Provisional text

OPINION OF ADVOCATE GENERAL
ĆAPETA
delivered on 26 October 2023(1)

**Case C-670/22**

**Staatsanwaltschaft Berlin**
**v**
**M.N.**

(Request for a preliminary ruling from the Landgericht Berlin (Regional Court, Berlin, Germany))

(Reference for a preliminary ruling – Judicial cooperation in criminal matters – Directive 2014/41/EU – European Investigation Order – Article 6(1) – Conditions for issuing a European Investigation Order – Transfer of evidence already in the possession of another Member State – Concept of issuing authority – Article 2(c)(i) – Admissibility of evidence)

## I. Introduction

1. A European Investigation Order (EIO) is an EU instrument that enables cross-border cooperation in criminal investigations. It is regulated by the EIO Directive. (2) The present reference invites the Court, for the first time, to interpret that directive in a situation where an EIO was issued for the transfer of evidence already in the possession of another State.

2. For the purposes of a criminal investigation in Germany, the Generalstaatsanwaltschaft Frankfurt am Main (Public Prosecutor's Office, Frankfurt, Germany) issued several EIOs requesting the transfer of evidence gathered during a joint French-Dutch criminal investigation of EncroChat users. EncroChat was an encrypted telecommunications network offering its users near-perfect anonymity. (3)

3. The present reference results from one of the criminal proceedings initiated before the Landgericht Berlin (Regional Court, Berlin, Germany) against M.N. based on intercepted telecommunications data, transferred based on the abovementioned EIOs. The question that arose before the referring court is whether the EIOs were issued in breach of the EIO Directive, and if so, what consequences that may have for the use of such evidence in the criminal procedure.

## II. Facts, the questions referred and the procedure before the Court

4. At the origin of the criminal procedure in the main proceedings is a criminal investigation initiated in France and that continued as a joint operation between France and the Netherlands in which the location, traffic and communication data, including texts and images transmitted in ongoing chats of the EncroChat network users, were intercepted.

5. That joint operation developed a piece of Trojan software which was uploaded to the server in Roubaix (France) in the spring of 2020 and, from there, was installed on the terminal devices via a simulated update. The tribunal correctionnel de Lille (Criminal Court, Lille, France) authorised the operation for the gathering of communication data. EncroChat users in 122 countries were affected by that interception, including approximately 4 600 users in Germany.

6. During a video conference held on 9 March 2020, the European Union Agency for Criminal Justice Cooperation (Eurojust) provided information to countries concerning the surveillance measures planned by the French police and the intended transfer of data. The representatives of the Bundeskriminalamt (Federal Criminal Police Office, Germany) and the Frankfurt Public Prosecutor's Office signalled their interest in the data collection of the German users.

7. The Frankfurt Public Prosecutor's Office opened a preliminary investigation against unknown persons on 20 March 2020. The data collected by the French-Dutch investigation team were made available to, among others, German authorities via a European Union Agency for Law Enforcement Cooperation (Europol) server from 3 April 2020.

8. On 2 June 2020, within the framework of a German preliminary investigation against unknown persons, the Frankfurt Public Prosecutor's Office requested, by way of an EIO, authorisation from the French authorities to use the EncroChat data for criminal proceedings. That request was based on the suspicion of illicit trafficking in substantial quantities of narcotic drugs by persons who had not yet been identified. However, they were suspected of being part of an organised crime group in Germany which used EncroChat phones. The Criminal Court, Lille authorised the EIO for the transmission and judicial use of the EncroChat data of the German users. Additional data were subsequently transmitted based on two supplementary EIOs of 9 September 2020 and 2 July 2021 respectively.

9. Based on the evidence received, the Frankfurt Public Prosecutor's Office separated the investigations to be conducted in respect of individualised EncroChat users and assigned them to local public prosecutor's offices. The Staatsanwaltschaft Berlin (Public Prosecutor's Office, Berlin, Germany) then charged the accused in the present case with several counts of illicit trafficking of substantial quantities of narcotic drugs and illegal possession of substantial quantities of narcotic drugs in Germany.

10. That criminal procedure is currently pending before the referring court. Even if that is not clearly explained in the order for reference, it seems that in those proceedings the question arose whether the EIOs issued by the Frankfurt Public Prosecutor's Office were issued in breach of the EIO Directive and, if so, whether they should be excluded as evidence in the criminal procedure against the accused.

11. In light of those facts, the referring court submitted the following questions to the Court of Justice for a preliminary ruling:

'(1) Interpretation of the concept of "issuing authority" under Article 6(1) of [the EIO Directive], in conjunction with Article 2(c) thereof …

(a) Must an [EIO] for obtaining evidence already located in the executing State (*in casu*: France) be issued by a judge where, under the law of the issuing State (*in casu*: Germany), the underlying gathering of evidence would have had to be ordered by a judge in a similar domestic case?

(b) In the alternative, is that the case at least where the executing State carried out the underlying measure on the territory of the issuing State with the aim of subsequently making the data

gathered available to the investigating authorities in the issuing State, which are interested in the data for the purposes of [a] criminal prosecution?

(c) Does an EIO for obtaining evidence always have to be issued by a judge (or an independent authority not involved in criminal investigations), irrespective of the national rules of jurisdiction of the issuing State, where the measure entails serious interference with high-ranking fundamental rights?

(2) Interpretation of Article 6(1)(a) of [the EIO Directive]

(a) Does Article 6(1)(a) of [the EIO Directive] preclude an EIO for the transmission of data already available in the executing State ([*in casu*:] France), obtained from the interception of telecommunications, in particular traffic and location data and recordings of the content of communications, where the interception carried out by the executing State covered all the users subscribed to a communications service, the EIO seeks the transmission of the data of all terminal devices used on the territory of the issuing State and there was no concrete evidence of the commission of serious criminal offences by those individual users either when the interception measure was ordered and carried out or when the EIO was issued?

(b) Does Article 6(1)(a) of [the EIO Directive] preclude such an EIO where the integrity of the data gathered by the interception measure cannot be verified by the authorities in the executing State by reason of blanket secrecy?

(3) Interpretation of Article 6(1)(b) of [the EIO Directive]

(a) Does Article 6(1)(b) of [the EIO Directive] preclude an EIO for the transmission of telecommunications data already available in the executing State ([*in casu*:] France) where the executing State's interception measure underlying the gathering of data would have been impermissible under the law of the issuing State ([*in casu*:] Germany) in a similar domestic case?

(b) In the alternative: does this apply in any event where the executing State carried out the interception on the territory of the issuing State and in its interest?

(4) Interpretation of Article 31(1) and (3) of [the EIO Directive]

(a) Does a measure entailing the infiltration of terminal devices for the purpose of gathering traffic, location and communication data of an internet-based [communications] service constitute interception of telecommunications within the meaning of Article 31 of [the EIO Directive]?

(b) Must the notification under Article 31(1) of [the EIO Directive] always be addressed to a judge, or is that the case at least where the measure planned by the intercepting State ([*in casu*:] France) could be ordered only by a judge under the law of the notified State ([*in casu*:] Germany) in a similar domestic case?

(c) In so far as Article 31 of [the EIO Directive] also serves to protect the individual telecommunications users concerned, does that protection also extend to the use of the data for criminal prosecution in the notified State ([*in casu*:] Germany) and, if so, is that purpose of equal value to the further purpose of protecting the sovereignty of the notified Member State?

(5) Legal consequences of obtaining evidence in a manner contrary to EU law

(a) In the case where evidence is obtained by means of an EIO which is contrary to EU law, can a prohibition on the use of evidence arise directly from the principle of effectiveness under EU law?

(b) In the case where evidence is obtained by means of an EIO which is contrary to EU law, does the principle of equivalence under EU law lead to a prohibition on the use of evidence where the measure underlying the gathering of evidence in the executing State should not have been ordered in a similar domestic case in the issuing State and the evidence obtained by means of such an unlawful domestic measure could not be used under the law of the issuing State?

(c) Is it contrary to EU law, in particular the principle of effectiveness, if the use in criminal proceedings of evidence, the obtaining of which was contrary to EU law precisely because there was no suspicion of an offence, is justified in a balancing of interests by the seriousness of the offences which first became known through the analysis of the evidence?

(d) In the alternative: does it follow from EU law, in particular the principle of effectiveness, that infringements of EU law in the obtaining of evidence in national criminal proceedings cannot remain completely without consequence, even in the case of serious criminal offences, and must therefore be taken into account in favour of the accused person at least when assessing evidence or determining the sentence?'

12. Written observations were submitted by the Berlin Public Prosecutor's Office, the German, Estonian, French, Netherlands, Polish and Swedish Governments and Ireland, as well as the European Commission.

13. A hearing was held on 4 July 2023 where M.N., the Berlin Public Prosecutor's Office, the Czech, German, Spanish, French, Hungarian, Netherlands and Swedish Governments and Ireland, as well as the Commission presented oral argument.

## III. Analysis

### *A. Preliminary remarks*

14. Challenges against criminal convictions resulting from the intercepted EncroChat data are making waves across the highest courts in Europe, (4) the Court of Justice being no exception in that regard.

15. Most of those cases challenge the interception measures undertaken by France. Even if such a question is obviously relevant in the criminal procedures that were initiated based on evidence gathered by such an interception, it is important to clarify that the present reference is not about the validity of the French interception measures.

16. Rather, the present case is about the possible incompatibility of the EIOs issued by the Frankfurt Public Prosecutor's Office with the EIO Directive and the consequences of such a finding. Those EIOs were not the trigger for the French measures of interception of telecommunications among EncroChat users. The interceptions happened independently of the EIOs at issue. The legal challenge against those interception measures is a matter for the competent French courts.

17. The EIOs that are at issue in the present case did not seek to gather data in France through the interception of telecommunications, but only requested the transfer of the evidence already gathered by the interception in France.

18. That set of facts must be properly characterised under the EIO Directive. Namely, Article 1(1) of the EIO Directive provides that an EIO may be issued, first, 'to have one or several specific investigative measure(s) carried out in another Member State', and second, 'for obtaining evidence that is already in the possession of the competent authorities of the executing State'. (5)

19. Simply put, an EIO may be issued either for gathering new evidence or for transferring existing evidence. I will use that terminology to refer to the two different types of an EIO.

20. In the main proceedings, the EIOs were issued for the latter purpose: the Berlin Public Prosecutor's Office sought the transfer of evidence that France already had in its possession.

21. However, it follows clearly from the order for reference that the referring court, first, considers that despite the distinction between the two types of EIO in Article 1(1) of the EIO Directive, an EIO for the transfer of existing evidence cannot be issued without taking into consideration how that evidence was originally gathered. Secondly, the referring court questions the proportionality, and therefore the legality, of the original measures of gathering the evidence in France that was later transferred to Germany. Finally, the referring court disagrees with the German Federal Court of Justice, (6) which found that the intercepted EncroChat data could be used as evidence in Germany. (7)

22. Bearing that in mind, the Court must clarify whether the conditions for issuing an EIO for the transfer of existing evidence require the assessment of the underlying measures of gathering evidence in the executing State. I would like to make it clear from the outset, and I will elaborate upon this later, that in such a scenario, the issuing authority cannot question the legality of the measures by which the executing State gathered evidence. The proportionality of the French measure ordering the interception of EncroChat phones is therefore not what this case is about.

### *B. Reorganising the questions of the referring court and the structure of the Opinion*

23. The referring court considers that the EIOs were issued contrary to the EIO Directive, because (i) they were in breach of the conditions set out by Article 6(1) thereof and (ii) they were issued by a public prosecutor and not by a court. Additionally, the French authorities should have, according to Article 31 of the EIO Directive, notified the competent German court of the interception measures. Finally, that court considers that EU law, more specifically the principles of equivalence and effectiveness, should be interpreted so as to prohibit the use, in the criminal procedure, of evidence gathered in breach of the EIO Directive.

24. Thus, the referring court in essence asks whether its understanding of the EIO Directive and the consequences that follow therefrom are correct. It organised its questions into five groups, which I have reorganised for the purpose of my analysis, as follows.

25. The first three groups of questions focus on the interpretation of the competent issuing authority of an EIO for the transfer of existing evidence and the conditions which govern the issuing of such an EIO. The questions on the conditions as stated in Article 6(1)(a) and (b) of the EIO Directive are intertwined with those about the competent issuing authority. I will therefore deal with them together under heading C.

26. The fourth group of questions, seeking the interpretation of Article 31(1) and (3) of the EIO Directive, may be dealt with separately. I shall do this under heading D.

27. Finally, I will analyse the last group of questions, relating to the consequences of a possible breach of the EIO Directive, under heading E. Those questions may be characterised as hypothetical if no breach of the EIO Directive results from the answers given to the preceding questions. However, given that that conclusion depends on the interpretation of the relevant national law, which it is for the referring court to do, I propose that the Court also answer those questions.

### *C. Conditions for issuing an EIO for the transfer of existing evidence and the competent issuing authority*

28. The conditions which the issuing authority must assess for issuing an EIO (8) are set out in Article 6(1) of the EIO Directive. That provision reads:

> 'The issuing authority may only issue an EIO where the following conditions have been met:

(a) the issuing of the EIO is necessary and proportionate for the purpose of the proceedings referred to in Article 4 taking into account the rights of the suspected or accused person; and

(b) the investigative measure(s) indicated in the EIO could have been ordered under the same conditions in a similar domestic case.'

29. The EIO Directive thus imposes two conditions for issuing an EIO. Those conditions aim to ensure that the EIO is not issued in contravention of the law of the issuing State. (9) As the criminal investigation or the subsequent criminal procedure takes place in the issuing State, those conditions are ultimately aimed at protecting the rights of the accused or suspected persons. Compliance with those conditions may, under Article 14(2) of the EIO Directive, be challenged exclusively in the issuing State.

30. To achieve those aims, Article 6(1) of the EIO Directive demands from the issuing authority an abstract and a concrete assessment.

31. The abstract assessment is provided in Article 6(1)(b) of the EIO Directive and requires that the issuing authority determine whether the investigative measure which will be the object of an EIO exists in its national law and under which conditions it may be ordered.

32. The concrete assessment in Article 6(1)(a) of the EIO Directive imposes an obligation on the issuing authority to determine whether a particular EIO is necessary and proportionate for the purposes of a concrete criminal procedure.

33. Only after the issuing authority has, under Article 6(1)(b) of the EIO Directive, determined that national law in principle allows for a certain investigative measure may it turn to the concrete case before it and conduct the necessity and proportionality assessment under Article 6(1)(a) of the EIO Directive. I therefore find it more logical to explain those two conditions in reverse order.

34. Both the abstract and the concrete conditions are connected with the question of how to define which authority is competent to issue an EIO in a concrete case. The referring court considers that the public prosecutor was not, in the circumstances of the present case, the authority competent to issue the EIOs for the transfer, from France, of evidence consisting of intercepted telecommunication data.

35. Article 2(c) of the EIO Directive sets out which authorities can issue an EIO. The relevant provision reads:

'"issuing authority" means:

(i) a judge, a court, an investigating judge or a public prosecutor competent in the case concerned;' (10)

36. Article 2(c)(i) of the EIO Directive thus enumerates authorities which may autonomously, without any additional authorisation, issue an EIO. Unlike the EAW Framework Decision, (11) the EIO Directive explicitly lists public prosecutors among such authorities. (12) Thus, in contrast to the EAW Framework Decision, in *Staatsanwaltschaft Wien (Falsified transfer orders)*, the Court held that a public prosecutor may be an issuing authority of an EIO even if it is not entirely independent from the executive. (13)

37. However, that principled empowerment of public prosecutors does not mean that they are the competent issuing authority in each case. Instead, that will depend on the circumstances of the case and is connected to the conditions imposed by Article 6(1) of the EIO Directive. Therefore, I will assess not only *what* those conditions require from an issuing authority, but also how they influence *which* authority that may be.

### *1. Article 6(1)(b) of the EIO Directive and a similar domestic case*

38. Article 6(1)(b) of the EIO Directive requires that an EIO be issued on the condition that the investigation measure is available *under the same conditions in a similar domestic case*.

39. It is, therefore, necessary to interpret what a similar domestic case is if an EIO is issued for the transfer of existing evidence.

40. A preliminary remark is due before interpreting the term 'similar domestic case'. That issue arose and was discussed by participants to this procedure because of the position of the Federal Court of Justice, (14) according to which Article 6(1)(b) of the EIO Directive does not apply at all to an EIO for the transfer of existing evidence. According to that court, the transfer of evidence is not an investigative measure as such, and is thus outside the scope of that provision.

41. I disagree with that view: Article 6(1)(b) of the EIO Directive sets out the conditions for issuing an EIO without distinguishing between the two types of measure mentioned in Article 1 of the EIO Directive. Its wording does not exclude the investigative measures requesting the transfer of already existing evidence from its scope. Article 6(1)(b) of the EIO Directive therefore also applies to an EIO issued for the purpose of the transfer of existing evidence, as in the present case. (15)

42. A similar domestic case relevant for assessing whether an EIO may be issued differs depending on whether an EIO is issued for gathering new evidence or for transferring evidence that already exists. Therefore, as suggested by the Commission, the Berlin Public Prosecutor's Office, and the German Government, a similar domestic case is one where evidence is transferred from one criminal procedure to another within Germany (for example, from the Public Prosecutor's Office in Munich to its Berlin counterpart).

43. Such an interpretation is confirmed by the wording of Article 6(1)(b) of the EIO Directive which states that 'the investigative measure(s) *indicated in the EIO*' (16) are those that the authority must be able to order domestically. In the present case, the measure indicated in the EIOs is the transfer of evidence already in the possession of French authorities.

44. Whether it is possible to transfer evidence consisting of intercepted communication gathered for one criminal investigation or procedure to another is a matter of German law. That is not an issue that is resolved by the EIO Directive itself; rather, that directive refers to the law of the issuing State.

45. Do the underlying measures through which the evidence was gathered in France play any role in this assessment?

46. To the extent that national law sets conditions on the transfer of evidence between criminal procedures, the underlying measure may become relevant. If, for example, German law would prohibit a domestic transfer of intercepted telecommunications from one criminal case to another, the issuing authority would likewise be prevented from ordering such a cross-border transfer.

47. However, that does not seem to be the case in the present proceedings. At the hearing, the German Government confirmed that the transfer of evidence between two criminal procedures is possible under German law, including evidence gathered through the interception of communications. The conditions of such a transfer are provided for in the German Strafprozessordnung (Code of Criminal Procedure; 'the StPO'). It is for the referring court to interpret German law to determine whether this is indeed the case. (17)

48. However, the issuing authority is not required by the EIO Directive – rather, it is even precluded – to assess whether the underlying measures through which the evidence was gathered were legally undertaken in the executing Member State. When issuing an EIO for the transfer of existing evidence, the issuing authority is bound by the principle of mutual recognition, which underpins cooperation in criminal matters in the European Union. Unless the underlying measures are found to be illegal in judicial

proceedings in France, which the person concerned must be able to initiate, (18) the issuing authority is not in a position to question their legality.

49. M.N. argued that distinguishing between the transfer of evidence and the measures through which they were gathered allows for the circumvention of the protection of suspects or accused persons under the law of the issuing State. In his view, the German authorities turned to their French counterparts to obtain evidence contrary to German law.

50. The circumstances of the present case do not lead to the suspicion of an abuse of cross-border investigation procedures. France gained possession of the evidence at issue in the course of its own criminal investigation. Even if that evidence happened to be of interest to Germany as well, France did not commence gathering it for the purposes of the German criminal investigation. Thus, even if it were true that a German judge would not authorise such an interception if it were to be undertaken in Germany, the French authorities have undertaken such measures in conformity with French law and with the authorisation of a competent French court.

51. Although criminal law systems of Member States differ significantly, (19) it does not mean that one system protects the fundamental rights of suspects and accused persons while another breaches them. Rather, EU judicial cooperation in criminal matters relies on the assumption that all Member States respect fundamental rights. While that assumption may be overturned in a particular case before the competent court, that cannot call into question the principle of mutual trust underlying the EIO and other instruments of cooperation in criminal matters.

52. Therefore, under Article 6(1)(b) of the EIO Directive, the issuing authority needs to check whether, within Germany, the data gathered by the interception of telecommunications for the purposes of one criminal procedure may be transferred to another criminal procedure. If that is so, that authority may issue an EIO for the transfer of evidence gathered by the interception of telecommunications in another EU Member State. When issuing such an EIO, the issuing authority may not question the legality of the measures through which evidence was gathered in the executing Member State.

53. Finally, in its alternative Question 3(b), the referring court asks whether it is of relevance that the interception undertaken by the executing State included data on mobile phones of users in Germany, or the fact that such an interception was in the interest of criminal prosecutions in that State. I am of the view that those circumstances, even if correct, are of no relevance for the interpretation of Article 6(1)(b) of the EIO Directive.

54. First, the fact that the interception took place in respect of mobile phones of users on German territory is of no relevance to the applicability of Article 6(1)(b) of the EIO Directive: regardless of where the evidence was collected, in order for it to be transferred from France to Germany by way of an EIO, it is necessary to comply with the German rules applicable to a similar domestic case.

55. Second, the assumption that the French authorities intercepted the communication in the interest of Germany is a factual assumption unsubstantiated in the order for reference and one that the Court is not able to make conclusions on; more importantly, nothing in Article 6(1)(b) of the EIO Directive leads to the conclusion that the interest of the issuing State is relevant for its interpretation.

*Interim conclusion*

56. When an EIO is issued for the transfer of evidence already in the possession of another State, the reference to a similar domestic case under Article 6(1)(b) of the EIO Directive requires the issuing authority to establish whether and under what conditions the relevant national law allows for a transfer of evidence gathered through the interception of communication between criminal procedures domestically.

57. When deciding whether it can issue an EIO for the transfer of existing evidence, the issuing authority cannot assess the legality of the underlying gathering of evidence in the executing State whose

transfer it requires by an EIO.

58. The fact that the underlying measures were undertaken on the territory of the issuing State, or were in the interest of that State, does not influence the preceding answer.

### *2. Article 6(1)(b) of the EIO Directive and the competent issuing authority*

59. The referring court considers that the EIOs in the present case should have been issued by a court, rather than by a public prosecutor. In that respect, the referring court asks, first, whether such a conclusion flows from the combined reading of Article 2(c)(i) and Article 6(1)(b) of the EIO Directive and, second, whether the fact that the French authorities intercepted mobile phones on German territory influences the answer to that question.

60. The Court has already explained that Article 6(1)(b) of the EIO Directive is indeed relevant for determining the competent issuing authority in a particular case. In *Spetsializirana Prokuratura (Traffic and location data)*, the Court connected Article 2(c)(i) of the EIO Directive to Article 6(1)(b) thereof. (20) It explained that an EIO must be issued by a court if so required by the law of the issuing Member State concerning the same measure in a domestic context. (21) In such a case, a court is the *competent* issuing authority despite the public prosecutor being mentioned in Article 2(c)(i) of that directive. (22)

61. In short, a public prosecutor may be an issuing authority in principle, but the national law applicable in a similar domestic case determines the issuing authority competent in a concrete case.

62. Taking into account my preceding analysis of what is to be understood as a similar domestic case under Article 6(1)(b) of the EIO Directive when an EIO is issued for the transfer of existing evidence, the EIO should have been issued by a court if German law requires it in a domestic transfer of the intercepted telecommunications data.

63. Thus, to determine the competent issuing authority, it is irrelevant whether, under German law, a court would have to authorise the interception measures. One only needs to ask whether a court would need to authorise a similar domestic transfer. That does not seem to be the case under German law.

64. That being said, an important concern remains. Had the transfer of existing evidence happened internally, from one public prosecutor to another (for example, from Munich to Berlin), the underlying measure of interception of telecommunications would have been, under German law, ordered by a court. Thus, the proportionality of the interference with fundamental rights would have been controlled by a court. That makes it acceptable, from the point of view of the protection of rights of suspects and accused persons, to allow the use of that evidence in another criminal procedure without yet again involving a court.

65. However, when the underlying measure is governed by a different legal system, a rule that does not require judicial control of the transfer of existing evidence operates in a different, unfamiliar context. (23)

66. Nevertheless, in the present case, the interception of telecommunications was authorised by French courts. (24) The principle of mutual recognition, on which the EIO system is based, requires that German authorities attribute to that procedural step the same value as they would domestically. That is so, even if in a concrete case a German court would decide differently.

67. However, what if French law did not require a judicial authorisation of the interception measures? At the hearing, the Commission stated that the situation would be different in such a case, alleging in this way that the EIO requesting the transfer of existing evidence might be considered contrary to EU law had the French courts not authorised the underlying measure. That would suggest that Article 6(1)(b) of the EIO Directive is not entirely indifferent to the underlying measure when an EIO is issued for the transfer of existing evidence.

68. When national law empowers a public prosecutor to request the transfer of evidence because the original collection of that evidence was authorised by a court, in my opinion that national rule becomes relevant under Article 6(1)(b) of the EIO Directive. That means that the issuing authority must verify whether the underlying measure received judicial authorisation as required under national law. However, the issuing authority would not be able to question the quality of such an authorisation, but would instead be required to accept the judicial authorisation in the executing State in the same way as it would a domestic one.

69. However, if the executing State did not involve a court in authorising the underlying measure, whereas the issuing State would require it in a similar domestic case, that latter State may require a judicial authorisation for issuing an EIO for the transfer of existing evidence. That is the case even if it does not require such an authorisation in an internal transfer of evidence.

70. In the present case, all the steps taken in order to gather data via the EncroChat server in France were authorised by competent French courts. (25) I therefore see no reason why a German public prosecutor would not be able to issue an EIO for the transfer of that evidence.

71. The referring court asks an alternative Question 1(b), which relies on the premiss that the German authorities triggered the gathering of the data by France in the interest of Germany, which took place on German territory. (26)

72. That question is hypothetical in part, as the gathering of evidence was a French initiative undertaken for the purpose of its own investigation. The discovery of the German EncroChat users was the consequence of, and not the reason for, the interception of telecommunications.

73. The circumstance that some EncroChat users were on German territory has, in my view, no relevance to the concept of an issuing authority. Because an EIO can only be issued for measures that are available in a similar domestic case, the same national rules concerning the issuing authority apply regardless of where the investigative measure was carried out and by whom. The only difference is whether an EIO or a domestic investigation order will be used. (27)

*Interim conclusion*

74. When an underlying measure in the executing State was authorised by a judge, an EIO for the transfer of such evidence does not need to be issued by a judge as well, even if under the law of the issuing State the underlying gathering of evidence would have to be ordered by a judge.

75. The fact that the interception has been carried out on the territory of another Member State does not make any difference when determining the issuing authority.

### *3. Article 6(1)(a) of the EIO Directive and proportionality*

76. According to Article 6(1)(a) of the EIO Directive, an EIO must be necessary and proportionate for the purposes of the criminal proceedings, taking into account the rights of the suspected or accused person. (28)

77. That proportionality assessment is guided by both EU law and the law of the issuing State. (29)

78. The issuing authority must be satisfied that the EIO is necessary and proportionate in the light of the circumstances that are present at the moment when the EIO was issued. In that respect, M.N. is right in arguing that for the assessment of proportionality of an EIO it is most certainly irrelevant whether the criminal investigation was very successful and resulted in numerous convictions for serious crimes.

79. The relevant question is, rather, whether the level of intrusion into private lives, entailed in the access of the public prosecutor to the transferred evidence, may be justified by the importance of the public

interest in the criminal investigation or procedure at issue, taking into consideration the circumstances of the particular case.

80. In that respect, in its case-law relating to the ePrivacy Directive, (30) the Court held that access of public authorities to traffic and location data always represents a serious interference with the private lives of the persons concerned. (31)

81. Whilst the ePrivacy Directive does not apply as such to the case at hand, (32) the findings concerning the serious interference with fundamental rights caused by access to traffic and location data is relevant also for the present case: the access of the German public authorities to communication data transferred from France may be characterised as a serious interference with fundamental rights. However, even a serious interference may be justified by a commensurately important public interest. (33)

82. That interest may be assessed only by the issuing authority (or the reviewing national court under Article 14(2) of the EIO Directive) in light of all the circumstances of the case, which is governed primarily by national law. (34) As I have already explained, the relevant national law is that regulating the transfer of evidence from one criminal procedure to another.

83. The Court cannot replace the issuing authority or the reviewing national court in the proportionality assessment of a concrete EIO. Besides having no competence to do so, the Court also lacks the full knowledge of all the relevant laws and facts surrounding a particular criminal investigation. Therefore, it is not for the Court to decide whether it is disproportionate to order the transfer of data of all EncroChat users in Germany if there was no concrete evidence of the crimes committed.

84. By its Question 2(b), the referring court asks whether the secrecy of the method of interception of data should be taken into consideration in the proportionality assessment, where the integrity of the data gathered cannot be verified by the authorities in the issuing State.

85. To my mind, the secrecy might indeed influence the possibility of defence of the suspect or accused persons. That, however, is relevant for the admissibility of evidence, addressed in the fifth group of questions of the referring court.

*Interim conclusion*

86. The assessment of the necessity and proportionality of an EIO requesting the transfer of the existing evidence is a matter for the issuing authority, with a possibility of review by the competent national court. Such an assessment must take into consideration that the access of the national authority to the intercepted communication data represents a serious interference with the private lives of the persons concerned. That interference must be counterbalanced by a serious public interest in the investigation and prosecution of crimes.

### *4. Does EU law require that proportionality be assessed by a court in cases of serious interference with fundamental rights?*

87. By its Question 1(c), the referring court asks whether EU law, notwithstanding the applicable national law, requires a court to authorise the access of a public prosecutor to evidence acquired by the interception of communications.

88. The referring court suggests that issuing an EIO for the transfer of evidence that consists in the intercepted telecommunications always requires a judicial authorisation. That court referred to the judgment in *Prokuratuur*.

89. In that judgment, the Court found that enabling the access of public authorities to data retained by telecommunications service providers requires the prior authorisation of a court or another impartial body. (35) The Court relied on the compelling argument of its Advocate General, (36) according to which a

public prosecutor's office, which is a party to a criminal procedure, cannot be considered impartial. For that reason, it is questionable whether such a body can perform the proportionality analysis without putting the interests of the prosecution ahead of the interests of the privacy and data protection of suspects and accused persons.

90. Given that Article 6(1)(a) of the EIO Directive also requires that an EIO be proportionate, one may ask whether, following the logic of *Prokuratuur*, a public prosecutor can ever be entrusted to carry out such a proportionality analysis.

91. The EIO Directive left the appraisal of whether a public prosecutor can issue an EIO to national legal orders. That makes sense given the differences in the organisation of criminal justice systems in the Member States. That appraisal by national legal orders entails the question whether a public prosecutor can undertake an impartial proportionality assessment. If being a party to the criminal proceedings would make it inappropriate for a public prosecutor to issue an EIO, Article 2(c)(i) of the EIO Directive would be rendered meaningless.

92. The referring court, however, wanted to suggest that EU law should step in and require a judicial authorisation only when measures entail serious interference with fundamental rights. That was indeed the situation in *Prokuratuur* and in other cases relating to the ePrivacy Directive.

93. The short answer is that the ePrivacy Directive and the pertinent case-law do not apply in the present situation. They are relevant only when telecommunications service providers are required by national law to retain traffic and location data associated with telecommunications and when public authorities require access to the data thus retained. When interception is performed directly by the Member States without any obligations being imposed on telecommunications service providers, the ePrivacy Directive does not apply, but national law does. (37)

94. However, if we dig deeper into the logic of the judgment in *Prokuratuur*, as was suggested by the referring court, we may nevertheless ask ourselves why it is that the Court found that by the nature of its functions, a public prosecutor is not in a position to conduct an impartial proportionality assessment when it comes to requesting access to telecommunications data from network service providers.

95. In the context of the ePrivacy Directive, the data accessed by a public prosecutor are always those in the possession of telecommunications operators which, under national law, are required to retain traffic and location data of the general population. The data thus retained are not the matter of a specific case, but rather of mass surveillance. The request for access by a public prosecutor for the purposes of a concrete criminal investigation is the first occasion in which individual circumstances may be taken into consideration. Therefore, it was justified to require that a court assess the proportionality of that access, as the involvement of a court is necessary in order to prevent the abuse of accessing massively and generally retained data.

96. That distinguishes the findings in the judgment in *Prokuratuur* from the situation in the present case. Here, the data to be transferred are not indiscriminately gathered from the entire population but for the purposes of a concrete criminal investigation in France. In that first step which made those data available, the gathering of those data was under the control of a court.

97. Therefore, the level of intrusion into fundamental rights of privacy and data protection, which triggered the judgment in *Prokuratuur*, is not the same as the level of intrusion in the scheme of the present case. The data, the transfer of which was requested by the three EIOs issued by the Frankfurt Public Prosecutor's Office, were limited only to EncroChat users in Germany in the context in which a suspicion existed that this service is used predominantly for committing criminal offences.

98. That is not to say that the intrusion into the private life of those individuals is not important. However, it is still not comparable to the mass surveillance of the general population.

99. Apart from obliging the issuing authority to undertake and explain its proportionality assessment, the EIO Directive provides further safeguards. If public prosecutors breach fundamental rights, Article 14(1) of the EIO Directive requires that Member States ensure legal remedies equivalent to those available in a similar domestic case. Therefore, the suspect or accused person should be able to challenge the proportionality assessment made by the public prosecutor when issuing an EIO for the transfer of evidence. (38) That is not the case in the context of the ePrivacy Directive.

100. Finally, I should like briefly to discuss the relevance of the Law Enforcement Directive (39) for determining the issuing authority. That question arose because the Court, in its judgment in *La Quadrature du Net*, explained that the ePrivacy Directive does not apply to the direct interception of data; instead, national law applies 'subject to the application of [the Law Enforcement Directive]'. (40) The question is, therefore, whether the obligation that a court issue an EIO for the transfer of existing evidence, when the evidence consists in the intercepted data, follows from the Law Enforcement Directive.

101. The Law Enforcement Directive, which protects personal data in the sphere of criminal investigations, can indeed be applied to the circumstances of this case. (41) Nevertheless, in my view, that directive does not contain any rule that would enable the Court to conclude that EU law imposes the obligation on Member States to ensure a prior judicial authorisation of direct access by the public prosecutor to data obtained through the interception of communications.

102. That directive governs the obligations of public authorities that act as data controllers, which are required, among other things, to undertake a proportionality assessment, (42) but does not determine which authorities that may be.

*Interim conclusion*

103. EU law does not require that an EIO for the transfer of existing evidence gathered through the interception of telecommunications be issued by a court, if national law provides that a public prosecutor may order such a transfer in a similar domestic case.

### *D. Article 31 of the EIO Directive and the notification requirement*

104. By its fourth group of questions, the referring court asks whether the interception of communication carried out by the French authorities should have been subject to the obligation of notification under Article 31 of the EIO Directive. If so, the referring court also asks whether such a notification should have been addressed to a judge, given that only a judge could have authorised the interception of communication under German law.

105. The relevant parts of Article 31 of the EIO Directive provide as follows:

> '1. Where, for the purpose of carrying out an investigative measure, the interception of telecommunications is authorised by the competent authority of one Member State (the "intercepting Member State") and the communication address of the subject of the interception specified in the interception order is being used on the territory of another Member State (the "notified Member State") from which no technical assistance is needed to carry out the interception, the intercepting Member State shall notify the competent authority of the notified Member State of the interception:
>
> (a) prior to the interception in cases where the competent authority of the intercepting Member State knows at the time of ordering the interception that the subject of the interception is or will be on the territory of the notified Member State;
>
> (b) during the interception or after the interception has been carried out, immediately after it becomes aware that the subject of the interception is or has been during the interception, on the territory of the notified Member State.

2. The notification referred to in paragraph 1 shall be made by using the form set out in Annex C.

…’

106. Article 31 of the EIO Directive concerns situations where one Member State conducts the interception of telecommunications on the territory of another Member State, without the need for any technical assistance of the latter State. (43)

107. That provision serves two purposes. First, as a continuation of international comity from previous mutual legal assistance arrangements, (44) the role of the obligation of notification is to strengthen mutual trust among the participants of the area of freedom, security and justice. (45) Second, the role of the notification is to enable the notified Member State to protect the fundamental rights of individuals on its territory. (46)

108. Article 31 of the EIO Directive applies to a situation where a cross-border measure is in operation, albeit without an EIO, because it is being carried out unilaterally by one Member State. (47)

109. That interpretation follows from the wording of Article 31 of the EIO Directive, which does not mention an EIO being issued at all, unlike Article 30 thereof. Equally, Article 31 does not use the expressions ‘issuing’ and ‘executing’, but rather the ‘intercepting’ and ‘notified’ Member States. (48)

110. To my mind, that provision aims precisely at situations such as the interception by France of telecommunications data on mobile phones in Germany in the context of the French criminal investigation. Therefore, France should have informed the German authorities as soon as it realised that part of the intercepted data originated from mobile phones in Germany. (49)

111. Which German authority should France have notified? The EIO Directive does not impose an obligation on the Member States to flag the national authority competent to receive such notifications, as it does in some other situations. (50) Therefore, the intercepting State cannot know which body is competent to receive such a notification in the notified Member State.

112. Thus, France was not under an obligation to notify a competent German court, but could have also notified, for instance, a public prosecutor. It falls to the notified Member States to receive such notification and forward it to the competent authority under national law.

*Interim conclusion*

113. A Member State which, in the course of its unilateral criminal investigation or procedure, intercepts telecommunications on the territory of another Member State must notify that other State of the interception.

114. That notification may be submitted to any authority that the intercepting Member State considers appropriate, as that State cannot know which authority is competent in a similar domestic case.

115. Article 31 of the EIO Directive has a purpose to protect both the individual telecommunications users concerned and the sovereignty of the notified Member State.

### *E. Admissibility of evidence*

116. By its fifth group of questions, the referring court asks, in essence, whether the finding that an EIO was issued contrary to the requirements of the EIO Directive results in the inadmissibility of that evidence in the criminal procedure in the issuing Member State. That court relies on the principles of equivalence and effectiveness. The latter is invoked in a way that if the evidence obtained contrary to the EIO Directive were nevertheless used in the issuing State, it would damage the effectiveness of that directive.

117. The answer to this group of questions can be short: EU law does not govern the admissibility of evidence in criminal procedures.

118. Although the European Union is empowered under Article 82(2)(a) TFEU to introduce minimum harmonisation of the mutual admissibility of evidence, this has not yet happened. (51)

119. The only mention of assessing the evidence obtained through an EIO is made in the second sentence of Article 14(7) of the EIO Directive: '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.' (52)

120. At the hearing, when asked whether that provision has any bearing on the rules on the admissibility of evidence in the Member States, the Commission stated that to make such a conclusion would be going too far. It explained that that sentence merely provides a reminder that the rights protected by Articles 47 and 48 of the Charter of the Fundamental Rights of the European Union ('the Charter') need to be respected. I tend to agree with such an interpretation, which acknowledges that the EU political process is currently not moving forward with regard to the regulation of the admissibility of evidence.

121. To the best of my knowledge, the closest that EU law has come to regulating the admissibility of evidence is Article 37(1) of the EPPO Regulation: (53) 'Evidence presented by the prosecutors of the EPPO or the defendant to a court shall not be denied admission on the mere ground that the evidence was gathered in another Member State or in accordance with the law of another Member State.'

122. However, that provision merely tells us that evidence should not be dismissed *because* it was collected abroad or under the law of another Member State; it does not provide further constraints on the national judge in how he or she is to assess admissibility of evidence.

123. The same approach may be found in the case-law of the ECtHR. That court clearly stated that admissibility of evidence is a matter of national law, (54) whereas in assessing the possible infringement of Article 6 ECHR, 'the Court … will look at the proceedings as a whole, having regard to the rights of the defence but also to the interests of the public and the victims that crime is properly prosecuted and, where necessary, to the rights of witnesses'. (55)

124. While the literature is critical of the insufficiency of such a standard, in particular in the light of the differences between procedural laws of Member States, (56) that does not change the fact that currently admissibility of evidence is not regulated at EU level.

125. In sum, in the present state of development of EU law, the question whether evidence obtained in breach of domestic or EU law is admissible is governed by the laws of Member States.

126. The consequences of possibly not complying with the conditions for issuing an EIO in the EIO Directive are few and far between: Article 6(3) of the EIO Directive provides that if the executing authority believes that Article 6(1) thereof was not complied with, it may consult the issuing authority on the importance of executing an EIO and, after such a consultation, the issuing authority may decide to withdraw the EIO.

127. In conclusion, the issue of the admissibility of evidence is, for the time being, a matter of national law. However, in matters where EU law applies, the relevant national provisions must not infringe Articles 47 and 48 of the Charter. (57)

128. The procedural principles of equivalence and effectiveness apply to situations where EU law grants to individuals rights without remedies. Member States must ensure that an EU right may be achieved under the same conditions as a comparable domestic right, and the applicable procedural rules should not make the enforcement of such rights virtually impossible. (58)

129. However, there is no right in relation to the (in)admissibility of evidence granted to individuals on the basis of EU law. The principles of equivalence and effectiveness have no application.

130. Finally, even if the inadmissibility of evidence as a consequence of an infringement of the EIO Directive (arguably) might increase its *effet utile*, that does not empower the Court to create such a rule.

*Interim conclusion*

131. EU law does not, at this stage of its development, regulate the admissibility of evidence collected by way of an EIO issued contrary to the requirements of the EIO Directive. The admissibility of evidence is a matter of national law, which, however, needs to comply with the requirements of the rights of the defence in Articles 47 and 48 of the Charter.

## IV. Conclusion

132. In light of the foregoing considerations, I propose that the Court answer the questions referred for a preliminary ruling by the Landgericht Berlin (Regional Court, Berlin, Germany) as follows:

(1) In response to the first group of questions as referred:

When an underlying measure in the executing State was authorised by a judge, a European Investigation Order (EIO) for transfer of such evidence does not need to be issued by a judge as well, even if under the law of the issuing State the underlying gathering of evidence would have to be ordered by a judge.

The fact that the interception has been carried out on the territory of another Member State does not make any difference for determining the issuing authority.

EU law does not require that an EIO for the transfer of existing evidence gathered through the interception of telecommunications be issued by a court, if national law provides that a public prosecutor may order such a transfer in a similar domestic case.

(2) In response to the second group of questions as referred:

The assessment of the necessity and proportionality of an EIO requesting the transfer of the existing evidence is a matter for the issuing authority, with a possibility of review by the competent national court. Such an assessment must take into consideration that the access of the national authority to the intercepted communication data represents serious interference with the private lives of the persons concerned. That interference must be counterbalanced by serious public interest in the investigation and prosecution of crimes.

(3) In response to the third group of questions as referred:

When an EIO is issued for the transfer of evidence already in the possession of another State, the reference to a similar domestic case under Article 6(1)(b) of Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters requires the issuing authority to establish whether and under which conditions the relevant national law allows for a transfer of evidence gathered through the interception of communication between criminal procedures domestically.

When deciding whether it can issue an EIO for the transfer of existing evidence, the issuing authority cannot assess the legality of the underlying gathering of evidence in the executing State whose transfer it requires by an EIO.

The fact that the underlying measures were undertaken on the territory of the issuing State, or were in the interest of that State, does not influence the preceding answer.

(4) In response to the fourth group of questions as referred:

A Member State which, in the course of its unilateral criminal investigation or procedure, intercepts telecommunications on the territory of another Member State must notify that other State of the interception.

That notification may be submitted to any authority that the intercepting Member State considers appropriate, as that State cannot know which authority is competent in a similar domestic case.

Article 31 of Directive 2014/41 has a purpose to protect both the individual telecommunications users concerned and the sovereignty of the notified Member State.

(5) In response to the fifth group of questions as referred:

EU law does not, at this stage of its development, regulate the admissibility of evidence collected by way of an EIO issued contrary to the requirements of Directive 2014/41. The admissibility of evidence is a matter of national law, which, however, needs to comply with the requirements of the rights of the defence in Articles 47 and 48 of the Charter of Fundamental Rights of the European Union.

---

1 Original language: English.

---

2 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 2014 L 130, p. 1) (‘the EIO Directive’).

---

3 This included a dual operating system (with an undetectable encrypted interface) where the device had no camera, microphone, GPS or USB port. Messages were able to auto-delete and users could, after using a special PIN code or after consecutively entering an incorrect password, immediately delete all data on the device. Finally, a remote helpdesk or reseller was also able to delete all the data on the device if necessary. For more information, see https://www.europol.europa.eu/media-press/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe.

---

4 For example, the Conseil constitutionnel (Constitutional Council, France) found in April 2022 that the French legislation, based on which the underlying measure of interception of communication in the present case was ordered, is in line with the French Constitution in Décision No 2022-987 QPC of 8 April 2022; the Bundesgerichtshof (Federal Court of Justice, Germany) found that the interception was legal under German law in judgment 5 StR 457/21 of 2 March 2022; finally, a challenge against using EncroChat data from France before United Kingdom courts is currently pending before the European Court of Human Rights (ECtHR) in Cases No 44715/20 (*A.L. v. France*) and No 47930/21 (*E.J. v. France*). On 3 January 2022, the ECtHR sent questions to the parties asking, among others, whether they had (but did not use) an opportunity to challenge the interception measures before competent French courts.

---

5 Prior to the EIO Directive, the transfer of evidence already in the possession of another Member State was regulated by Council Framework Decision 2008/978/JHA of 18 December 2008 on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters (OJ 2008 L 350, p. 72). According to recitals 4 to 7 of the EIO Directive, the previous system was too fragmented and complicated, therefore the EIO was designed as a single instrument for the purpose of obtaining new and already existing evidence.

6 See the decision of that court cited in footnote 4.

7 This reference is, therefore, an example of the classic narrative according to which the preliminary reference procedure resulted in the judicial empowerment of ordinary national courts vis-à-vis their superior courts, most famously articulated by Alter, K.J., 'The European Court's Political Power', *West European Politics*, Vol. 19(3), 1996, p. 452. For the empirical demonstration of the reverse dynamic, one where superior domestic courts refer questions to the Court of Justice to pre-empt their inferior counterparts from doing so, see Pavone, T. and Kelemen, D.R., 'The Evolving Judicial Politics of European Integration: The European Court of Justice and national courts revisited', *European Law Journal*, Vol. 25(4), 2019, p. 352.

8 See Article 6(2) of the EIO Directive.

9 See, in that regard, judgment of 16 December 2021, *Spetsializirana prokuratura (Traffic and location data)* (C-724/19, EU:C:2021:1020, paragraph 44). See, also, Csúri, A., 'Towards an Inconsistent European Regime of Cross-Border Evidence: The EPPO and the European Investigation Order', in Geelhoed, W. et al., *Shifting Perspectives on the European Public Prosecutor's Office*, T.M.C. Asser Press, The Hague, 2018, p. 146.

10 Under Article 2(c)(ii) of the EIO Directive, another authority competent under national law may also issue an EIO, when such an EIO is then validated by one of the authorities listed in Article 2(c)(i) thereof.

11 Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (OJ 2002 L 190, p. 1), as amended by Council Framework Decision 2009/299/JHA of 26 February 2009 amending Framework Decisions 2002/584, 2005/214/JHA, 2006/783/JHA, 2008/909/JHA and 2008/947/JHA, thereby enhancing the procedural rights of persons and fostering the application of the principle of mutual recognition to decisions rendered in the absence of the person concerned at the trial (OJ 2009 L 81, p. 24) ('the EAW Framework Decision').

12 In judgment of 2 March 2023, *Staatsanwaltschaft Graz (Düsseldorf tax office for criminal tax matters)* (C-16/22, EU:C:2023:148, paragraphs 33 to 36), the Court found that points (i) and (ii) of Article 2(c) of the EIO Directive are mutually exclusive.

13 Judgment of 8 December 2020, *Staatsanwaltschaft Wien (Falsified transfer orders)* (C-584/19, EU:C:2020:1002, paragraphs 57 to 63). In contrast, in judgment of 27 May 2019, *OG and PI (Public Prosecutor's Offices, Lübeck and Zwickau)* (C-508/18 and C-82/19 PPU, EU:C:2019:456, paragraphs 88 to 90), the Court found that the German public prosecutors in that case did not satisfy the independence requirement necessary for issuing a European arrest warrant (EAW). It would follow that a public prosecutor that is not entirely independent from the executive cannot issue an EAW, but can, nevertheless, issue an EIO. It is worth underlining that in those two judgments, a legal remedy against the public prosecutor was deemed sufficient for the protection of fundamental rights in the context of issuing an EIO, but insufficient in the context of issuing an EAW.

14 See the decision of the Federal Court of Justice referred to in footnote 4.

15 It should be added that, at the hearing, the question arose whether the fact that Germany was given, via Europol, real-time access to the intercepted communication (at least as of 3 April 2020) should mean that

Germany needed to issue an EIO seeking the *gathering* of those data. As explained by the Berlin Public Prosecutor's Office, and the German Government, that direct access was not made possible for the purposes of criminal prosecution, but for preventive police purposes only. They argued that the EIOs were subsequently required for the use of that evidence in the German criminal procedure. On the contrary, an EIO for gathering the data made accessible in real time via Europol was not necessary (or indeed possible) as that access to data did not happen in relation to proceedings enumerated in Article 4 of the EIO Directive. That directive, therefore, did not apply to the police's access to real-time data.

---

16 My emphasis.

---

17 According to my own, necessarily superficial, research of the StPO, Section 477(2) provides for an *ex officio* transmission of personal data from one criminal procedure to another, and Section 480(1) provides that this be ordered by a public prosecutor in preparatory proceedings and after the final conclusion of those proceedings; in any other situation it is for the presiding judge seised of the matter to order it. A duty to transmit evidence may be derived from the principle of mandatory prosecution laid down in Section 152(2). In principle, transmission is possible only if the relevant evidence concerns a criminal offence for the prosecution of which such a measure could have been ordered; otherwise, the consent of the affected person is necessary. Vogel, B., Köppen, P. and Wahl, T., 'Access to Telecommunication Data in Criminal Justice: Germany', in Sieber, U. and von zur Mühlen, N. (eds), *Access to Telecommunication Data in Criminal Justice. A Comparative Analysis of European Legal Orders*, Duncker & Humblot, Berlin, 2016, p. 518; Gieg, G. in Barthe, C. and Gericke, J. (eds.), *Karlsruher Kommentar zur Strafprozessordnung*, Section 477(1); Section 479(3), C.H. Beck, München, 2023.

---

18 Whether the persons concerned by the EncroChat interceptions were able to challenge that in France is an issue pending before the ECtHR. See footnote 4.

---

19 National criminal procedures vary widely among the Member States, not only in terms of available investigative measures (Armada, I., 'The European Investigation Order and the Lack of European Standards for Gathering Evidence: Is a Fundamental Rights-Based Refusal the Solution?', *New Journal of European Criminal Law*, Vol. 6(1), 2015, p. 9) but also in terms of the conditions attached to their usability (Bachmaier, L., 'Mutual Recognition and Cross-Border Interception of Communications: The Way Ahead for the European Investigation Order', in Brière, C. and Weyembergh, A. (eds), *The Needed Balances in EU Criminal Law: Past, Present and Future*, Hart Publishing, Oxford, 2018, p. 317). For example, when it comes to the interception of communication, some Member States provide a list of criminal offences for the investigation of which such a measure may be prescribed (for example, Germany); others focus on the minimum penalty requirement (for example, France); others still use a mix of the two approaches. In addition, different national laws allow for such an investigative measure on the condition that there is a certain degree of suspicion or on a mandatory assessment of necessity (whether a less intrusive measure would achieve the same result). Finally, Member States diverge in terms of the maximum length of the interception order and the possibility of its prolongation (see Tropina, T., 'Comparative Analysis', in Sieber, U. and von zur Mühlen, N. (eds), *Access to Telecommunication Data in Criminal Justice. A Comparative Analysis of European Legal Orders*, Duncker & Humblot, Berlin, 2016, pp. 67-72 and 77-79).

---

20 Judgment of 16 December 2021, *Spetsializirana prokuratura (Traffic and location data)* (C-724/19, EU:C:2021:1020, paragraphs 35 and 44). See also judgment of 8 December 2020, *Staatsanwaltschaft Wien (Falsified transfer orders)* (C-584/19, EU:C:2020:1002, paragraph 52).

---

21 Judgment of 16 December 2021, *Spetsializirana prokuratura (Traffic and location data)* (C-724/19, EU:C:2021:1020, paragraphs 35 and 45).

---

22 This also makes sense from the point of view of preventing forum shopping: if national law requires the participation of a court domestically, using an EIO should not do away with that requirement. Mangiaracina, A., '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 Review*, Vol. 10(1), 2014, p. 126.

---

23 It should be said, however, that the efforts taken in ensuring minimum harmonisation in the field of criminal procedural law play a significant role in 'familiarising' the different legal systems of Member States. I have in mind instruments such as Directive (EU) 2016/343 of the European Parliament and of the Council of 9 March 2016 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings (OJ 2016 L 65, p. 1) or Directive 2012/13/EU of the European Parliament and of the Council of 22 May 2012 on the right to information in criminal proceedings (OJ 2012 L 142, p. 1).

---

24 In that context, I have already mentioned that the French Constitutional Council found in April 2022 that the French legislation under which the EncroChat interception was ordered is in line with the French Constitution. See footnote 4.

---

25 According to the order for reference, this was authorised by the Criminal Court in Lille.

---

26 Given that the mobile phones of German users on which data were stored were in Germany.

---

27 The relevance of the interception being carried out on the territory of the issuing State will be dealt with within the scope of the fourth group of questions concerning the interpretation of Article 31 of the EIO Directive. See Section D below.

---

28 Recital 11 of the EIO Directive further clarifies that provision by stating that the 'issuing authority should therefore ascertain whether the evidence sought is necessary and proportionate for the purpose of the proceedings, whether the investigative measure chosen is necessary and proportionate for the gathering of the evidence concerned, and whether, by means of issuing the EIO, another Member State should be involved in the gathering of that evidence'. As it follows from its wording, that recital is mostly focused on the first type of an EIO, which is for gathering new evidence.

---

29 The form by way of which an EIO is issued provides space for the issuing authority to explain in detail why the EIO is necessary in the circumstances of a particular case (Annex A to the EIO Directive, Section G). On the relevance of that form for the proportionality assessment, see Bachmaier Winter, L., 'The Role of the Proportionality Principle in Cross-Border Investigations Involving Fundamental Rights', in Ruggeri, S., (ed.), *Transnational Inquiries and the Protection of Fundamental Rights in Criminal Proceedings: A Study in Memory of Vittorio Grevi and Giovanni Tranchina*, Springer, Berlin, 2013, p. 318.

---

30 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ 2002 L 201, p. 37) ('the ePrivacy Directive').

---

31 See, for example, judgments of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)* (C-746/18, EU:C:2021:152, paragraph 39), and of 5 April 2022, *Commissioner of An Garda Síochána and Others* (C-140/20, EU:C:2022:258, paragraph 44).

32 That directive applies only to situations in which the authorities of a State access the traffic and location data retained by the telecommunications operators. On the contrary, it does not apply when those authorities directly intercept telecommunications data. See, in that respect, judgment of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 103).

33 See, by analogy, judgment of 21 June 2022, *Ligue des droits humains* (C-817/19, EU:C:2022:491, paragraph 122).

34 For example, when it comes to the degree of suspicion necessary to order a certain investigation measure.

35 Judgment of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)* (C-746/18, EU:C:2021:152, paragraphs 51, 53, and 54).

36 Opinion of Advocate General Pitruzzella in *Prokuratuur (Conditions of access to data relating to electronic communications)* (C-746/18, EU:C:2020:18, points 103 to 123).

37 Judgment of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 103).

38 The case-law developed by the ECtHR in relation to Article 8 of the European Convention of Human Rights (ECHR), guaranteeing a right to privacy, found violations when the law did not require a proportionality assessment and did not provide for judicial review. See, for example, ECtHR, 12 January 2016, *Szabó and Vissy v. Hungary*, CE:ECHR:2016:0112JUD003713814, § 89.

39 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ 2016 L 119, p. 89) ('the Law Enforcement Directive').

40 Judgment of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 103).

41 When assessed in light of the Law Enforcement Directive, the present case may be described as two instances of processing personal data: first, the competent French authorities were the controller when they intercepted and collected electronic communications data for the purposes of the prevention, investigation, detention or prosecution of criminal offences; second, by transferring those data to the Frankfurt Public Prosecutor's Office, which requested them for the purpose of a criminal investigation in Germany based on the EIOs, that public prosecutor's office became the controller.

42 The Court stated that in the context of repurposing under Article 4(2) of the Law Enforcement Directive, the assessment of compliance with the principles governing data processing in the scope of that directive must be carried out each time data are processed as specific and distinct (see judgment of 8 December 2022, *Inspektor* v

*Inspektorata kam Visshia sadeben savet (Purposes of the processing of personal data – Criminal investigation)*, (C-180/21, EU:C:2022:967, paragraph 56)).

---

43 In situations where technical assistance is required from the Member State on whose territory the interception is being carried out, Article 30 of the EIO Directive applies.

---

44 The text of Article 31 of the EIO Directive corresponds in large part to Article 20 of the Convention established by the Council in accordance with Article 34 of the Treaty on European Union, on Mutual Assistance in Criminal Matters between the Member States of the European Union (OJ 2000 C 197, p. 3).

---

45 Bachmaier, L., footnote 19, p. 330.

---

46 Specifically, Article 31(3) of the EIO Directive allows the relevant authority of the notified State to verify whether such an interception would be allowed in a similar domestic case, and notify, within 96 hours from the receipt of the notification, the intercepting Member State that the interception may not be carried out, shall be terminated, or that the data obtained may not be used at all or only under certain conditions.

---

47 I therefore do not agree with the French Government, which argued that Article 31 of the EIO Directive does not apply to the present case because the interception of communication was not carried out for the purposes of executing an EIO, but rather took place before any EIO was issued.

---

48 Bachmaier, L., footnote 19, p. 331.

---

49 To comply with the notification obligation imposed by Article 31 of the EIO Directive, France should have used the form in Annex C to that directive.

---

50 See Article 33(1) of the EIO Directive.

---

51 Ligeti, K. et al. mention that Member States refuse to take that step due to concerns related to subsidiarity and proportionality, and that this would influence the systems of checks and balances on the national level (Ligeti, K., Garamvölgy, B., Ondrejová, A. and von Galen, M., 'Admissibility of Evidence in Criminal Proceedings in the EU', *eucrim*, Vol. 3, 2020, p. 202 footnote 14).

---

52 Recital 34 of the EIO Directive in addition states: 'Furthermore, for the same reason, the assessment of whether the item is to be used as evidence and therefore be the object of an EIO should be left to the issuing authority.'

---

53 Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office, (OJ 2017 L 283, p. 1) ('the EPPO Regulation').

---

54 Judgments of the ECtHR, 12 July 1988, *Schenk v. Switzerland*, CE:ECHR:1988:0712JUD001086284, §§ 45 and 46; of 11 July 2017, *Moreira Ferreira v. Portugal (no. 2)*, CE:ECHR:2017:0711JUD001986712, § 83; and of 1 March 2007, *Heglas v. the Czech Republic*, CE:ECHR:2007:0301JUD000593502, § 84.

55 Judgment of the ECtHR, 17 January 2017, *Habran and Dalem v. Belgium*, CE:ECHR:2017:0117JUD004300011, § 96.

56 Hecker, B., 'Mutual Recognition and Transfer of Evidence. The European Evidence Warrant', in Ruggeri, S., (ed.), *Transnational Inquiries and the Protection of Fundamental Rights in Criminal Proceedings: A Study in Memory of Vittorio Grevi and Giovanni Tranchina*, Springer, Berlin, 2013, p. 277; Armada, I., footnote 19, p. 30.

57 Judgment of 7 September 2023, *Rayonna prokuratura (Fouille corporelle)* (C-209/22, EU:C:2023:634, paragraphs 58 and 61).

58 Established in judgments of 16 December 1976, *Rewe-Zentralfinanz and Rewe-Zentral* (33/76, EU:C:1976:188, paragraph 5), and of 16 December 1976, *Comet* (45/76, EU:C:1976:191, paragraph 13). Most recently, see, for example, judgment of 13 July 2023, *CAJASUR Banco* (C-35/22, EU:C:2023:569, paragraph 23).