall establish at least what are the links between the evidence/information requested and the aims of the criminal investigation, and why such information is needed. The terms "substantial value" (Article 26 DEIO) and "relevance" (Articles 27 and 28 DEIO) for the purpose of the proceedings should not be interpreted in different ways, but rather as synonymous terms referring both to the necessity of the measure for the criminal investigation. Regarding the facts that may establish the presumption that a person may have a bank account in a certain MS, the approach should be always "pro cooperation", interpreting in a flexible way the facts required to underpin such presumption.

### *g) What shall be the consequences of not providing enough reasons for the EIO?*

407. Apart from the fact that the criteria on the basis of which the reasons justifying the request are not clear, it should be highlighted that none of the three provisions, i.e. articles 26, 27 and 28 DEIO, establish what shall be the consequences in case such justification is not detailed enough or if the issuing authority does not indicate any reasons justifying the issuing of the EIO. The question to be answered here is the following: may the executing authority refuse to execute an EIO issued in order to obtain information on bank accounts and banking operations on the ground that there are no reasons justifying the request or that the reasons indicated are not enough detailed? The answer to this question is particularly important from a practical point of view.

408. The answer to this question is NO. In the first place, there is no explicit indication of that and the Directive did not consider the lack of adequate motivation as a ground for refusal. In the second place, such an interpretation would run counter to the logic of mutual recognition and mutual trust between MSs which permeates the DEIO. The approach here as stated earlier, does not differ from the other investigative measures: the executing authority shall as a rule trust that the requesting authorities have already checked the legality, necessity and proportionality of the measure requested. In comparison to the system of mutual assistance, under the mutual recognition principle, the requested State would "not check and is not allowed to check the grounds that have motivated the request".[189]

409. In the third place, this interpretation is confirmed by in the Explanatory Memorandum, where with regard to Article 26 it is said that "the provision does not allow the executing authority to question whether the requested information is likely to be of substantial value for the purpose of the investigation concerned pursuant to the first indent of the paragraph".[190]

**94) Proposed best practice:** The executing authority cannot refuse to execute an EIO only because the issuing authority did not indicate detailed reasons justifying the request for bank information/monitoring. However, an interpretation according to which the executing authority is obliged to execute an EIO issued in order to request information on bank account or banking operations which does not contain any reasons cannot be accepted either. If the executing authority considers that the reasons given in the EIO are not sufficient, it shall consult with the issuing authority and eventually ask for further details.

[189] See L. Bachmaier Winter, "European investigation order for obtaining evidence in the criminal proceedings Study of the proposal for a European directive", ZIS 9/2010, p. 582.

[190] Explanatory memorandum, p. 25.

### *h) How is the bank customer's fundamental right to data protection safeguarded?*

410. Another important issue concerns the identification of the law applicable to the protection of the bank users' personal data that are exchanged between executing and issuing MS. In this regard a relevant question is: do specific rules apply to protect the data of the bank customer's whose data are exchanged through the EIO or does the general legal framework? In this case, which rules would, in particular, apply?

411. As mentioned above, the exchange of information on bank accounts and banking and financial operations is regulated in specific provisions of the DEIO. One of the reasons of the inclusion in the Directive of specific provisions concerning the exchange of bank data could be the need to protect particularly sensible data of the bank customer. Out of bank data it is possible to find out many personal details of the bank customer; in particular, the level of intrusiveness into the personal sphere of the data subject depends on the kind of data that are collected by the competent authorities.

412. The collection of identifying data is the less intrusive, while the obtaining of details concerning the banking and financial operations of the bank customer's allows the competent authorities to obtain much more sensible information. The monitoring in real time of the banking and financial transactions of the bank customer finally entails the highest degree of intrusiveness, as it allows the national authorities to survey in real time all the financial movements of the bank customer. The protection of those confidential personal data, which could entail interferences with the right to private life, was, *inter alia*, one of the reasons that justified the establishment of the bank secrecy: to protect the secrecy and confidentiality of the data confided by the client to the bank. As it is known until very recently banks were allowed not to disclose their client's bank information invoking the bank secrecy, that is to say, to invoke against the investigating authorities "the right or the obligation of a

banker to keep secret information he/she obtains in the course of his/her activities".[191]

413. In particular, bank secrecy covers all the information which can be used to personally identify the client and are confided by him/her to the financial institution or generated by the bank in relation to this client;[192] thus, any information which contributes to identifying the client and that the banker knows by reason of his/her profession. Before, bank secrecy could be invoked against the exchange of information requests. Now, however, bank secrecy has been considerably lifted for the purposes of cross-border exchange requests.

414. In fact, the financial crisis occurred in 2008, the high number of tax evasion and aggravated tax fraud cases, the fight against money laundering and financing of terrorism gradually restricted and, then, completely removed bank secrecy in all the European MSs.[193] In this regard, the political pressure exerted on those States which did not substantially apply the OECD standards relating to the exchange of information, i.e. those countries which were included in the so-called Grey List of countries which are not compliant with OECD tax cooperation rules,[194] played an important role. The reason some countries were included in the Grey List was the reservation to article 26(5) of the OECD Model Tax Convention concerning the exchange of information regarding income and capital.[195] However, from 2010 on, the European States included in the Grey List among which Austria, Luxembourg and Switzerland took back this reservation and negotiated new bilateral conventions integrating article 26(5). Thus, now, according to the OECD Model Convention, it seems that a requested authority may refuse to exchange information only in case of a fishing expedition.

---

[191] Such a definition is given by S. Braum, V. Covolo, "European Criminal Law and the Exchange of Tax Information: Consequences for Luxembourg's Bank Secrecy Law", *in* A. Rust, E. Fort (eds.), *Exchange of Information and Bank Secrecy*, Alphen aan den Rijn, 2012, p. 32, who cite, in turn, A. Steichen, "Le secret bancaire face aux autorités publiques nationales et étrangères", *Bulletin Droit et Banque*, 24, p. 27.

[192] See D. Spielmann, "Le secret bancaire et l'entraide judiciaire internationale pénale au Grand-duché de Luxembourg", Bruxelles, 1999, p. 25.

[193] See, for an in depth analysis, A. Rust, E. Fort (eds.), "Exchange of Information and Bank Secrecy", op. cit.

[194] The Grey List is available at the address https://www.oecd.org/tax/exchange-of-tax-information/42497950.pdf. The list refers to the progress made as at 2nd April 2009.

[195] See the OECD Model Convention on Income and on Capital at www.oecd.org.

415. It should be noted that, although bank secrecy has been recently considerably lifted, the need to ensure the protection of the confidential data of the bank customer remains essential. Access to banking data consists, in fact, of access to confidential personal data,[196] which may entail the interference with the right to private life[197] and data protection. In particular, the fundamental right to the protection of personal data and respect for private life is guaranteed at three levels within the European Union. In the first place, it is enshrined in the Charter of Fundamental Rights of the European Union, which, according to article 6 TEU, has the same legal values as the Treaties. In addition, it constitutes a general principle of the Union's law guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and as it results from the constitutional traditions common to the MSs.[198]

416. In the first place, it is enshrined in articles 7 and 8 of the Charter of Fundamental Rights of the European Union (CFREU), which respectively protect the right to private life[199] and the right to the protection of personal data. In this respect, although limitations on the exercise of these rights are possible, they must be provided for by law, they must respect the essence of these rights and freedoms and, by virtue of the principle of proportionality, "limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others".[200] Furthermore, the right to the protection of personal data is guaranteed by article 16 TFEU.

417. In the second place, it is enshrined in article 8 of the European Convention on Human Rights (ECHR). However, as far as the most intrusive

[196] Opinion 10/2006 of the "Article 29 Data Protection Working Party" on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), 22 November 2006.

[197] ECtHR, *M.S. v. Sweden*, App no 20837/92, 27 August 1997, § 35.

[198] See article 6(3) TEU.

[199] The Court of Justice specified that the right to respect to private life must not be interpreted restrictively; even activities of a professional nature are, in fact, covered by this provision. See CJEU, C-465/00, C-138/01 and C-139/01, *Rechnungshof v Österreichischer Rundfunk*, 20 May 2003, para. 73 ff.; CJEU, C-92/09 and 93/09, *Schecke, Eifert v Land Hessen,* 9 November 2010, para. 59.

[200] See article 52(1) of the Charter of Fundamental Rights of the European Union.

investigative measure is concerned, i.e. the monitoring of bank accounts, there is no a specific jurisprudence of the ECtHR, as the case law of the ECtHR on article 8 ECHR concerns mostly the interception of communications. The clarifications of the Court in this respect are nevertheless important also with regard to the monitoring of bank transactions, provided the high degree of intrusiveness of both measures and their common nature as "special investigative techniques" which should be conducted, on the one hand, without informing the target and, on the other hand, by using always more advanced technological devices to execute them.

418. Thus, according to the jurisprudence of the ECHtR, in view of their intrusive nature and in order to prevent the competent authorities to use them in an arbitrary way, the legal framework regulating them should specify the potential target of the measure and its duration, as well as the treatment of the persons accidentally monitored and any means of judicial control. These guarantees must thus be provided for by the law regulating the data protection of the bank customer, which, as mentioned below, is the Directive (EU) 2016/680. Despite the peculiar sensitiveness of these data, it follows from a combined reading of Articles 20, 26, 27 and 28 that there are no specific rules aimed at protecting the secrecy of these data.

419. On the contrary, the right of the bank customer to data protection is to be balanced against the need to ensure the confidentiality of the investigation. Article 19 of the DEIO, in fact, apart from obliging each MS to "take the necessary measures necessary to ensure that in the execution of an EIO the issuing authority and the executing authority take due account of the confidentiality of the investigation", specifically provides, in the last paragraph, that each MS "shall take the necessary measures to ensure that banks do not disclose to the bank customer concerned or to other third persons that information has been transmitted to the issuing State in accordance with Articles 26 and 27 or that an investigation is being carried out".

420. This duty of confidentiality must nevertheless be balanced against the right of the bank customer to the protection of his/her personal data. This balance between confidentiality of the investigation and right to protection of

the personal data of the person concerned forms the basis of the Directive (EU) 2016/680, which is the applicable law in case of an EIO issued to obtain information on bank accounts and banking and financial operations.

421. The applicability of the Directive 2016/680 to the case at issue is particularly derived from the combined reading of article 20 DEIO, which makes explicit reference to Council Framework Decision 2008/977/JHA, which has been repealed by Directive 2016/680, recital 42 of the DEIO and by Articles 1 and 2 of the 2016/680 Directive, which describe the objectives and the scope of application of Directive 2016/680.

422. Directive 2016/680 imposes strict requirements on the processing and transmission of data. However, the scope of application of that directive is rather limited, as legal persons are not included within its scope of application. According to article 1 of Directive 2016/680 it is aimed at protecting "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, including the safeguarding against and the prevention of threats to public security".[201]

423. By virtue of the Directive there are certain rights which must be guaranteed to the data subject;[202] among them, the data subject, i.e. the identified or identifiable natural person, whose data are retained,

- has the right to know at least the information listed in article 13 of the directive, i.e. the identity and the contact details of the controller, the contact details of the data protection officer, where applicable, the purpose of the processing for which the personal data are intended, the right to lodge a complaint with a supervisory authority and the contact details of the supervisory authority, as well as the existence of the right to request from the

[201] See article 1 of 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, L 199/89, 4.5.2016.

[202] See Article 12 et seq. Directive 2016/680.

controller access to and rectification or erasure of personal data and restriction of processing of the personal data concerning the data subject.

- In addition to that information, the data subject is to be provided by the controller with other additional data in some other specific cases.[203]

- Another right which should be granted to the data subject is the right to know whether or not personal data concerning him or her are being processed and, where that is the case, the right to access to personal data and some additional information. In this regard, it should nevertheless be highlighted that the content and scope of the rights of the data subject according to the directive depends partly on the implementation given to it in different MSs, as the rights of the subject, such as the right of access, may be restricted by MSs "to the extent that, and for as long as such a partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the natural person concerned".[204] MSs may, thus, within certain limits restrict the rights provided for in the Directive.

424. - Another important right guaranteed by the directive is the right to rectification or erasure of personal data and restriction of processing.[205]

**95) Proposed best practice:** In order to ensure the protection of the personal data of the bank customer, both issuing and executing authorities, must comply with the provisions of Directive 2018/680 and grant him/her the rights there enshrined, balancing these rights with the necessity to ensure the confidentiality of the investigations. Thus, in certain cases, the bank customer will have the right to know whether the data concerning him/her are processed and, in some other specific circumstances, to access to the data related to the criminal investigation.

## 16. EIO AND BREXIT

425. The negotiations on Brexit are not finalised yet. Therefore it is not

[203] See in this sense article 13.2 Directive 2016/680.
[204] See article 15(1) of the 2016/680 Directive.
[205] See Article 16 of the Directive 2016/680.

possible to identify a "best practice" nor to foresee the situation that the EU MSs will face in the judicial cooperation in criminal matters with the UK authorities after the exit of the UK from the EU. Despite the uncertainties, some thought has to be given to the after-Brexit scenario, if not to set clear guidelines which is not possible at the moment, at least to describe some of the situations that will be arise and how, in our opinion, should be addressed. Some of these questions are being addressed by the MSs, as is the case of Spain. Spanish Ministry of Justice is preparing a legislative decree to address the cooperation in criminal matters after the no deal Brexit. This decree is planned to be adopted by the end of March, thus its content and impact cannot be analysed here. What can be specified already is the type of questions the MSs will be facing after 29 March, if the no deal Brexit takes place. Regarding the EIO, some of these questions will be addressed here.

**16.1. What shall happen with the EIOs already issued and received by the UK before the exit day, but not yet executed? Should they continue to be executed as EIOs? Would it be necessary to handle them as letters rogatory? Which legal framework would be applicable to them?**

426. This question will need to be determined in the transitional dispositions adopted by the UK. It could be said that in order to favour the swift cooperation in the gathering of evidence in criminal matters, the Brexit should not hamper such effective cooperation. Therefore, it would be desirable that the UK authorities establish the possibility to continue executing the pending EIOs according to the rules applicable when the relevant EIO was received in the UK. This would be the best solution in order to prevent uncertainties, while at the same time, fostering the efficient cooperation. But this is just a desideratum, as it goes without saying that it is not within the objective of this project to set guidance to the UK authorities on the transitional rules that they should adopt.

427. If the UK would not contemplate any transitional provisions regarding the pending EIOs when the UK is executing State, it should be considered that after 29th March the EIO would not be applicable to the requests sent to the UK, and thus they should be executed following the MLA Conventions and its

Protocols, whose validity would be re-activated. As the forms of the EIOs would contain the relevant information that would amount to the information required for a letter rogatory, a flexible approach in the executing of such requests should be followed. This would entail, that the UK authorities would not reject the EIOs received, but adapt them to the provisions of the MLA Conventions.

**96) Proposed best practice:** In case of no-deal Brexit, MSs shall establish what shall be the rules applicable during the transitional period. What is to be recommended is that those rules in the diverse MSs seek certain uniformity, so that a similar legal framework in each of the MSs would not make more complex the judicial cooperation in criminal matters with the UK. Coordination among the relevant Ministries of Justice would be positive.

**16.2. In case of no deal, will it be possible to cooperate with the UK on the basis of the MLA Conventions (2001 and 1959)? Would these instruments cover all possible investigative measures as included in the EIO?**

428. The answer to this question is clearly yes. As the MLA Conventions have not been derogated by the entering into force of the EIO Directive, but only those rules "corresponding" to the EIO were substituted, the rules contained in the MLA Conventions, once the EIO rules lack force, will, as mentioned earlier, be re-activated, and thus become applicable in the assistance in gathering evidence in criminal matters. In principle, all the investigative measures covered by the EIO could also be requested under the MLA Conventions, although the grounds for refusal apply differently as well as the formal requirements, and deadlines.

**97) Proposed best practice:** In case of Brexit without deal, the judicial cooperation in criminal matters could continue functioning upon the MLA rules and proceedings.

### 16.3. Would it be possible to amend/complete an EIO that was issued and sent before the exit day, after the exit day?

429. The answer to this question will depend obviously on the transitional rules adopted by the UK, as to the applicable legal framework of the pending requests. Anyhow, the issuing authority could complement and amend the issued and sent EIO that would not be problematic. The question is how the receiving authority will be dealing with it. The answer would be the same as to any other EIO already issued and sent to the UK, as has been already addressed above.

**98) Proposed best practice:** Changing the legal framework should nevertheless not mean a refusal to cooperate in gathering evidence: adapting to the MLA conventional setting, interpreting the grounds for refusal in accordance to the willingness to cooperate –as agreed previously under the EIO instrument–, would be the most desired approach in the cross-border gathering of evidence.

### 16.4. What should the receiving/executing MSs do when they get an EIO from the UK after the exit date?

**99) Proposed best practice:** As best practice the receiving and executing judicial authorities should adopt a flexible approach in the sense that they should endeavour to provide the requested assistance within the framework of the applicable law, which would be the MLA Conventions or the existing bilateral agreements. The fact that the request is sent using the forms of the EIO should not impede to execute it according to the rules on MLA.

## 17. Beyond the EIO: Admissibility of evidence

430. Admissibility of evidence collected abroad will depend on how such evidentiary elements have been obtained and which rules have been applied during such a process. There is no uniform practice among the EU Member States. While several legal systems require that for evidence to be admissible, it

must have been obtained in accordance with the *lex fori*, other States admit such evidence as long as the *lex loci* has been complied with.[206] There are countries that do not check the process through which the evidence was collected abroad and apply an almost blind trust, the so-called *principle of non-inquiry*: the formalities or norms that governed the evidence-gathering abroad are not checked and there might not even be a control of the lawfulness of such evidence.[207] The diversity of solutions existing in each of the Member States hinders the establishment of what has been named 'an area of free movement of criminal evidence' and on the other hand may also have a negative impact on the defendant's rights of defence.

431. Until sufficient procedural harmonisation at the European level is reached, the best solution to ensure admissibility of cross-border evidence is that the executing authority respects as much as possible the rules and formalities indicated by the issuing authority. Such accommodation of the investigative measure to the *lex fori*, which was already foreseen in the EU MLA Convention of 2000 (Article 4), is set out in Article 9.2 DEIO. Its purpose is to avoid the evidence collected abroad becoming inadmissible because of non-compliance with the *lex fori*, while at the same time preventing the *lex fori* from being imposed in the executing State if it is not compatible with the basic principles of the executing State.

432. The Directive on the EIO has introduced a general rule aimed at advancing the protection of the defence rights, also in the proceedings where cross-border evidence has been collected within the EU. Without prejudice to national procedural rules Member States shall ensure that in criminal

[206] On the admissibility of evidence obtained abroad in Spanish criminal proceedings, see, among others, F. Grande Marlaska-Gómez and M. Del Pozo Pérez, "La obtención de fuentes de prueba en la Unión Europea y su validez en el proceso penal español" 24 *Revista General de Derecho Europeo* 1–41, 13 ff; F. Gascón Inchausti, "Report on Spain" in S. Ruggeri (ed), *Transnational Inquiries and the Protection of Fundamental Rights in Criminal Proceedings* (Springer, 2013) 475–95.

[207] A. van Hoek and M. Luchtman, "Transnational cooperation in criminal matters and the safeguarding of human rights" (2005) 1 (2) *Utrecht Law Review* 1–39, 15; S. Ruggeri, "Introduction to the Proposal of a European Investigation Oder: Due Process Concerns and Open Issues" in S. Ruggeri (ed), *Transnational Evidence and Multicultural Inquiries in Europe* (Heidelberg 2014) 29–35, 15.

proceedings in the issuing State the rights of the defence and the fairness of the proceedings are respected when assessing evidence obtained through the EIO (Article 14.7 DEIO)

433. This rule, which was added to the text of DEIO at the final stage of the negotiations, certainly represents a significant step forward in the protection of the defendant's rights. Even if it does not explicitly abolish the principle of *non-inquiry*, it sets out the obligation of the courts to check how evidence was collected in another Member State and whether the defendant's fundamental guarantees were respected. This rule should not be understood as a mere recommendation, but as a real obligation for the trial court to exercise certain control over the lawfulness of the evidence collected abroad. The real effect of this rule depends of course on how it is applied by the courts. The transposition of the DEIO in the countries studied does not shed light on how this rule is to be applied/interpreted. Further studies on its application should be carried out, in order to check whether the defence rights are adequately protected. It would be interesting to see how this rule would be interpreted by the Court of Justice of the European Union, but for that, some national court should file a preliminary question asking what is the control that the forum court shall exercise when admitting/assessing cross-border evidence.

434. Despite not being related to the issuing and executing of the EIO, this CBP would not be incomplete without setting guidelines on the application of one of the provisions included in the DEIO, namely Article 14.7 DEIO which states that MS shall ensure that the "rights of the defence and the fairness of the proceedings are respected when assessing evidence obtained through the EIO." It may sound reiterative to make a recommendation upon a rule that appears to be quite clear, but its importance for the defence rights demands to explain what should be its impact.

**100) Proposed best practice:** When assessing the evidence obtained through the EIO, the trial court shall ensure that the fair trial rights and the fairness of the proceedings are respected. To that end, the acting public prosecutor as well as the adjudicating court shall not follow the principle of non-inquiry, but undertake a reasonable control upon the rules followed in the obtaining of the

evidence, in particular, when it is unclear how the investigative measure was carried out.

## 18. LIST OF PROPOSED BEST PRACTICES

1) **Proposed best practice:** The MLA Conventions will also still be applicable to those acts of judicial cooperation that are not aimed at gathering evidence (not "corresponding provisions" pursuant Art. 34.1 DEIO), such as service of documents and summons (Art. 5 EU MLA Convention 2000), spontaneous exchange of information (Art. 7 EU MLA Convention 2000), returning of objects to the injured party (Art. 8 of EU MLA Convention 2000) or information with a view to opening proceedings by another country (Art. 21 EU MLA Convention 1959). Letters rogatory shall be used for requesting such judicial cooperation.
2) **Proposed best practice:** When the measure requested by the EIO is the controlled delivery of drugs or undercover police operations, the Spanish executing authorities shall treat these measures as measures restricting fundamental rights, with results in the ability to replace the measure or deny its recognition and implementation for any of the grounds for refusal foreseen by the LRM.
3) **Proposed best practice:** When the EIO requires the execution of a non-coercive measure, as a rule, the executing authority shall not analyse if it should be substituted by a less intrusive measure, and as a rule it shall not be refused, because such a measure shall exist in all MS. However, this does not mean that it shall be recognised automatically or that the general grounds for refusal do not apply.
4) **Proposed best practice:** The EIO applies also to administrative sanctioning proceedings and administrative authorities –if recognized as competent authorities– can also issue EIOs, even for the purpose of administrative punitive enforcement, as long as the procedural safeguards appropriate to criminal matters do apply. In identifying if a certain administrative proceeding falls within the scope of the EIO, the criteria set out by the CJEU in the *Baláž* case are to be followed.

5) **Proposed best practice:** The issuing authority within an administrative sanctioning procedure for a petty offence should evaluate whether it is proportional to issue an EIO for obtaining the information/evidence needed. MSs should elaborate internal instructions as to how the use of the EIO should be balanced against the possible costs that it may entail, when facing the sanctioning of a petty administrative offence. Information that can be obtained by way of police cooperation or cooperation with administrative bodies, such as the domicile of identity of a person, should be requested by those channels, rather than through an EIO.

6) **Proposed best practice:** Although a "best practice" cannot be identified or established here, but according to the autonomous concept of "criminal proceedings" of the CJEU and the nature of the investigations carried out by OLAF, it should not be excluded that OLAF could issue EIOs, subject, of course, the required validation procedure by a "judicial authority".

7) **Proposed best practice:** It is advocated to interpret the concept "criminal proceedings" also covering those stages that, according to the national law of the issuing State, are within the criminal jurisdiction, such as the enforcement stage or the breach of the conditions of parole.

8) **Proposed best practice:** It should be accepted that an EIO is issued for identifying and freezing assets to establish the factual basis of the non-conviction based confiscation measure. However, resorting to the EIO and justifying the use of this instrument because the close link of the assets to the evidentiary procedure, should not avoid to apply the rules on distribution of the sums confiscated among the MSs involved in such confiscation. Such distribution of assets should be governed by the rules provided in the Regulation (EU) 2018/1805 on the mutual recognition of freezing orders and confiscation orders.[208]

9) **Proposed best practice:** The issuing State should notify the "affected" State (once they have knowledge of it), to make them aware of the "interception";

[208] Regulation (EU) 2018/1805 of the European Parliament and of the Council of 14 November 2018 on the mutual recognition of freezing orders and confiscation orders OJ L 303, 28.11.2018.

the notified State should not oppose to the measure on the sole ground that it is not provided in their territory. The treatment of this measure should not be equalled to a coercive measure[209] as it does not encroach seriously upon the privacy or the property or other fundamental rights. This is why the flexible approach of the "affected" territory is advisable. As to the admissibility of evidence, this should lie exclusively within the forum court.

10) **Proposed best practice:** If the assistance of another MS is required for the interception –but not for the covert operation–, then it appears reasonable that the rules for the EIO on interception of communications should be applied. We are inclined to support this interpretation, and not subject every on-line covert investigation to the signature of a previous agreement. It would not be consistent with the logic of cyberspace and cybercrime investigations. Thus, the same requirements, conditions and grounds for refusal applicable to interception of telecommunications provided under Art. 30 DEIO, should apply.
11) **Proposed best practice:** In cases where not even the technical support of the affected State is necessary to carry on the online covert investigation, provisions of Art. 31 DEIO should be followed: notify the other MS where the measure is going to have effects (if known), and the executing State at the view of the intrusiveness of such measure, should decide on it in accordance with Art. 31.3 DEIO. Same principles established for the measure on interception of telecommunications without technical assistance, are to be applied here.
12) **Proposed best practice:** The instrument of cooperation and exchange of information between tax administrations is not intended to serve for requesting evidence needed in criminal proceedings. Before issuing an EIO to request tax information needed for the criminal proceedings, the authority may check if such information is already within the tax authority of the forum, but this is not a pre-requisite to issue the EIO or to determine the necessity of the EIO.

[209] See Recital 16.

13) **Proposed best practice:** Within the EAW proceedings it is still possible to request property as defined under Art. 29 FD EAW to be sent together with the arrested person. This should not be considered as incompatible with the DEIO.

14) **Proposed best practice:** As set out in the EPPO Regulation's Explanatory Memorandum, the assignment system does not replace the EIO, but supplements it. Therefore, in all other aspects not covered by the EPPO assignment system the EIO shall continue being applicable. Therefore, the defendant will be able to make use of it as provided under Article 1.3 DEIO.

15) **Proposed best practice:** Other rules provided in the DEIO for ensuring the fairness of the proceedings in the cross-border evidence proceedings, shall also be applicable to the EPPO assignment procedure. This applies specifically to the provision foreseen in Article 14.7 DEIO: "Without prejudice to national procedural rules MSs shall ensure that in criminal proceedings in the issuing State the rights of the defence and the fairness of the proceedings are respected when assessing evidence obtained through the EIO."

16) **Recommendation:** Once it is established that the ISP operating in the EU are obliged to produce e-data when requested by a EU judicial authority –regardless the location of the data–, it is unclear whether such obligation shall apply only within the scope of application of the EPO Regulation or if it could be understood that it also should apply to any request of e-evidence, regardless if it is transmitted by way of an EIO or an EPOC. As for now, this aspect is not clear, and therefore, until the Regulation on the EPO is adopted, it would be unreasonable to try to set any guideline in this regard. At this moment it can only be proposed, that the future text of the Regulation, if finally adopted, clarifies this point.

17) **Proposed best practice:** For practical reasons, when the issuing authority only needs stored e-evidence for the purpose of the criminal proceedings, he/she should opt for the issuing of an EPOC, which should in principle be quicker and easier to handle. However, if the issuing authority is requesting to the same MS also other types of evidence, it might not be worth to fragment the request, and it would be probably easier to issue an EIO for requesting jointly all the evidence requested from the same MS.

18) **Proposed best practice**: It is appropriate that the receiving authority is the one who has to execute the EIO. It is adequate that the receiving authority is in all three countries the PP, as they will also have competence to execute many of the EIOs. If the execution of the EIO requires to leave the execution in the hands of a judge –because this is required by domestic law of the executing state or because the issuing authority specifically requests so–, the PP shall transfer the EIO to the competent court.

19) **Proposed best practice:** Keeping the reception of the EIOs in the hands of one single institution (the PP), can also facilitate the registering, the elaboration of statistics and the dissemination of best practices, for the action of the PPs is better coordinated, due to their hierarchical structure. It will also ensure uniformity in the handling and transfer of the EIOs. Moreover, in those cases where the PP is directly competent also for the execution, this solution is to be viewed as the most efficient.

20) **Proposed best practice:** identifying the PP office of the relevant territory where the measure/s are to be executed as the receiving authority is a good option for handling incoming EIOs.

21) **Proposed best practice:** Once the EIO has been received by the PP (not in Poland), and the PP considers that the EIO is to be carried out by a judge, the way to proceed for optimising the efficiency, is that the same PP decides on the recognition before transferring the EIO to the judge, although the judge can later revise such decision. This is the solution adopted by Italy.

22) **Proposed best practice:** The best solution will depend on the contextual elements: depending which authorities are best prepared, more experienced and less overloaded. As for the moment, Spanish law has opted for concentrating the execution of "mixed EIOs" in the hands of the judges. It will need time to see how efficient this is dealt with in practice.

23) **Proposed best practice:** while the competence for executing each of the measures requested in an EIO will need to be divided, the competence (and coordination) for the recognition, coordination of execution of measures and transfer of evidence, can still be kept under one single judge/authority.

24) **Proposed best practice:** Questions and conflicts of competence among the executing authorities that would delay the whole procedure of the execution of the EIO should be avoided. To that end, certain flexibility should be applied so that the issues of territorial and material competence are solved in a swift manner: in gathering of evidence the principle of the legally pre-established judge is not to be interpreted in a strict way; therefore, issues of competence and jurisdiction should be addressed with flexibility, taking always into account the principle of efficiency in providing the requested judicial cooperation.
25) **Proposed best practice**: It does not seem that the Central Authority is to be involved in any form in the procedure of issuing or executing an EIO. However, in case of non-compliance or a systematic infringement of the obligations set out in the EIO Directive, the Central Authority can play a crucial role in collecting complaints regarding the EIO implementation.
26) **Proposed best practice:** The decision rejecting the issuing of an EIO requested by the defence should be motivated. Victims and other parties should be entitled to request the issuing of an EIO, as long as this is not incompatible with the principles of the national criminal procedure.
27) **Proposed best practice:** It should also be possible, to hear the parties to the process/proceeding before taking a decision on the issuing of the EIO, if such hearing does not endanger the outcome of the proceedings.
28) **Proposed best practice:** In cases of several measures requested within the same EIO, the decision on the competence of the executing authority might be quicker if the whole procedure is coordinated by one single authority.
29) **Proposed best practice:** Direct contact between requesting and executing judicial authority is crucial. The communication channels should work equally regardless who is the receiving/executing authority. Where according to national laws, receiving authority in certain cases cannot execute the measure, coordination between both authorities is to be ensured.
30) **Proposed best practice:** Before issuing an EIO, the issuing authority shall determine if the requested information can be provided by way of judicial cooperation or not.

31) **Proposed best practice:** Early involvement of Eurojust should be promoted, in particular with regard to EIOs that entail complexity of the investigation entails several measures and/or countries. Taking advantage of the support that Eurojust can give in the issuing of the EIO as well as in facilitating the execution, is to be promoted.

32) **Proposed best practice:** As a general rule, the form is enough and there is no need to attach the judicial decision. However, as an exception, if the executing State needs more information which are not possible to obtain from the form, it may request the issuing authority to send the judicial decision. It is however recommended that the issuing authority include in the EIO certain additional data with a view to seek the admissibility of evidence and/or facilitate the role of the executing authority. Thus, it is desirable that in Section I, besides recording the formalities and procedures required for the execution of the EIO, there are set out the measures or actions which can not be carried out in a "in a similar domestic case".

33) **Proposed best practice:** If such information is missing, before refusing, the receiving/executing authority shall communicate with the issuing authority asking to complement the data required. In certain cases where a coercive measure that entails a serious encroachment of the fundamental rights is requested via EIO, the executing authority may ask the judicial decision upon which the EIO is based to be sent.

34) **Proposed best practice:** To contribute to ensuring the admissibility of evidence, the issuing authorities shall include in the EIO those requirements that will facilitate the admissibility of the evidence and which should be followed by the executing authority. The issuing authority shall specify which requested measures are to be adopted by a judge and also whether the issuing authority could carry out the requested investigative measure in a similar domestic case.

35) **Proposed best practice:** Establishing precise conditions on privileges and immunities when the EIO requests the interrogation of a witness is also crucial to ensure that the admissibility of such statements are not challenged later. In cases where the witness is to be protected or is already within a witness protection programme, the issuing authority shall inform exactly the executing

authority what safeguards and confidentiality protections are to be adopted to shield the identity of the protected witness.

36) **Proposed best practice:** Within Section J (Legal remedies), it should be specified not only whether an appeal against the issuing of the EIO has been lodged, but also whether such an appeal is admissible according to the *lex fori*.

37) **Proposed best practice:** In order to avoid unnecessary translation costs, it is recommended to fill out the form of Annex A in *Word*, eliminating from the document the Sections and/or paragraphs not applicable to the specific EIO which is issued. In any event, the Italian and Spanish issuing authorities must not to fill Section L of Annex A DEIO.[210]

38) **Proposed best practice:** Before issuing the EIO authorities should check whether the EIO has to be sent/notified to other authorities of the executing State. In particular, in Italy the EIO shall be transmitted to the *Direzione Nazionale Antimafia e Antiterrorismo* when the investigations refer to some of the crimes mentioned in Art. 51 (3 and 3bis) ICPP[211]. Furthermore, copy of the issued EIO should be sent also to the *Ministero della Giustizia*[212].All MSs shall inform Eurojust (through its national member) of the transmission of an EIO, when the necessary conditions for the action of this body are met[213]. When such conditions exist, it is also possible to request the assistance of Eurojust in identifying the authorities competent to receive the EIO[214].

39) **Proposed best practice:** Each country shall identify clearly which is the authority to receive and execute those EIOs that relate to an investigative measure which is not linked to a precise territory. The same approach is to be done in order to identify the authorities that are to be notified following Art. 31 DEIO.

---

[210] Section L of the Annex XIII LRM, as regards Spain; and the Section L of the Annex A LD, as regards Italy.

[211] Art. 27(2) DL

[212] See Eurojust, Italian Desk, "L'ordine di indagine europea. Cosa è utile sapere? Domande e risposte", p. 10, 12.

[213] In Spain this obligation is explicitly set out in Art. 9(3) LRM, as well as in Art. 24 of the Law 16/2015, of the 7 of July. In Italy, in Art. 7 of the Law 4/2005, núm. 41.

[214] Art. 3 of the consolidated version of the Council Decision on the strengthening of Eurojust and amending Council Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime.

40) **Proposed best practice:** It shall be ensured that all information regarding incoming and outgoing EIOs is centralised for statistical aims in one body.

41) **Proposed best practice:** Certain information on DNA which is already kept in national data bases, can be provided by a central single unit. This practice is in conformity with the approach suggested below, regarding the identification of one single authority for executing EIOs that are not related to a certain territory. The practice in Spain allows to present this as best practice.

42) **Proposed best practice:** The information obtained by way of EIO should not be used to trigger a national separate criminal investigation. If such information raises doubts on the jurisdiction, it has to be called upon the involvement of Eurojust.

43) **Proposed best practice:** If during the execution of the requested investigative measure evidence of a new offence is discovered which does not present any connection with the initial one, the executing authorities shall proceed with such evidence according to their national rules on accidental findings. Consultations with the requesting authority shall always take place to decide how to proceed with the newly accidentally discovered evidence, unless it is manifest that such evidence is completely unrelated to the case that triggered the EIO.

44) **Proposed best practice:** An EIO should not be refused on this ground. It would be contrary to the principle of mutual recognition, as well as to the principle of mutual trust which "requires, particularly with regard to the area of freedom, security and justice, each of those States, save in exceptional circumstances, to consider all the other MSs to be complying with EU law and particularly with the fundamental rights recognised by EU law".[215]

45) **Proposed best practice:** In addition, the executing authority has no legitimacy to question the competence of the issuing or validating authority, as long as such authorities according to their own domestic legal system, qualify as "judicial authority" in accordance with the criteria set forth by the DEIO [Art. 2

[215] CJEU, C-404/15 and C-659/15 PPU, *Aranyosi and Căldăraru*, 5 April 2016, para. 78, and case law cited there.

(c) i)] and by the CJEU itself[216]. Furthermore, it should be noted that neither Art. 9.3 and 11 DEIO, nor the corresponding implementing law envisage expressly this circumstance as a ground for refusal of the EIO.

46) **Proposed best practice:** In general, the executing authority should NOT check whether the issuing authority has judicial nature under its national law. Only exceptionally when the executing authority has really grounds to believe/fear that the issuing authority might not be a judicial authority in the meaning of Art. 2 (c) (i) DEIO, may the executing State check it on the condition that coercive measures are concerned, and under its national law, according to fundamental constitutional principles, this authority can not be considered a judicial one. In this case, it can ask the issuing State to have the EIO validated by a judicial authority and if the latter does not validate it, it may refuse it or refer a preliminary question to the CJEU.

47) **Proposed best practice:** The participation of the lawyers in the execution of an EIO should be facilitated in order to protect the defence rights. Thus, as long as it is compatible with the investigations and those are not secret, intervention of the lawyers in the execution of the measures carried out in another MS should be promoted. To that end, the issuing authority should require that the defence lawyers are informed of the date scheduled for its practice.

48) **Proposed best practice:** It is recommended that the issuing or validating authority undertakes some kind of proportionality test, before issuing an EIO, which is not only focused on the need for the evidence to prosecute the crime, but also with regard to the costs that it may entail faced with the gravity of the offence.

49) **Proposed best practice:** One criterion is to be followed: the description of the facts have to be so precise as to allow the executing authority to identify the

[216] The case law of the CJEU on the concept "judicial authority", although adopted in the context of the EAW, may be applied to the EIO: "the words 'judicial authority' (…) are not limited to designating only the judges or courts of a Member State, but may extend, more broadly, to the authorities required to participate in administering justice in the legal system concerned". CJEU, C-477/PPU, *Kovalkovas*, 10 November 2016, para. 34; C-452/16 PPU, *Poltorak*, paras. 33, 38.

precise offence that is being investigated, and be able to exclude that the EIO is used for carrying out fishing expeditions.

50) **Proposed best practice:** Forms are aimed at facilitating, not at hindering the cooperation. In this sense, formalities are never to be invoked as a ground for refusal, as long as the issuing authority is one of the authorities listed in conformity with the DEIO.

51) **Proposed best practice:** If the request for an EIO is sent as a letter rogatory, or the other way round, an MLA request is transferred via an EIO form, in both cases, the executing authority shall promote the execution: proceed to execute under the applicable rules, and at the same time inform the issuing authority on the mistake detected.

52) This is more than a proposal for practitioners, but rather a proposal for taking legislative action at the EU level on common rules on professional immunities/privileges.

53) **Proposed best practice:** The rule is that the certificate "is" the judicial decision. Executing authority shall only exceptionally request the issuing authority for the judicial order granting the requested investigative measure. This should occur only very exceptionally, when the content of the EIO is unclear or open doubts on the legality of the execution of such measure in the executing state.

54) **Proposed best practice:** When the costs appear to be exceptionally high the executing authority shall consult on the: 1) relevance of the evidence to the proceedings; 2) on the relevance to the criminal policy; and 3) on the relevance to the overall costs. The general social interest has to taken into account when the problem of exceptionally high costs of an investigative measure arises.

55) **Proposed best practice:** Domestic rules should regulate all grounds for refusal provided under the DEIO as optional grounds for refusal, allowing the domestic judicial authorities to assess if they exist or not in each single case.

56) **Proposed best practice:** Refusal grounds are to be interpreted in a restrictive way, so that the EIO execution is not checked under the whole domestic legal framework of the executing state.

57) **Proposed best practice:** The executing authority, following Art. 11(1)(a) EIO, before refusing the execution of the EIO on the basis of an immunity, it should

seek to request the waiver of the immunity, which may be legally difficult, and also raise diplomatic concerns.

58) **Proposed best practice:** the only best practice that could be proposed with regard to this ground of refusal, is the general guiding principle: before deciding on the non-execution of the EIO, the issuing authority shall be consulted (Art. 11(2) DEIO).

59) **Proposed best practice:** If the laws of the executing state would allow the executing judge to control the classified nature of the evidence requested or, if he/she would be authorised to require and obtain the declassification of classified documents, this should also the way to proceed when executing an EIO affecting such interests. And again, here applies also Art. 11(4) EIO: before deciding on the non-recognition or non-execution of the EIO, the executing judicial authority shall consult the issuing authority.

60) **Proposed best practice:** This ground for refusal, if kept, should always have optional character. In those jurisdictions where the grounds for refusal have been regulated as mandatory, it shall be applied only in very exceptional occasions, and as a rule should not constitute an obstacle in the cooperation in the gathering of transnational evidence by way of an EIO.

61) The measures listed under Art. 10.2 DEIO shall be granted execution without undergoing any proportionality test, provided that the other formal requirements are complied with.

62) **Proposed best practice:** The preferred way to carry out the witness interrogations is to request to do it via video-conference. This should be the preferred way in all cases.[217] When such a way for whatever reasons is not feasible, issuing and executing authority should keep connected while the interrogation is being carried out. This would allow deciding immediately how to proceed in the case where out of the answers the initial witness turns out to be a suspect. If such immediate communication is not possible, we are inclined to propose that the interview is suspended until the issuing authority can be

[217] See also L. Bachmaier, *Transnational criminal proceedings, witness evidence and confrontation: lessons from the ECtHR's case law*, Utrecht Law Rev., special issue, 2013, September 2013, Volume 9, Issue 4 (September) 2013, pp. 126-148.

consulted. In no case the interrogation should continue as a witness, when according to the executing authority the witness should be held as suspect.

63) **Proposed best practice:** In the absence of a clear guideline, the proposed interpretation with regard to the use of evidence obtained under administrative proceedings without ensuring the right against self-incrimination in criminal proceedings, should always be in favour of the protection of human rights. Therefore if the evidence requested refers to data already in the possession of the executing authorities, but those data would not be admissible as evidence in the requested state, they should not be transferred to any other state.

64) **Proposed best practice:** The lack of double criminality should be interpreted in a very flexible way as a ground for refusal to cooperate with the requesting State. It has to be recalled that the grounds for refusal should as a rule have been regulated as optional and not mandatory. Those MSs whose legal framework have "transformed" the grounds for refusal into mandatory, when acting as executing State should not focus primarily in identifying grounds for refusal to avoid the cooperation, but rather in a flexible way.

65) **Proposed best practice:** When the EIO aims to determine whether the acts and persons suspected by the issuing authority have already been judged, this should be explicitly indicated in Annex A DEIO (preferably in Section G). Similarly, when the issuing authority fears that the EIO may be refused in the executing State for this reason, it should specify in Annex A (and preferably in its Section G) that the evidence obtained would not be used to prosecute or impose a sanction on a person whose can already been finally disposed in another MSs for the same acts.

66) **Proposed best practice***:* In order to effectively enforce the *ne bis in idem* principle, issuing and executing authorities should ensure that, as far as possible, the parties to the process are aware of the issuing and/or receipt of the EIO and can oppose to it. If the executing authority considers that an EIO might be against the principle of the *ne bis in idem*, before taking a decision in this regard, it will initiate a consultation process with issuing authority and,

where necessary, with the judicial authority which rendered the final decision on the same acts (if it is a third state).

67) **Proposed best practice*:*** Upon the receipt of an EIO the receiving or executing authority realize that the same facts are being investigated/prosecured in the requested State, the relevant authority shall notify this to the requesting authority and also involve Eurojust to address the issue on the jurisdiction, or eventually the setting up of a joint investigation team.

68) **Proposed best practice:** Article 6 (3) DEIO shall be interpreted in the sense that it requires to consult the issuing authority in all cases where there are questions related to the proportionality of the measure in terms of encroachment of fundamental rights as well as questions of the proportionality of the costs of the measure (related to the seriousness of the crime). Although Article 6 (3) DEIO states that the executing authority "may" consult, it should be advocated to consult in any event these doubts arise.

69) **Proposed best practice:** When receiving an EIO the executing authority shall substitute the requested measure by a less intrusive on, if such a measure would allow gathering the evidence requested. This practice has been observed frequently in the context of the request for bank data, where the requested measure of entry, search and seizure is being substituted by production orders. It would be possible that all MSs would provide for the possibility of accessing to bank information without the need to resort to a measure of entry and search.

70) **Proposed best practice:** The effective legal remedies against the EIO must be available for the parties to the criminal proceeding and for the third parties affected by the EIO. Consequently, when the respective national laws provide for an appeal in a similar domestic case, will be considered part of the process those third parties, at least for the purposes of challenging the decision or measure which affects them. This, of course, this is possible if the information about the possibility to use these legal remedies is given to the third persons as

soon as this information does not undermine the successful outcome of the investigations[218].

71) **Proposed best practice:** In case that MS A is requested to forward to MS C via an EIO the information obtained from MS B in execution of an EIO, it is recommended that, in case of non-coercive measures MS A forwards the information without needing to ask for the consent/authorisation of MS B from which it obtained the information. On the contrary, in case of coercive measures, it is recommended that MS A, either ask for the consent of MS B or of the data subject, or assess itself whether the processing of the information for this other purpose is necessary and proportionate for this other purpose in accordance with national and European law.

72) **Proposed best practice:** The best practice for transfer of evidence that can be transmitted via internet communication, is to implement the secured communications channel in each MS and if possible in each judicial district. While this is not implemented, the authorities should use any of the reliable existing channels (via EJN, Eurojust, SIS, COM Secure Online Portal, or e-MLA), which enable to establish the identity of the sender, the recipient, the content of the message + attachments and the date and time of the transfer, without possibilities of being manipulated. For other objects, it would be positive to adopt a common protocol on how the evidence should be transported, in order to ensure the authenticity and integrity of such evidence. The aspects of the costs should also be further studied.

73) **Proposed best practice:** If the issuing authority requests to seize data stored in a computer, in order to comply with the *lex loci* in Spain a specific justification is needed, in addition to the ordinary search and seizure. The receiving authority should make aware the issuing authority of such requirement and consult whether the seizure of computer data is also requested. If this is the case, the issuing authority should complement the previous EIO, and add the specific motivation for searching the computer and seizing the stored data.

[218] In Spain this notification represents a legal obligation in the cases where the person concerned by the measure is resident or domiciled in this State. See Art. 22 (1) LRM.

74) **Proposed best practice:** As a rule the executing authority shall not check the grounds that led to the issuing of the EIO by the issuing authority, nor compare the degree of suspicion required for a precise investigative measure in the issuing State and in the executing State. The rule is to trust the assessment made by the issuing authority on the legality, need and proportionality of the measure. Nevertheless, exceptionally, when the executing authority considers that there is a manifest lack of grounds for the issuing of an EIO or the reasons to issue it are not sufficiently described, it may refer to the issuing authority and ask for further clarifications.

75) **Proposed best practice:** In establishing the duration of the interception of communications in the executing state, the executing authority should try to respect the principle of mutual recognition in so far as this does not collide with its own laws and constitutional principles. In that vein, as long as the "desired" duration expressed in the EIO is not contrary to the national provisions, the executing authority should not apply its own criteria to limit such duration.

76) **Proposed best practice:** For taking the decision on the possible extension of the interception of communications, issuing and executing authority shall agree on the periodicity of the transfer of the results of the interception. Fluent communication between the issuing and executing authorities should be promoted for swiftly addressing these issues, as well as other possible incidents that may appear during the execution of the interception of telecommunications. The control by the issuing authority over the execution of the measure in order to decide over the possible prolongation would be clearly facilitated if there were an immediate transmission of the intercepted communications.

77) **Recommendation:** EU should strive to agree on a common understanding of the concept of sovereignty in connection to the digital space in order to clarify and establish common principles and standards of protection when digital evidence is gathered without technical assistance of any other EU MS. This endeavour is crucial for ensuring the admissibility of evidence, and the EU would have legislative competence on this subject, according to Article 82.2 (a) TFEU.

78) **Proposed best practice:** As done in Spain, Italy or Germany, for notification purposes under Article 31.1 DEIO, a specific judicial authority should be identified. This authority or authorities (in the case of Germany it is divided due to its federal structure), shall receive the incoming notification, register it for the aims of statistics, and communicate with the "intercepting authority" on the authorization or refusal to continue with the interception. In case such authority is not identified in a relevant MS, the notification should be sent to the central authority. Where several authorities are appointed as receiving authorities of the notification provided under 31.1 DEIO, those authorities shall establish a uniform interpretation and approach, so that the standards applied are consistent.

79) **Proposed best practice:** "Intercepting" State shall always notify the States that have been affected by the interception measure, because the subject was located in its territory. If the subject is moving from one country to another, all of them should receive the notification.

80) **Proposed best practice:** Notified States should take a flexible approach towards the interceptions of telecommunications carried out in their territory without their technical support, when it affects a person who is travelling. They should not apply the possibilities provided under Article 31.3 DEIO in a strict way. This provision should not operate as a validity check of the interception according to the national standards applicable to the measure in a similar domestic case. A too strict approach might case the undesired effect that the intercepting authorities would skip the obligation to notify the affected State and use such evidence according their own standards on admissibility of evidence, and thus contribute to creating more distrust. In any event, the best approach should be to take action at the EU level on the concept of sovereignty in the digital space, as expressed above.

81) **Proposed best practice:** Until a common agreement on the rules applicable to the digital space are adopted, the case of the interception of communications carried out from abroad using remote interception devices to intercept the communications of physical or legal persons that are resident in a foreign

country, should undergo the same standards as to the interceptions of communications with technical assistance via EIO.

82) **Proposed best practice:** As long as there are no common EU rules on admissibility of evidence, the domestic procedural rules on evidence will apply, and as long as these rules are in conformity with the general principles set out by the ECtHR, the MS enjoy a broad leeway. Compliance with *lex loci*, is not required as a pre-requisite for admissibility of cross-border evidence in every MS. Nevertheless, the best practice would be that the trial court in the forum State, in conformity with Article 14.7 DEIO, shall check if the infringement of the *lex loci* in the gathering of evidence would violate the procedural rights of the defendant.

83) **Recommendation:** In order to promote the free circulation of evidence and to avoid that the diverse standards of admissibility of evidence end up in lowering the defence rights on the one hand, or represent an obstacle in the cooperation on the other hand, it would be advisable to advance in establishing common standards on admissibility of criminal evidence in cross-border criminal proceedings.

84) **Proposed best practice:** Each MS should ensure that the relevant judicial authorities comply with the obligation set out under Article 31.1 DEIO. Non-compliance with such an obligation should trigger consequences for infringement of EU law. Further, it would be advisable that the EU continues advancing in building up the AFSJ and makes use of the legislative process as provided under Article 82.2 (a) TFEU.

85) **Proposed best practice:** The lack of certain data to be specified in Annex C should not lead to the prohibition to continue the interception or to use the gathered elements as evidence. The notified authority shall consult the intercepting authority before taking any decision. In any event, the interpretation shall always be pro cooperation. The timeframe of 96 hours (4 days) shall preclude the possibility to exercise the objection under Article 31.2 DEIO.

86) **Proposed best practice**: Even if the difficulties might appear to be insurmountable, both from technical and legal points of view, the ASFJ needs to

advance towards the direct access to the interception of communications, developing the needed software and technical support, as well as by harmonising the regulation on immunities and privileges.

87) **Proposed best practice:** The regulation of the remote search of computers requires a common approach at the EU level in order to prevent that diverse requirements and criteria for assessing the proportionality of this measure, end up making the investigations in the digital space subject to a cumbersome fragmentation, not justified by technical issues but by a somewhat artificial territorial concept of the cyberspace. As long as this common rules are not implemented, MSs should make use of Article 31.3 DEIO very sparsely, and prohibit the use of evidence gathered without technical support only in very exceptional cases.

88) **Proposed best practice:** The information whether a person "holds or controls one or more accounts" is to be defined in the broad sense as expressed in the EU MLA Convention, Recital 27 DEIO, and Article 26.3 DEIO. It should be ensured that the practice in all MSs regarding the definition of legal or physical person who "holds or controls" an account is applied uniformly. Following Article 26.6 DEIO, and regardless how this measure is labelled in the domestic legal framework, the execution of this measure related to non-bank financial institutions, could also be refused if it were not available in a similar domestic case. However, not being a coercive measure, this ground for refusal should be applied in a restrictive way.

89) **Proposed best practice:** It follows from Article 27 paragraph 1 in conjunction with Article 27.4 DEIO and the Explanatory Memorandum that the EIO may also cover accounts held by third persons who are not themselves subject to any criminal proceedings, but whose accounts are linked to a criminal investigation. The issuing authority shall refer to the facts that allow to establish such a link in order to protect the rights of third persons that are not related to the criminal acts investigated, and that are unaware of the use that is being made of their bank accounts.

90) **Proposed best practice:** The adoption and implementation of the Proposal for a Directive of 17 April 2018 will enable a swifter and more effective execution

of the EIOs. From the point of view of the cross-border gathering of evidence in criminal proceedings, its adoption should be seen as very positive. It would reduce timeframes and costs in the execution of EIOs related to the financial information covered by it.

91) **Proposed best practice:** As with other investigative measures that are very intrusive in the fundamental rights of the persons affected by them, the issuing authority shall specify very clearly what are the accounts to be monitored and give specific grounds when the holder of the account is a person not linked to the criminal acts and the criminal investigation. As at present bank information can provide a vast amount of information affecting the privacy of the users (not only financial aspects, but others as e.g. what has been purchased, at what time, where, etc.), the issuing authority shall scrutinize thoroughly the requirements of proportionality and necessity of the measure. The development of common criteria/thresholds for authorizing this investigative measure within the EU would be very positive.

92) **Proposed best practice: a) Relationship between art. 26 (2), 27 (2) and 10 (1)(5) DEIO:** If the information requested via the EIO concerns a bank, the ground for non-execution referred to in article 10.1 (5) of the EIO does not apply. MSs shall comply with articles 26.2 and 27.2 DEIO. There is no possibility to refuse the measure because it does not exist or would not be available to a similar domestic case. This is specially important in those cases where the executing State executes these requests for bank information under the rules of search and seizure and/or interception of communications. The request for bank data cannot be refused because the search and seizure or the interception of communications is limited to offences with a minimum threshold of penalty. **b) Relationship between articles 26, 27, 28 DEIO and article 11 DEIO:** The general grounds for refusal under article 11 DEIO apply also in respect of articles 26 and 27 DEIO.

93) **Proposed best practice:** While it is impossible to define in abstract what level of detail shall have the reasons given by the issuing authority on the value or relevance of the information requested for the purposes of the criminal investigation concerned, the issuing authority shall establish at least what are

the links between the evidence/information requested and the aims of the criminal investigation, and why such information is needed. The terms "substantial value" (Article 26 DEIO) and "relevance" (Articles 27 and 28 DEIO) for the purpose of the proceedings should not be interpreted in different ways, but rather as synonymous terms referring both to the necessity of the measure for the criminal investigation. Regarding the facts that may establish the presumption that a person may have a bank account in a certain MS, the approach should be always "pro cooperation", interpreting in a flexible way the facts required to underpin such presumption.

94) **Proposed best practice:** The executing authority cannot refuse to execute an EIO only because the issuing authority did not indicate detailed reasons justifying the request for bank information/monitoring. However, an interpretation according to which the executing authority is obliged to execute an EIO issued in order to request information on bank account or banking operations which does not contain any reasons cannot be accepted either. If the executing authority considers that the reasons given in the EIO are not sufficient, it shall consult with the issuing authority and eventually ask for further details.

95) **Proposed best practice:** In order to ensure the protection of the personal data of the bank customer, both issuing and executing authorities, must comply with the provisions of Directive 2018/680 and grant him/her the rights there enshrined, balancing these rights with the necessity to ensure the confidentiality of the investigations. Thus, in certain cases, the bank customer will have the right to know whether the data concerning him/her are processed and, in some other specific circumstances, to access to the data related to the criminal investigation.

96) **Proposed best practice:** In case of no-deal Brexit, MSs shall establish what shall be the rules applicable during the transitional period. What is to be recommended is that those rules in the diverse MSs seek certain uniformity, so that a similar legal framework in each of the MSs would not make more complex the judicial cooperation in criminal matters with the UK. Coordination among the relevant Ministries of Justice would be positive.

97) **Proposed best practice:** In case of Brexit without deal, the judicial cooperation in criminal matters could continue functioning upon the MLA rules and proceedings.

98) **Proposed best practice:** Changing the legal framework should nevertheless not mean a refusal to cooperate in gathering evidence: adapting to the MLA conventional setting, interpreting the grounds for refusal in accordance to the willingness to cooperate –as agreed previously under the EIO instrument–, would be the most desired approach in the cross-border gathering of evidence.

99) **Proposed best practice:** As best practice the receiving and executing judicial authorities should adopt a flexible approach in the sense that they should endeavour to provide the requested assistance within the framework of the applicable law, which would be the MLA Conventions or the existing bilateral agreements. The fact that the request is sent using the forms of the EIO should not impede to execute it according to the rules on MLA.

100) **Proposed best practice:** When assessing the evidence obtained through the EIO, the trial court shall ensure that the fair trial rights and the fairness of the proceedings are respected. To that end, the acting public prosecutor as well as the adjudicating court shall not follow the principle of non-inquiry, but undertake a reasonable control upon the rules followed in the obtaining of the evidence, in particular, when it is unclear how the investigative measure was carried out.

## 19. REFERENCES

### Case law

### European Court of Justice


CJEU, C-465/00, C-138/01 and C-139/01, *Rechnungshof v Österreichischer Rundfunk*, 20 May 2003

CJEU, C-187/01 and C-385/01, *Gözütok and Brügge*, 11 February 2003

CJEU, C-496/03, *Miraglia*, 10 March 2005

CJEU, C-436/04, *Van Esbroek*, 9 March 2006

CJEU, C-150/05, *Van Straaten*, 28 September 2006

CJEU, C-467/04, *Gasparini and others*, 28 September 2006

CJEU, C-367/05, *Kraaijenbrink*, 18 July 2007

CJEU, C-288/05, *Kretzinger*, 18 July 2007

CJEU, C-297/07, *Bourquain*, 11 December 2008

CJEU, C‑491/07, *Turanský*, 22 December 2008

CJEU, C-92/09 and 93/09, *Schecke, Eifert v Land Hessen,* 9 November 2010

CJEU, C-261/09, *Mantello*, 16 November 2010

CJEU, C-489/10, *Åklagaren Bonda*, 5 June 2012

CJEU, C-617/10, *Łukasz Marcin Fransson*, 26 February 2013

CJEU, C‑129/14 PPU, *Spasic*, 27 May 2014

CJEU, C-398/12, *M*, 5 June 2014

CJEU, C‑404/15 and C‑659/15 PPU, *Aranyosi and Căldăraru*, 5 April 2016

CJEU, C‑486/14, *Kossowski*, 29 June 2016

CJEU, C-477/PPU, *Kovalkovas*, 10 November 2016

CJEU, C-217/15 and C-350/15, *Orsi y Baldetti*, 5 April 2017

C-324/17, *Gavanozov*, 31 May 2017, OJEU C 256/16

CJEU, C-524/15, *Luca Menci*, 20 March 2018

CJEU, C‑537/16, *Garlsson Real Estate and others*, 20 March 2018

CJEU, C-596/16 and 597/16, *Enzo di Puma y Commissione Nazionale per la Società e la Borsa (Consob)*, 20 March 2018

CJEU, C‑60/12, *Marián Baláž*, 14 November 2013

CJEU C-452/16 PPU, *Poltorak*, 10 November 2016

**European Court of Human Rights**

ECtHR, *Engel v. The Netherlands*, App no 5100/71, 8 June 1976

ECtHR, *Klass and others v Germany*, App no 5029/71, 6 September 1978

ECtHR, *Lüdi v Switzerland*, App no 12433/86, 15 June 1992

ECtHR, *Dombo Beheer v. The Netherlands*, App no 14448/88, 27 October 1993

ECtHR, *Saunders v. UK*, App no 19187/91, 17 December 1996

ECtHR, *M.S. v. Sweden*, App no 20837/92, 27 August 1997

ECtHR, *IJL et al v. UK*, App no 29522/95, 30056/96, and 30574/96, 19 September 2000

ECtHR, *J.B. v. Switzerland*, App no 31827/96, 3 May 2001

ECtHR, *Weh v. Austria*, App no 38544/97, 8 April 2004

ECtHR, *Shannon v. United Kingdom*, App no 6563/03, 4 October 2005

ECHtR, *Grayson and Barnham v. the United Kingdom*, App no 19955/05, 15085/0623, September 2008

ECtHR, *Chambaz v. Switzerland*, App no 11663/04, 5 July 2012

ECtHR, *Bochan v. Ukraine*, App no 22252/08, 5 February 2015

ECtHR, *MN and Others v. San Marino*, App no 28005/12, 7 July 2015

ECtHR, *Brito Ferrinho Bexiga Villa-Nova v. Portugal*, App no 69436/10, 1 December 2015

**Others**

German Constitutional Court judgment 1 BvR 370/07,1 BvR 595/07, of 27 February 2008

Spanish Constitutional Court judgment 253/2006 of 11 September 2006

Spanish Constitutional Court judgment 272/2006, of 25 September 2006

Spanish Constitutional Court judgment 206/2007, of 24 September 2007

Spanish Constitutional Court judgment 142/2009, of 15 June 2008

Spanish Constitutional Court judgment 70/2008 of 23 June 2008

Spanish Constitutional Court judgment 199/2013, of 5 December 2013

Spanish Constitutional Court, judgment 43/2014, of 27 March 2014

Spanish Constitutional Court Judgment 54/2015 of 16 March 2015

Spanish Supreme Court Decision of 18 June 1992

US District Court for the District of Vermont*, United States v. Hunter,* 13 F. Supp. 2d 574 (D. Vt. 1998), 10 June 1998

US Supreme Court, *Carpenter v. United States*, Certiorari to the United States Court of Appeals for the Sixth Circuit, 22.6.2018

**European official documents**

Council Decision on the strengthening of Eurojust and amending Council Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime

Council Document, Initiative of the Kingdom of Belgium, the Republic of Bulgaria, the Republic of Estonia, the Kingdom of Spain, the Republic of Austria, the Republic of Slovenia and the Kingdom of Sweden for a Directive of the European Parliament and of the Council regarding the European Investigation Order in criminal matters - Explanatory Memorandum, 9288/10 ADD 1, 3 June 2010

Council Document, "Note on the meaning of "corresponding provisions" and the applicable legal regime in case of delayed transposition of the EIO Directive", doc 9936/17 LIMITE, 13 June 2017, Annex II.

Council Document, "Extracts from Conclusions of Plenary meetings of the EJN concerning the practical application of the EIO", 15210/17, 8 December 2017

Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States

Council Framework Decision 2008/947/JHA of 27 November 2008 on the application of the principle of mutual recognition to judgments and probation decisions with a view to the supervision of probation measures and alternative sanctions

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

Council Framework Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Record Information System (ECRIS)

Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings

Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, OJ L 309, 25.11.2005, pp. 15-36

Directive 2011/16/EU of 15 February 2011 on administrative cooperation in the field of taxation and repealing Directive 77/799/EEC, OJ L 64, 11.3.2011, pp. 1–12

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

Directive 2014/42/EU of the European Parliament and of the Council of 3 April 2014 on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union, O.J. L127/39, 29.4.2014, pp. 39–50

Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, OJ L 141, 5.6.2015, pp. 73-117

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, L 199/89, 4.5.2016, pp. 89–131

Explanations relating to the Charter of Fundamental Rights, OJ C 303, 14.12.2007, p. 17–35

Eurojust and EJN, Joint Note of 2.5.2017, “Note on the meaning of corresponding provisions and the applicable legal regime in case of delayed transposition of the EIO Directive”, Council doc. 9936/17

European Convention on Mutual Assistance in Criminal Matters of 1959, Strasbourg, 20 April 1959

Opinion 10/2006 of the "Article 29 Data Protection Working Party" on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), 22 November 2006

Proposal for a Directive of the European Parliament and of the Council laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences and repealing Council Decision 2000/642/JHA, COM(2018) 213 final

Proposal from the Commission for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters, COM/2018/225 final

Recommendation No. R (80) 8 of the Committee of Ministers to Member States concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters, of 27 June 1980

Regulation (EU) 2018/1805 of the European Parliament and of the Council of 14 November 2018 on the mutual recognition of freezing orders and confiscation orders OJ L 303, 28.11.2018

**Other official documents**

FGE, Circular 1/2000 of 18 December regarding the application criteria of the Organic Law 5/2000 of 12 January, regulating the Minors' criminal liability

FGE, Circular 4/2013 of 30 December 2013 "sobre diligencias de investigación" ("Instructions of the Prosecutor's General Office on investigative measures"), pp. 19-25

Legislative Decree n. 108 of 21 June 2017, "Norme di attuazione della direttiva 2014/41/UE del Parlamento europeo e del Consiglio, del 3 aprile 2014, relativa all'ordine europeo di indagine penale"

Ley 22/2015, de 20 de julio, de Auditoría de Cuentas ("Law 22/2015, 20 July, Audit Of Accounts")

Order ECC/2503/2014, of 29 December, BOE n. 316, 31.12.2014, p. 107641 ff. ("Orden ECC/2503/2014, de 29 de diciembre, por la que se crea el fichero de datos de carácter personal denominado «Fichero de Titularidades Financieras»")

**Books and book chapters**

M. Aguilera Morales, *Proceso penal y causa general,* Madrid 2008

L. Bachmaier Winter, "The role of the proportionality principle in cross-border investigations involving fundamental rights", *in* S. Ruggeri (ed), *Transnational inquiries and the protection of fundamental rights in criminal proceedings. A study in memory of Vittorio Grevi and Giovanni Tranchina*, Heidelberg, 2013

L. Bachmaier Winter, "The proposal for a Directive on the European Investigation Order and the grounds for refusal. A critical assessment", *in* S. Ruggeri (ed.), *Transnational evidence and multicultural inquiries in Europe*, Heidelberg, 2014, pp. 71–90

L. Bachmaier Winter, "Access to Telecommunication Data in Criminal Justice: Spain", in U. Sieber, N. von zur Mühlen (eds.), *Access to Telecommunication Data in Criminal Justice* Berlin, 2016, pp. 647–704

M. Böse, "Human rights violations and mutual trust: recent case law on the European arrest warrant", *in* S. Ruggeri (ed.), *Human rights in European Criminal law. New Developments in European Legislation and case law after the Lisbon Treaty*, Heidelberg, 2015

G. Boulet, P. De Hert, "Access to Telecommunication Data in Criminal Justice: Belgium", *in* U. Sieber and N. von zur Mühlen (eds.), *Access to Telecommunication Data in Criminal Justice,* Berlin, 2016, pp. 123–246

S. Braum, V. Covolo, "European Criminal Law and the Exchange of Tax Information: Consequences for Luxembourg's Bank Secrecy Law", *in* A. Rust, E. Fort (eds.), *Exchange of Information and Bank Secrecy*, Alphen aan den Rijn, 2012

L. Buono, "The genesis of the European Union's new proposed legal instrument(s) on

e-evidence Towards the EU Production and Preservation Orders," *ERA Forum,* 3.9. 2018, accesible at https://doi.org/10.1007/s12027-018-0525-4

Cameron, "Access to Telecommunication Data in Criminal Justice: Sweden", in U Sieber, N. von zur Mühlen (eds), *Access to Telecommunication Data in Criminal Justice,* Berlin, 2016, pp. 611–44

J.A. Choclán Montalvo, *La aplicación práctica del delito fiscal: cuestiones y soluciones,* Barcelona, 2011

S. De Miguel Arias, "Algunos aspectos de la protección jurídica de los obligados tributarios ante los requerimientos de información en la Unión Europea", *in* F.A. García Prats (ed.), *Intercambio de información, blanqueo de capitales y lucha contra el fraude fiscal,* Madrid, 2014, pp. 379-397

M.G. Findley, D.L. Nielson, J.C. Sharman, "Global Shell Games: Experiments in Transnational Relations, Crime, and Terrorism", Cambridge, 2014

F. Gascón Inchausti, "Inmunidades procesales y tutela judicial frente a Estados extranjeros", Cizur Menor, 2008

S. Gless, *Beweisgrundsätze einer grenzüberschreitende Rechtsverfolgung*, 2006

H.H. Herrnfeld, "The draft regulation on the establishment of the European Public Prosecutor's Office - issues of balance between prosecution and defence", *in* C. Briére, A. Weyembergh (eds.), *The needed balances in EU criminal law*, Oxford, 2017, pp. 382-412

F. Jiménez-Villarejo Fernández, "Orden europea de investigación: ¿Adiós a las comisiones rogatorias?", *in* C. Arangüena (ed), *Cooperación judicial civil y penal en el nuevo escenario de Lisboa*, Granada, 2011

M. Kloth, "Immunities and the Right of Access to Court under Art. 6 of the European Convention on Human rights", Leiden, 2010

M. Panzavolta, "Ordine di indagine europeo e indagini bancarie: spunti di riflessione sul concetto di caso interno analogo e atto di indagine alternativo", *in* A. Di Pietro, M. Caianiello (eds.), *Indagini penali e amministrative in materia di frodi IVA e di imposte doganali. L'impatto dell'European Investigation Order sulla cooperazione*

*transnazionale*, Bari, 2016

M. Panzavolta, "Forfeiture and Fundamental Rights: Open Questions in the Twenty-First Century", *in* Ligeti K./Simonato M. (eds.), *Chasing Criminal Money. Challenges and Perspectives on Asset Recovery in the EU*, Oxford, 2017, pp. 25-52

N. Rodríguez García, "El decomiso de activos ilícitos", Cizur Menor, 2017

J.P. Rui, U. Sieber, "Non-Conviction-Based Confiscation in Europe. Bringing the Picture Together", *in* Rui, J.P./Sieber, U. (eds.), *Non-Conviction-Based Confiscation in Europe*, Berlin, 2015, pp. 245-304

A. Rust, E. Fort (eds.), "Exchange of Information and Bank Secrecy", Alphen aan den Rijn, 2012

M.E. Schulz, "Beneficial ownership: The private sector perspective", *in* G. Fenner Zinkernagel, C. Monteith, P. Gomes Pereira, *Emerging Trends in Asset Recovery*, Bern, 2013

M. Simonato, M. Lassalle, "A fragmented approach to asset recovery and financial investigations: a threat to effective international cooperation?", *in* Z. Durdevic, E. Ivicevic Karas, (eds.), *European Criminal Procedure Law in Service of Protection of European Union Financial Interests: State of Play and Challenges*, Croatian Association of European Criminal Law, Zagreb, 2016

T. Tropina, *in* U. Sieber and N. von zur Mühlen (eds.), *Access to Telecommunication Data in Criminal Justice*, Berlin, 2016, pp. 13–117

J.A.E. Vervaele, "Secreto de estado y "privilegios probatorios" en los procesos de terrorismo en los estados Unidos. ¿Control judicial de los arcana imperii?", *in* L. Bachmaier Winter (ed.), *Terrorismo, proceso penal y derechos fundamentals*, Madrid, 2012, pp. 229-261

T. Wahl (with B. Vogel and P. Köppen) "Access to Telecommunication Data in Criminal Justice: Germany" in U. Sieber, N. von zur Mühlen (eds), *Access to Telecommunication Data in Criminal Justice,* Berlin, 2016, pp. 499–610

**Legal Journals**

W. Abel, "Agents, Trojans and tags: The next generation of investigators", *International Rev. of Law Computers & Technology,* vol. 23, 2009, pp. 99-108

M. Aguilera Morales, "El exhorto europeo de investigación: a la búsqueda de la eficacia y la protección de los derechos fundamentales en las investigaciones penales transfronterizas", *BIMJ*, 2012, 2145, p. 11 ff

I. Armada, "The European Investigation Order and the lack for European standards for gathering evidence. Is a fundamental rights-based refusal the solution?", *NJECL*, Vol 6, issue 1, 2005, pp. 8-31

L. Bachmaier Winter, "European investigation order for obtaining evidence in the criminal proceedings Study of the proposal for a European directive", ZIS 9/2010, pp. 580-589

L. Bachmaier, "Transnational criminal proceedings, witness evidence and confrontation: lessons from the ECtHR's case law", *Utrecht Law Rev.,* special issue, 2013, September 2013, Volume 9, Issue 4 (September) 2013, pp. 126-148

L. Bachmaier Winter, "Transnational evidence: towards the transposition of the Directive 2014/41 regarding the European Investigation Order in criminal matters", *eucrim*, 2015/2, pp. 47-59

T. Böckenförde, "Auf dem Weg zur elektronischen Privatsphäre", *Juristenzeitung,* 19/2008, pp. 925-939

P. Caeiro, "Jurisdiction in criminal matters in the EU: negative and positive conflicts, and beyond", *Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft (KritV),* vol. 93, No. 4, 2010, pp. 366-379

P. Csonka, C. Juszczak, E. Sason, "The establishment of the European Public Prosecutor's Office. The road from vision to reality", *eucrim* 2017/3, pp. 125-133

J.M. Calderón Carrero, "Hacia una nueva era de cooperación fiscal europea: las Directivas 2010/24 UE y 2011/16 UE de asistencia en la recaudación y de cooperación administrativa en materia fiscal", *Rev. Contabilidad y Tributación,* núm. 343, 2011, pp. 49-86

C. Di Francesco, "Repercussions of the establishment of the EPPO via enhanced cooperation. EPPO's added value and the possibility to extend its competence", *eucrim* 2017/3, pp. 156–160

V. Franssen, "The European Commission's E-evidence Proposal: Toward an EU-wide Obligation for Service Providers to Cooperate with Law Enforcement?", *European Law Blog*, October 12, 2018, available at http://europeanlawblog.eu/2018/10/12/the-european-commissions-e-evidence-proposal-toward-an-eu-wide-obligation-for-service-providers-to-cooperate-with-law-enforcement/

J. Espina, "The EIO and its relationship with other cooperation instruments: basic replacement and compatibility rules", *eucrim*, 2019 (forthcoming)

C. García Novoa, "Una aproximación del Tribunal Constitucional al derecho a no autoinculparse ante la Inspección Tributaria en relación con los delitos contra la Hacienda Pública", *Jurisprudencia Tributaria Aranzadi*, 53/2005, pp. 1-9

S. Gless, "Transnational Cooperation in Criminal Matters and the Guarantee of a Fair Trial: Approaches to a General Principle", *Utrecht Law Rev.,* Vol 9, Issue 4, 2013, pp. 90-108

J.L. Goldsmith, "The internet and the legitimacy of the remote cross-border searches", *University of Chicago Legal Forum,* 2001, pp. 103–18

C. Heard, D. Mansell, "The European Investigation Order: Changing the Face of Evidence-gathering in EU Cross-Border Cases", *NJECL*, Vol 2, Issue 4, 2011, pp.133-147

L. Kuhl, "The European Public Prosecutor's Office – more effective, equivalent and independent criminal prosecution against fraud?", *eucrim*, 2017/3, pp.135–143

A. Mangiaracina, "A new and controversial scenario in the gathering of evidence at the European level: the proposal for a Directive on the European Investigation Order", *Utrecht Law Rev*, 2014, 10, pp. 113–133

A. Mangiaracina, "L'acquisizione "europea" della prova cambia volto: l'Italia attua la Direttiva relativa all'ordine europeo di indagine penale*", Diritto penale e processo*, 2/2018 p. 169 ff

C. Palao Taboada, “El Derecho a no autoinculparse en el ámbito tributario: una revisión”, *Revista española de Derecho Financiero,* num.159/2013, pp.1-25

C. Rhoden, “Challenging Searches and Seizures of Computers at Home or in the Office: From reasonable Expectation of Privacy to Fruit of the Poisonous Tree Doctrine”, *American Criminal Law Journal,* 30, 2002-2003, pp. 107-134

L. Salazar, “Definitivamente approvato il Regolamento istitutivo della Procura Europea (EPPO)”, *Diritto Penale Contemporaneo*, 10/2017, pp. 328–333

T. Sánchez Núñez, “La jurisprudencia del Tribunal Constitucional sobre el uso de las nuevas tecnologías en la investigación penal”, in *Los nuevos medios de investigación en el proceso penal. Especial referencia a la vídeovigilancia, CGPJ, Cuadernos de Derecho Judicial,* Madrid, 2007, pp. 251-299

A. Steichen, “Le secret bancaire face aux autorités publiques nationales et étrangères”, *Bulletin Droit et Banque*, 24

D. Spielmann, “Le secret bancaire et l'entraide judiciaire internationale pénale au Grand-duché de Luxembourg”, Bruxelles, 1999

V. Mitsilegas, “The privatisation of mutual trust in Europe’s area of criminal justice: The case of e-evidence”, *Maastricht Journal of European and Comparative Law* 2018, Vol. 25(3), pp. 263–265

J. Vervaele, S. Gless, “Law Should Govern: Aspiring General Principles for Transnational Criminal Justice”, *Utrecht Law Rev.,* Vol 9, Issue 4, 2013, pp. 1-1

I. Zerbes, “Fragmentiertes Strafverfahren. Beweiserhebung und Beweisverwertung nach dem Verordnungsentwurf zur Europäischen Staatsanwaltschaft”, ZIS 3/2015, pp.145-155

**Reports**

E. Sellier, A. Weyembergh “Criminal procedural laws across the European Union – A comparative analysis of selected main differences and the impact they have over the

development of EU legislation" study for the European Parliament, LIBE Committee (PE 604.977), 2018

E. van der Does de Willebois et al., "The Puppet Masters: How the Corrupt Use Legal Structures to Hide Stolen Assets and What to Do About It", World Bank, 2011, available at https://openknowledge.worldbank.org/handle/10986/2363 License: CC BY 3.0 IGO."

Report of the General Council of the Judiciary to the draft law modifying Law 23/2014, 20 November, "On Mutual Recognition of Criminal Sentencing in the European Union"

T. Ramphal, PHD Thesis, Conflict of Laws in Judicial Cooperation in Criminal Matters between the Member States of the European Union: the case of the European Investigation Order Directive, defended 2018 in Leiden University.

**Other online resources**

Grey List of countries which are not compliant with OECD tax cooperation rules, available at https://www.oecd.org/tax/exchange-of-tax-information/42497950.pdf

Eurojust, Italian Desk, "L'ordine di indagine europea. Cosa è utile sapere? Domande e risposte", available at: http://eurocoord.eu/wp-content/uploads/2018/12/Eurojust-Desk-italiano.pdf

Website of the EJN *Status of implementation of the Directive on the European Investigation Order*