Case C-670/22

Summary of the request for a preliminary ruling pursuant to Article 98(1) of the Rules of Procedure of the Court of Justice

Date lodged:

24 October 2022

Referring court:

Landgericht Berlin (Germany)

Date of the decision to refer:

19 October 2022

Criminal prosecution authority:

Staatsanwaltschaft Berlin

Accused person:

M.N.

Subject matter of the main proceedings

Judicial cooperation in criminal matters – Directive 2014/41/EU – European Investigation Order in criminal matters – Concept of 'issuing authority' – Spying on and transmitting traffic and location data of an internet-based communications service provider – Mobile phones equipped with encryption software – Illicit trafficking in substantial quantities of narcotic drugs – Use of evidence in criminal proceedings

Subject matter and legal basis of the request

Interpretation of EU law, Article 267 TFEU

Questions referred for a preliminary ruling

1. Interpretation of the concept of 'issuing authority' under Article 6(1) of Directive 2014/41, in conjunction with Article 2(c) thereof,

(a) Must a European Investigation Order ('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 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 Directive 2014/41

(a) Does Article 6(1)(a) of Directive 2014/41 preclude an EIO for the transmission of data already available in the executing State (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 Directive 2014/41 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 Directive 2014/41

(a) Does Article 6(1)(b) of Directive 2014/41 preclude an EIO for the transmission of telecommunications data already available in the executing State (France) where the executing State's interception measure underlying the gathering of data would have been impermissible under the law of the issuing State (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 Directive 2014/41

(a) Does a measure entailing the infiltration of terminal devices for the purpose of gathering traffic, location and communication data of an internet-based communication service constitute interception of telecommunications within the meaning of Article 31 of Directive 2014/41?

(b) Must the notification under Article 31(1) of Directive 2014/41 always be addressed to a judge, or is that the case at least where the measure planned by the intercepting State (France) could be ordered only by a judge under the law of the notified State (Germany) in a similar domestic case?

(c) In so far as Article 31 of Directive 2014/41 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 (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?

Provisions of European Union law relied on

Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters ('Directive 2014/41'), in particular Article 6(1), in conjunction with Article 2(c), Article 31(1) and (3)

Charter of Fundamental Rights of the European Union ('the Charter'), Articles 7, 8 and 11

Provisions of national law relied on

Strafprozessordnung (Code of Criminal Procedure; 'the StPO'), in particular Paragraphs 100a, 100b, 100e

Gesetz über die internationale Rechtshilfe in Strafsachen (Law on international mutual assistance in criminal matters; 'the IRG'), Paragraph 91g

Succinct presentation of the facts and procedure in the main proceedings

1 From 2017 onwards, the French investigating authorities found that suspects were using 'cryptophones' from the provider 'EncroChat' in the commission of offences, primarily in crime involving narcotic drugs. Those mobile phones, equipped with special security components, enabled end-to-end encrypted communication via a server in Roubaix (France), which could not be intercepted by means of conventional investigative methods.

2 With judicial authorisation, the French police managed to secure images of the server data in 2018 and 2019. On the basis of the knowledge gained from those images, a piece of Trojan software was developed within the framework of a transnational investigation group (Joint Investigation Team; 'the JIT'), which, with the authorisation of the Criminal Court, Lille (France), was uploaded to the server in Roubaix in the spring of 2020 and, from there, was installed on the terminal devices via a simulated update. Users in a total of 122 countries were affected by the measure, including 380 users in France and approximately 4 600 users in Germany.

3 Between 1 April 2020 and 28 June 2020, the Trojan software enabled the French authorities to capture the device identifiers of the terminals detected in the respective countries, as well as location, traffic and communication data,

including texts and images transmitted in the ongoing chats. Furthermore, the authorities read the device memories, including the chats from the time before 1 April 2020 that had not yet been deleted. Technical details about the function of the Trojan software and the storage, allocation and filtering of the data by the French authorities or Europol are not known. The functioning of the Trojan software is in principle subject to French military secrecy.

4 In so far as the terminal devices were located abroad, the captured data were made available to a number of national investigative authorities, including the German Bundeskriminalamt (Federal Criminal Police Office; 'the BKA'), via a Europol server from 3 April 2020.

5 Since 2018, the BKA had knowledge that EncroChat telephones were being used in the commission of serious crimes in Germany, in particular those involving narcotic drugs. From the beginning of 2020, the BKA and the Generalstaatsanwaltschaft Frankfurt am Main (General Prosecutor's Office, Frankfurt am Main ('the Frankfurt GStA') held discussions about the possibility of investigative measures in respect of the German EncroChat users.

6 In a Eurojust video conference held on 9 March 2020, at which information was provided in relation to the surveillance measure planned by the French police and the intended transfer of data to the other countries, representatives of the BKA and the Frankfurt GStA signalled their interest in the data of the German users.

7 At the suggestion of the BKA in a letter of 13 March 2020, proposing that a preliminary investigation be opened in respect of all unknown users of the EncroChat service, on suspicion of engaging in illicit trafficking in substantial quantities of narcotic drugs as part of an organised group and of forming a criminal organisation, the Frankfurt GStA opened such a preliminary investigation in respect of unknown persons ('UJs investigation') on 20 March 2020. Initially, investigative measures were neither taken nor sought by application to the investigating judge.

8 On 27 March 2020, the BKA received, via the European SIENA messaging system, a communication from the JIT addressed to the police authorities of the countries interested in the EncroChat data, requesting that they confirm in writing that they had been informed of the methods used to obtain data from devices on their territory. At the same time, they were to ensure that the data initially transmitted only for analysis purposes would be used for ongoing preliminary investigations only after approval by the JIT countries. The German authorities granted the consents and confirmations requested in the communication. The French authorities did not make a notification in accordance with Article 31(1) of Directive 2014/41, or Paragraph 91g of the Gesetz über die Internationale Rechtshilfe in Strafsachen (Law on international mutual legal assistance in criminal matters; 'the IRG'); nor was any objection raised on the German side in that regard.

9 In the period from 3 April 2020 to 28 June 2020, the BKA retrieved the data of the terminal devices used in Germany which were made available on the Europol server on a daily basis. After the data analysis had revealed a concrete suspicion of the commission of an offence in respect of a number of users, the BKA sought from the French Public Prosecutor's Office, by letter of 13 May 2020, authorisation to apply to the investigating judge – while the measure was still in progress, and if possible without reference being made to the subject matter of the French investigation and the nature of the measure – for individual orders for establishing the identification of those users. After the authorisation was granted, the Frankfurt GStA then obtained individual judicial orders for the collection of location data and for other investigative measures.

10 On 2 June 2020, within the framework of the UJs investigation, the Frankfurt GStA requested authorisation from the French authorities, by way of an EIO, to use the EncroChat data without restriction in criminal proceedings. The request was based on the ground that there was a suspicion that a large number of very serious criminal offences (in particular the import and trafficking of substantial quantities of narcotic drugs) were being committed in Germany by persons who had not yet been identified, using EncroChat phones. In response to that request, the Criminal Court, Lille authorised the transmission and judicial use of the EncroChat data of the German users. Additional data was subsequently transmitted on the basis of two supplementary EIOs of 9 September 2020 and 2 July 2021.

11 In the period that followed, the Frankfurt GStA separated from the UJs procedure the investigations being conducted in respect of individual users, including the accused person in the present case, and assigned them to local public prosecutors' offices.

Succinct presentation of the reasoning in the request for a preliminary ruling

12 The Staatsanwaltschaft Berlin (Public Prosecutor's Office, Berlin) charged the accused person with several counts of illicit trafficking in substantial quantities of narcotic drugs and illegal possession of substantial quantities of narcotic drugs in Germany. He allegedly used the 'EncroChat' communication service to conduct his distribution activities and communicated via it by text and image messages. The text and image messages allegedly created by or sent to the accused person were obtained by way of the telecommunications interception operation carried out by the French authorities within the framework of the investigations conducted there. The charges are based substantially on those messages.

13 By means of the request for a preliminary ruling, the referring court seeks to clarify whether the German investigating authorities infringed rules of Directive 2014/41 when obtaining the data and whether, if so, the infringements must prevent the data from being used in the criminal proceedings – with the consequence of an acquittal – or otherwise affect the verdict.

14 The referring court states the following with regard to the questions referred:

15 Questions 1(a) to (c): Under national law, Paragraph 100a et seq. of the Strafprozessordnung (Code of Criminal Procedure; 'the StPO'), govern the interception of telecommunications for the purposes of criminal prosecution. The first sentence of Paragraph 100a(1) of the StPO permits the interception of ongoing communications. Furthermore, it is permissible to intercept ongoing communications by installing spyware on the terminal devices (second sentence of Paragraph 100a(1) of the StPO), to capture communications already transmitted and stored on the device at the time of the order (third sentence of Paragraph 100a(1) of the StPO) and to read all the data stored on the terminal device (Paragraph 100b of the StPO). All of those measures require a concrete suspicion of a criminal offence, whereby the group of triggering offences is restricted to certain 'catalogue' offences in Paragraphs 100a(2) and 100b(2) of the StPO. Under Paragraph 100e(1) and (2) of the StPO, the measures may be ordered by the court only at the request of the public prosecutor's office; in that respect, in accordance with Paragraph 100e(2) of the StPO, in conjunction with Paragraph 74a(4) of the Gerichtsverfassungsgesetz (Law on the constitution of the courts; 'the GVG), the online surveillance ('*Online-Durchsuchung*') under Paragraph 100b of the StPO comes within the exclusive competence of a special chamber of the regional court not ruling in main proceedings in criminal cases.

16 The French measure appears to resemble a combination of online surveillance within the meaning of Paragraph 100b of the StPO and one or more of the measures regulated in Paragraph 100a(1) of the StPO. Accordingly, under Paragraph 100e(2) of the StPO, the regional court would have been competent to order it. Since, in accordance with the general German rules, an EIO by which the interception of telecommunications abroad is sought can be issued by the investigating public prosecutor's office in the preliminary investigation prior to indictment, the Bundesgerichtshof (Federal Court of Justice, Germany), in its fundamental decision of 2 March 2022 (5 StR 457/21, paragraph 47), proceeds on the assumption, by contrast, that the Frankfurt GStA, which is investigating in the UJs procedure, is competent to issue the EIO for the transfer of evidence.

17 In particular in light of the judgment of the Court of Justice of 16 December 2021, *Spetsializirana prokuratura (Traffic and location data)* (C-724/19, EU:C:2021:1020, paragraph 32 et seq.), the referring court has concerns as to whether the issuance of the EIOs of 2 June 2020, 9 September 2020 and 2 July 2021 by the Frankfurt GStA is compatible with Directive 2014/41. There are grounds for taking the view that, in accordance with Article 6(1) of Directive 2014/41, in conjunction with Article 2(c) thereof, a court (territorially and substantively: the Regional Court, Frankfurt am Main) would have been competent if the above case-law is applied to the case where the executing State has already carried out the investigative measure and the issuing State requests, by way of the EIO, the transfer of the data thus obtained or permission to use them in a judicial capacity. The wording of Article 2(c)(i) and (ii) of Directive 2014/41

and the assessment steps provided for in Article 6(1)(a) and (b) thereof militate in particular in favour of a court having competence.

18 Furthermore, the data subsequently requested by way of the EIOs originate exclusively from users in the territory of the issuing State (Germany). From the outset, the executing State (France) had collected and stored those data only with the aim of subsequently transmitting them to the issuing State for the purposes of criminal prosecution there. The German criminal prosecution authorities were informed of the surveillance measure before it began. They endorsed the measure by means of the consent declared in the reply to the SIENA message of 27 March 2020 and the undertakings given therein, without which the data would not have been made available on the Europol server. In view of this, the natural course of action for the German authorities would have been to instruct the French authorities to carry out the measure against the German users by way of an EIO before the measure began. Alternatively, the French authorities would have been under an obligation to notify in accordance with Article 31 of Directive 2014/41, whereby such notification would also have led to a prior judicial review of the measure in Germany in accordance with Article 31(3) of Directive 2014/41, and Paragraph 91g(6) of the IRG.

19 Since Directive 2014/41 is also aimed at ensuring national minimum standards, it seems appropriate for an EIO to be issued with a view to data transfer to be subject to the same jurisdictional rules that would have applied to an EIO to be issued with a view to interception. This applies in particular to the EIO of 2 June 2020, when the interception measure was still ongoing. The fact that the measure had been ordered by a judge in France did not render the decision of the German court unnecessary (see, regarding the judicial recognition of an EIO in the executing State, judgment of the Court of Justice of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)*, C-746/18, EU:C:2021:152, paragraph 53).

20 The referring court takes the view that it can be concluded from that judgment of the Court of Justice that the EIOs in the present case should also have been issued by a judge irrespective of the national rules of jurisdiction. The statements of the Court of Justice regarding the interpretation of Article 15(1) of Directive 2002/58 in the light of the fundamental rights under Articles 7, 8 and 11 of the Charter can be applied to the interpretation of Article 6(1)(a) of Directive 2014/41. For the purpose of interpreting Article 2(c) of Directive 2014/41, it can be concluded from that case-law that, irrespective of the national rules of jurisdiction in a similar domestic case, an EIO for the purpose of criminal prosecution must be issued by a judge not ruling on the specific investigative measures where – as in the present case – the assessment of proportionality under Article 6(1)(a) of Directive 2014/41 involves a complex balancing exercise and concerns serious interferences with high-ranking fundamental rights.

21 In accordance with the case-law of the Court of Justice, the transmission of traffic or location data to a public authority already constitutes a serious interference with

the fundamental rights under Articles 7 and 8 of the Charter (see 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 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:929, paragraph 116). The interference was further intensified by the fact that the entire content of the communications, spanning a period of several months, was transmitted. In so far as the EncroChat service does not constitute 'conventional' telecommunications within the meaning of the first sentence of Article 2 of Directive 2002/58, in conjunction with Article 2(c) of the Framework Directive 2002/21, but rather an internet-based 'over-the-top' service, this does not justify a different assessment.

22 Questions 2(a) and (b) and 3(a) and (b): National law does not contain any rules governing the substantive requirements for an outgoing EIO. Recourse must therefore be had, on a supplementary basis, to Article 6 of Directive 2014/41.

23 Under Paragraphs 100a and 100b of the StPO, the secret interception of telecommunications for the purposes of criminal prosecution requires a suspicion that a criminal offence has been committed. Paragraphs 100a and 100b of the StPO restrict the group of triggering offences – graded according to the severity of their interference with fundamental rights – to certain catalogue offences, whereby the suspicion must be based on 'certain facts'. Since the non-specific grounds for suspicion given prior to the commencement of the measure in the present case and the list of various criminal offences that may enter into consideration in the alternative do not meet the constitutional requirements that are applicable in that regard, surveillance of all EncroChat users would not have been permissible under Paragraph 100a et seq. and Paragraph 100e(3), points 2 and 4, of the StPO.

24 Under Article 6(1)(a) of Directive 2014/41, the issuing of the EIO must be necessary and proportionate for the purpose of the proceedings. The referring court takes the view that an EIO seeking access to data from the interception of telecommunications for the purposes of criminal prosecution fulfils that requirement only where there is a suspicion, based on concrete facts, of involvement in a serious criminal offence, in respect of each person concerned.

25 In its decision of 2 March 2022 (5 StR 457/21, paragraph 55), the Federal Court of Justice took the view that the 'unspecified situation of suspicion' with regard to the 'multiple criminal offences in question' was sufficient to issue the EIO in accordance with Article 6(1)(a) of Directive 2014/41. The referring court does not wish to follow that view.

26 The grounds for suspicion described by the Federal Court of Justice were criminal findings from – in relation to the total number of users – a very small number of earlier criminal proceedings, without any reference being made to the individual users concerned by the EIO. In addition, it was apparent from particular features of the functions of the EncroChat telephones and the methods by which they were distributed that they were particularly attractive to criminal users. However,

investigations into lawful possibilities of use for persons with an above-average need for secure communications were not carried out at any time. Concrete facts that could have given rise to criminal prosecution were not known, even in broad terms. In so far as there was evidence that the EncroChat operators targeted their system to meet the needs of criminals, this only allowed the conclusion that some, but by no means (almost) all, users were engaged in criminal activities. There was nothing to indicate that all EncroChat users were part of an interconnected criminal group.

27 The referring court takes the view that those grounds for suspicion are not sufficient to justify the issuance of an EIO. Since the structure and interpretation of Paragraph 100a et seq. of the StPO is decisively shaped by the requirements of the German constitution, and since the protection of fundamental rights under EU law against the secret interception of communications is comparably strong, it is evident that comparably strong and specific grounds for suspicion are also required under Article 6(1)(a) of Directive 2014/41.

28 That interpretation of Article 6(1)(a) of Directive 2014/41 is supported by the case-law of the Court of Justice on the permissibility of data retention, in accordance with which the retention of traffic or location data and access to such data by the authorities seriously interferes with the fundamental rights under Articles 7 and 8 of the Charter (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*, C-140/20, paragraph 44). The principles regarding proportionality within the meaning of Article 15(1) of Directive 2002/58 which are developed in that case-law can be applied to proportionality within the meaning of Article 6(1)(a) of Directive 2014/41.

29 Further concerns regarding the proportionality of the EIO arise with regard to the right to a fair trial (second paragraph of Article 47 of the Charter, Article 6(1) of the European Convention on Human Rights; 'the ECHR'), in accordance with which a party to court proceedings must have a real opportunity to comment on a piece of evidence. This is particularly true where the evidence pertains to a field of which the judges and the party have no knowledge (judgments of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)*, C-746/18, EU:C:2021:152, paragraph 44 and the case-law cited, and of 10 April 2003, *Steffensen*, C-276/01, EU:C:2003:228, paragraph 77 and the case-law cited).

30 The present case also involves evidence that raises various complex issues, in particular in relation to the integrity of the data (that is to say its correctness, completeness and consistency). Moreover, the EncroChat data constitute the only evidence. Since the criteria for the alleged offence of trafficking in narcotic drugs are already fulfilled by the genuine negotiation of a sale of narcotic drugs, the defence depends not only on the analysis of individual messages, but also on the temporal and contextual connection between sent and received messages.

Technical errors and incompleteness therefore entail a risk of chat histories being unintentionally distorted. There are grounds for taking the view that that restriction of the possibilities of defence in the subsequent criminal proceedings must have an advance effect on the assessment of proportionality under Article 6(1)(a) of Directive 2014/41. Thus, it is conceivable that evidence of the type described above, against which the accused person will not be able to defend himself or herself effectively in subsequent criminal proceedings, may not be requested by way of an EIO intended to make criminal prosecution possible.

31 In accordance with Article 6(1)(b) of Directive 2014/41, the issuing authority must review the measure specified in the EIO on the basis of national law. The referring court takes the view that, in the case of an EIO seeking a transfer of evidence, that review must extend to the investigative measure underlying the collection of evidence in the executing State: if the interception measure should not have been ordered in a similar domestic case, the data obtained from such a measure may also not be requested by way of an EIO. Since the requirements of Paragraph 100a et seq. of the StPO were not met in the present case due to the lack of a concrete suspicion of an offence having been committed, the EIOs should not have been issued.

32 However, in its decision of 2 March 2022 (5 StR 457/21, paragraph 47 et seq.), the Federal Court of Justice took the view that Article 6(1)(b) of Directive 2014/41 was not applicable to an EIO that was directed only at the transfer of evidence which already existed and that a review of the measure on the basis of national law was therefore unnecessary. At the level of the issuing State, protection of the individual was to be guaranteed solely by the examination under Article 6(1)(a) of Directive 2014/41 and by the subsequent assessment in the national criminal proceedings of the evidence obtained, in accordance with the second sentence of Article 14(7) of Directive 2014/41.

33 There are reservations about the view taken by the Federal Court of Justice. It is true that the transfer of evidence as such is not an appropriate criterion for examining whether such a measure could be ordered in a domestic case, since it concerns an originally international factual situation without a purely domestic equivalent. Unlike the Federal Court of Justice, however, the referring court does not wish to conclude from this that Article 6(1)(b) of Directive 2014/41 is inapplicable to an EIO seeking a transfer of evidence. Rather, in this case, the issuing authority must apply the assessment, against the standards of national law, to the investigative measure underlying the collection of the data: it may request evidence already available in the executing State by way of an EIO only if the investigative measure by which the evidence was obtained in the executing State would have been admissible in the issuing State in a similar domestic case.

34 Although the restriction of the scope of application made by the Federal Court of Justice is consistent with the wording of the provision, the assessment against the standards of national law must be applied to the ‘investigative measure specified in the EIO’, which does not necessarily have to be the measure ‘ordered’ by that

EIO; in order to describe the data to be transmitted, it is generally also necessary to refer to the original measure and thus to 'specify' it. The scheme of the provision also militates against Article 6(1)(a) and (b) of Directive 2014/41 having different scopes of application. According to the introductory wording in paragraph 1, both rules concern 'an EIO' without differentiation. Article 6(2) and (3) of Directive 2014/41 also refers, without restriction, to both assessment steps under paragraph 1. Paragraph 2 expressly states that the conditions referred to in paragraph 1 – that is to say, the conditions under points (a) and (b) – are to be assessed 'in each case'. The distinction advocated by the Federal Court of Justice is also at odds with the conception of the EIO as a single instrument. Furthermore, not carrying out the assessment under Article 6(1)(b) of Directive 2014/41 would result in a failure to fulfil the objective pursued by the provision, of ensuring compliance with minimum national standards protecting the individual and preventing 'forum shopping'.

35 Even if, by contrast, Article 6(1)(b) of Directive 2014/41 were not to be applied to an EIO seeking a transfer of evidence as a matter of principle, the referring court considers that something different should apply in the situation in the present case. The surveillance of the German users, which was advocated by the German authorities in advance, in their own interests in conducting a criminal prosecution, and which was carried out by the French authorities in the interest of the German authorities, comes close to an investigative measure of the German authorities themselves, the ordering of which by means of an EIO would have been the natural course of action. In accordance with Article 6(1)(b) of Directive 2014/41, the lawfulness of that EIO would have had to have been assessed on the basis of German law of criminal procedure. The fact that informal forms of cooperation were initially used does not remove the need for protection addressed in Article 6(1)(b) of Directive 2014/41. This is all the more true given that there was no notification pursuant to Article 31(1) of Directive 2014/41, which would have likewise led to an examination under German law that would have been independent of exploitation interests and would have therefore guaranteed similar protection. The foregoing suggests that the assessment under Article 6(1)(b) of Directive 2014/41 should be extended to the subsequent EIO for obtaining evidence.

36 Questions 4(a) to (c): Paragraph 91g(6) of the IRG, which was created to implement Article 31(1) of Directive 2014/41, provides that the German authority must prohibit the implementation of the measure or the use of the data within 96 hours at the latest or must make the use subject to conditions if the measure would not be authorised in a similar domestic case. The IRG does not expressly state whether the notification of the planned interception measure is to be addressed to the public prosecutor's office or to the court. For the most part, it is assumed that the courts have competence.

37 In its decision of 2 March 2022 (5 StR 457/21, paragraph 41), the Federal Court of Justice doubted whether the French data gathering measure constituted interception of telecommunications within the meaning of Article 31(1) of

Directive 2014/41. By contrast, the referring court proceeds on the assumption that Article 31(1) of Directive 2014/41 is applicable in the present case and that the French authorities would have been obliged to notify the competent German authority (that is to say the competent court) of the planned infiltration of the German EncroChat terminal devices prior to the commencement of the measure. The concept of 'telecommunications' should be understood in a broad sense – in view also of the objective of Directive 2018/1979 of uniform treatment of all forms of electronic communication involving intensive interference (see recital 7). The concept of 'interception' within the meaning of Article 31(1) of Directive 2014/41 should also be interpreted broadly and cover any gathering of data from ongoing communications, in particular traffic data, location data or content, including through the use of malware on terminal devices.

38 Article 31(1) of Directive 2014/41 leaves, in principle, the determination of the 'competent authority' for the purpose of receiving the notification to the law of the Member State concerned by the interception. In the light of the fundamental rights under Articles 7, 8 and 11 of the Charter, however, the referring court is inclined towards the interpretation that 'competent authority' within the meaning of Article 31(1) of Directive 2014/41 can only be a body which acts independently of any instructions and is not interested in the data for investigative purposes – namely a court.

39 Article 31(1) and Article 6 of Directive 2014/41 have the same premiss of protection and aim to ensure compliance with national minimum standards of protection and respect for fundamental rights in the cross-border interception of telecommunications. Under both Article 6(1)(b) and Article 31(3) of Directive 2014/41, the measure must be reviewed on the basis of national law. The consideration of the Court of Justice in its judgment of 16 December 2021, *Spetsializirana prokuratura (Traffic and location data)* (C-724/19, EU:C:2021:1020, paragraph 34), that such an assessment can be carried out only by a court, is therefore also applicable to Article 31 of Directive 2014/41. The same applies to the judgment of the Court of Justice of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)*, (C-746/18, EU:C:2021:152, paragraph 51 et seq.), in accordance with which the balancing of the State's interest in pursuing criminal prosecution and the protection of fundamental rights may not be left to the investigating authorities which are interested in the data, but must be entrusted to a court which acts independently of any instructions.

40 Article 31(1) of Directive 2014/41 and Paragraph 91g of the IRG, which serves to implement that provision, protect the sovereignty of the State to be notified and take into account the particular sensitivity of fundamental rights towards secret access to the spoken word. The Federal Court of Justice (decision of 2 March 2022, 5 StR 457/21, paragraph 41) takes the view that the protection of individuals' fundamental rights concerned only the use of evidence abroad (*in casu*: France), but not, however, in the State to be notified (*in casu*: Germany). In addition, that regulatory objective was subordinate to the protection of national

sovereignty. By contrast, the referring court considers that, according to the conception of Article 31(1) and (3) of Directive 2014/41, the protection of the individuals concerned extends to any use of evidence for the purposes of criminal prosecution, whether domestically or abroad, and is at least equivalent to the protection of sovereignty.

41 Article 31 of Directive 2014/41 supplements the rules on EIOs to be executed and is intended to comprehensively prevent national levels of protection from being undermined by the transnational interception of telecommunications. The comparison with an EIO to be executed militates in favour of an extension of the protection of individuals to the use of evidence in the notified State. If the German authorities interested in the data of German users had issued an EIO extending the planned measure to German territory prior to the commencement of the measure, the protection of the fundamental rights of the German users would have been guaranteed via Article 6(1) of Directive 2014/41; that protection would also apply to the use of data by German criminal prosecution authorities.

42 In the case of cross-border measures in the common interest of several States, an EIO to be executed and the notification under Article 31 of Directive 2014/41 cannot be demarcated in a clear-cut manner; rather, they can be taken into account as alternatives. Moreover, with respect to the fundamental rights concerned and the severity of the interference, it makes no fundamental difference in which country or countries the data are collected, stored and used. Accordingly, it is the referring court's understanding that Article 31 of Directive 2014/41 must at least protect the persons concerned from the use of evidence in the country in whose interest the data are collected (*in casu*: Germany).

43 Questions 5(a) to (d): The German Code of Criminal Procedure does not contain an express provision on the use of illegally obtained evidence. According to settled case-law of the Federal Court of Justice, an (unwritten) prohibition of use requires that the infringed provision serves to protect the individual. Even then, however, it enters into consideration only in exceptional cases and on the basis of a comprehensive balancing exercise. In particular, the importance of the legal interests concerned and the severity of the infringement must be taken into account in that balancing exercise. Particular weight is always attached to procedural violations in the context of interception measures under Paragraph 100a et seq. of the StPO. A prohibition of the use of evidence is always a natural course of action in the case of a measure carried out without a court order (see BGH NJW 1999, 959, 961 with further references). Having regard to the principles of due process of law, a prohibition of use is always to be assumed if essential substantive requirements for ordering the interception measure were not met, and in particular if the suspicion that a catalogue offence under Paragraph 100a of the StPO had been committed did not exist from the outset. Only in special exceptional cases is a prohibition of use derived directly from the constitution possible without a finding of an infringement under ordinary law (see BGH, decision of 2 March 2022, 5 StR 457/21, paragraph 65 et seq.).

44 The decisions delivered so far by the higher and supreme courts all assume that EncroChat data can be used. In so far as infringements of EU law are assumed or at least considered, the interests of criminal prosecution are given priority in the balancing exercise, by reference to the seriousness of the criminal offences identified on the basis of the EncroChat data. As far as can be seen, the courts ruling on the substance are also not required to take account of this elsewhere – in particular in the assessment of evidence or the sentencing; the Federal Court of Justice has even expressly criticised the mitigating consideration of the infringement of Article 31 of Directive 2014/41 as erroneous (Federal Court of Justice, judgment of 3 August 2022, 5 StR 203/22, paragraph 19).

45 According to settled case-law of the Court of Justice, it is in principle for national law to regulate the legal consequences of infringements of EU law. However, the procedural autonomy of the Member States is limited by the principle of effectiveness (judgment of the Court of Justice of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)*, C-746/18, EU:C:2021:152, paragraph 42 et seq. and the case-law cited): According to that judgment, national law must ensure that the accused person does not suffer any unreasonable disadvantages in criminal proceedings as a result of information and evidence unlawfully obtained, which can be achieved not only by prohibiting the use of evidence, but also by taking the infringements of the law into account when assessing evidence or determining the sentence. Nevertheless, according to the case-law of the Court of Justice, the principle of effectiveness may, in individual cases, oblige the national court to exclude unlawfully obtained evidence from the proceedings (judgment of 20 September 2022, *VD and SR*, C-339/20 and C-397/20, EU:C:2022:703, paragraph 106 and the case-law cited; fundamental judgment of 10 April 2003, *Steffensen*, C-276/01, EU:C:2003:228, paragraph 77 et seq.). In the view of the referring court, this means that the infringement in such a case must always result in the exclusion of the evidence under EU law, without any balancing against national interests in pursuing criminal prosecution.

46 There are grounds to take the view that a prohibition of use derived directly from the principle of effectiveness under EU law is to be assumed in the present case also, since the principle of a right to a fair trial has been undermined in several respects: the very fact that the data requested by way of the EIO cannot be examined by a technical expert because of French secrecy is likely to fulfil the conditions developed by the Court of Justice in the judgment of 10 April 2003, *Steffensen*, C-276/01, EU:C:2003:228, under which the court must exclude evidence. In addition, there are the multiple breaches of formal and substantive safeguards under Article 31 and Article 6 of Directive 2014/41, for which the German law criminal prosecution authorities are directly responsible or to which they have at least turned a blind eye. Furthermore, the European agencies and the German criminal prosecution authorities have further impeded the investigation of the facts and the defence by refusing to hand over parts of the case file that are of importance for the defence and to include documents relevant to the proceedings in the case file in the first place. The refusal to file the messages exchanged via the SIENA system has a particularly serious effect in that respect. The

withholding of essential information from the investigating judge, as announced in the BKA's letter of 13 May 2020, also fits into that context, since the task of the investigating judge, which follows from the rule of law, to examine the investigations under its own responsibility was undermined. Overall, an independent external review of the gathering and further use of the data was prevented at all stages of the procedure.

47 The autonomy of the Member States in regulating the legal consequences of infringements of EU law is further limited by the principle of equivalence. According to that principle, infringements of EU law may not be sanctioned to a lesser extent than similar infringements of domestic law (Court of Justice, judgment of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)*, C-746/18, EU:C:2021:152, paragraph 42). A mandatory prohibition of use enters into consideration from that point of view also. This is because, under German law of criminal procedure, in the case of a interception measure, both the breach of the requirement for judicial authorisation and the lack of a concrete suspicion that a catalogue offence had been committed would result in the data being unusable. In so far as, by contrast, EU law does not provide for a mandatory prohibition of use, German law of criminal procedure requires a comprehensive weighing of interests.

48 The Federal Court of Justice attaches decisive importance to the weight of the criminal offences to be investigated and concludes from this that the State's interest in pursuing criminal prosecution enjoys priority over the protection of the individual EncroChat users concerned (see Federal Court of Justice, decision of 2 March 2022, 5 StR 457/21, paragraphs 36, 44, 57). The referring court has doubts as to whether that line of argument is compatible with EU law. The Court of Justice has held on several occasions that the objective of combating serious crime cannot justify general and indiscriminate retention of data (judgments of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)*, C-746/18, EU:C:2021:152, paragraph 50, and 5 April 2022, *Commissioner of An Garda Síochána*, C-140/20, EU:C:2022:258, paragraph 65 and the case-law cited). This applies all the more so if, as in the present case, there is a certain probability that persons subject to professional secrecy – such as lawyers and journalists – are also affected by the data gathering (see Court of Justice, judgment of 20 September 2022, *SpaceNet*, C-793/19 and C-794/19, EU:C:2022:702, paragraph 82) and communication content is covered.

49 It could be contrary to that evaluation and the principle of effectiveness if a breach of the law stemming directly from the lack of a suspicion of an offence remains unpunished, by reference to subsequent findings from the data unlawfully obtained. Accordingly, the referring court is inclined to the view that, in weighing up whether data obtained without sufficient suspicion of an offence can be used despite the infringement of Article 6(1)(a) and (b) of Directive 2014/41, the weight of the specific offences in question may be taken into account only with reduced weight, with the consequence that, in the case of an interference with high-ranking fundamental rights, that aspect alone cannot outweigh the

infringement of the law and therefore cannot justify the use. A comparable argument can be made with regard to Article 31(1) of Directive 2014/41: the seriousness of the infringement results from the fact that the competent German court would have prohibited the measure due to the lack of suspicion of an offence.

50 Need for expedition: The Court of Justice is requested to deal with the case under the expedited procedure pursuant to Article 105(1) of the Rules of Procedure or, in the alternative, on a priority basis, as it is a case involving detention, even if the arrest warrant is not currently being executed. The decision of the Court of Justice is also of importance to a large number of similar proceedings.