Reports of Cases

JUDGMENT OF THE COURT (Grand Chamber)

30 April 2024*

(Reference for a preliminary ruling – Judicial cooperation in criminal matters – Directive 2014/41/EU – European Investigation Order (EIO) in criminal matters – Obtaining of evidence already in the possession of the competent authorities of the executing State – Conditions for issuing an EIO – Encrypted telecommunications service – EncroChat – Need for the decision of a judge – Use of evidence obtained in breach of EU law)

In Case C-670/22,

REQUEST for a preliminary ruling under Article 267 TFEU from the Landgericht Berlin (Regional Court, Berlin, Germany), made by decision of 19 October 2022, received at the Court on 24 October 2022, in the criminal proceedings against

**M.N.,**

THE COURT (Grand Chamber),

composed of K. Lenaerts, President, L. Bay Larsen, Vice-President, A. Prechal, K. Jürimäe (Rapporteur), C. Lycourgos, T. von Danwitz, Z. Csehi and O. Spineanu-Matei, Presidents of Chambers, M. Ilešič, J.-C. Bonichot, I. Jarukaitis, A. Kumin, D. Gratsias, M.L. Arastey Sahún and M. Gavalec, Judges,

Advocate General: T. Ćapeta,

Registrar: D. Dittert, Head of Unit, and K. Hötzel, Administrator,

having regard to the written procedure and further to the hearing on 4 July 2023,

after considering the observations submitted on behalf of:

– Staatsanwaltschaft Berlin, by R. Pützhoven and J. Raupach, acting as Agents,

– M.N., by S. Conen, Rechtsanwalt,

– the German Government, by J. Möller, P. Busche and M. Hellmann, acting as Agents,

– the Czech Government, by L. Halajová, M. Smolek and T. Suchá, acting as Agents,

– the Estonian Government, by M. Kriisa, acting as Agent,

* Language of the case: German.

– Ireland, by M. Browne, Chief State Solicitor, M.A. Joyce and D. O'Reilly, acting as Agents, and by D. Fennelly, Barrister-at-Law,

– the Spanish Government, by A. Gavela Llopis and A. Pérez-Zurita Gutiérrez, acting as Agents,

– the French Government, by G. Bain, R. Bénard, B. Dourthe, B. Fodda and T. Stéhelin, acting as Agents,

– the Hungarian Government, by M.Z. Fehér, acting as Agent,

– the Netherlands Government, by M.K. Bulterman, A. Hanje and J. Langer, acting as Agents,

– the Polish Government, by B. Majczyna, acting as Agent,

– the Swedish Government, by F.-L. Göransson and H. Shev, acting as Agents,

– the European Commission, by H. Leupold, M. Wasmeier and F. Wilman, acting as Agents,

after hearing the Opinion of the Advocate General at the sitting on 26 October 2023,

gives the following

## Judgment

1 This request for a preliminary ruling concerns the interpretation of Article 2(c), Article 6(1) and Article 31 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 (OJ 2014 L 130, p. 1), and of the principles of equivalence and effectiveness.

2 The request has been made in the context of the criminal proceedings brought against M.N. and concerns the lawfulness of three European Investigation Orders issued by the Generalstaatsanwaltschaft Frankfurt am Main (Public Prosecutor's Office, Frankfurt am Main, Germany) ('the Frankfurt Public Prosecutor's Office').

## Legal context

### *European Union law*

#### *Directive 2002/58/EC*

3 Article 15(1) of 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) states:

'Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic

society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC [of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31)]. … All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) [TEU].'

*Directive 2014/41*

4 Recitals 2, 5 to 8, 19 and 30 of Directive 2014/41 are worded as follows:

'(2) Pursuant to Article 82(1) [TFEU], judicial cooperation in criminal matters in the [European] Union is to be based on the principle of mutual recognition of judgments and judicial decisions, which is, since the Tampere European Council of 15 and 16 October 1999, commonly referred to as a cornerstone of judicial cooperation in criminal matters within the Union.

…

(5) Since the adoption of [Council] Framework Decisions 2003/577/JHA [of 22 July 2003 on the execution in the European Union of orders freezing property or evidence (OJ 2003 L 196, p. 45)] and 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)], it has become clear that the existing framework for the gathering of evidence is too fragmented and complicated. A new approach is therefore necessary.

(6) In the Stockholm Programme adopted by the European Council of 10-11 December 2009, the European Council considered that the setting up of a comprehensive system for obtaining evidence in cases with a cross-border dimension, based on the principle of mutual recognition, should be further pursued. The European Council indicated that the existing instruments in this area constituted a fragmentary regime and that a new approach was needed, based on the principle of mutual recognition, but also taking into account the flexibility of the traditional system of mutual legal assistance. The European Council therefore called for a comprehensive system to replace all the existing instruments in this area, including Framework Decision 2008/978/JHA, covering as far as possible all types of evidence, containing time limits for enforcement and limiting as far as possible the grounds for refusal.

(7) This new approach is based on a single instrument called the European Investigation Order (EIO). An EIO is to be issued for the purpose of having one or several specific investigative measure(s) carried out in the State executing the EIO ("the executing State") with a view to gathering evidence. This includes the obtaining of evidence that is already in the possession of the executing authority.

(8) The EIO should have a horizontal scope and therefore should apply to all investigative measures aimed at gathering evidence. However, the setting up of a joint investigation team and the gathering of evidence within such a team require specific rules which are better dealt with separately. Without prejudice to the application of this Directive, existing instruments should therefore continue to apply to this type of investigative measure.

…

(19) The creation of an area of freedom, security and justice within the Union is based on mutual confidence and a presumption of compliance by other Member States with Union law and, in particular, with fundamental rights. However, that presumption is rebuttable. Consequently, if there are substantial grounds for believing that the execution of an investigative measure indicated in the EIO would result in a breach of a fundamental right of the person concerned and that the executing State would disregard its obligations concerning the protection of fundamental rights recognised in the Charter [of Fundamental Rights of the European Union ("the Charter")], the execution of the EIO should be refused.

…

(30) Possibilities to cooperate under this Directive on the interception of telecommunications should not be limited to the content of the telecommunications, but could also cover collection of traffic and location data associated with such telecommunications, allowing competent authorities to issue an EIO for the purpose of obtaining less intrusive data on telecommunications. An EIO issued to obtain historical traffic and location data related to telecommunications should be dealt with under the general regime related to the execution of the EIO and may be considered, depending on the national law of the executing State, as a coercive investigative measure.'

5 Under the heading 'The European Investigation Order and obligation to execute it', Article 1 of that directive states:

'1. A European Investigation Order (EIO) is a judicial decision which has been issued or validated by a judicial authority of a Member State ("the issuing State") to have one or several specific investigative measure(s) carried out in another Member State ("the executing State") to obtain evidence in accordance with this Directive.

The EIO may also be issued for obtaining evidence that is already in the possession of the competent authorities of the executing State.

2. Member States shall execute an EIO on the basis of the principle of mutual recognition and in accordance with this Directive.'

6 Article 2 of that directive, headed, 'Definitions', provides:

'For the purposes of this Directive the following definitions apply:

…

(c) "issuing authority" means:
(i) a judge, a court, an investigating judge or a public prosecutor competent in the case concerned; or
(ii) any other competent authority as defined by the issuing State which, in the specific case, is acting in its capacity as an investigating authority in criminal proceedings with competence to order the gathering of evidence in accordance with national law. In addition, before it is transmitted to the executing authority the EIO shall be validated,

after examination of its conformity with the conditions for issuing an EIO under this Directive, in particular the conditions set out in Article 6.1, by a judge, court, investigating judge or a public prosecutor in the issuing State. Where the EIO has been validated by a judicial authority, that authority may also be regarded as an issuing authority for the purposes of transmission of the EIO;

(d) "executing authority" means an authority having competence to recognise an EIO and ensure its execution in accordance with this Directive and the procedures applicable in a similar domestic case. Such procedures may require a court authorisation in the executing State where provided by its national law.'

7 Article 4 of Directive 2014/41, headed 'Types of proceedings for which the EIO can be issued', states:

'An EIO may be issued:

(a) with respect to criminal proceedings that are brought by, or that may be brought before, a judicial authority in respect of a criminal offence under the national law of the issuing State;

…'

8 Article 6 of Directive 2014/41, headed 'Conditions for issuing and transmitting an EIO', provides:

'1. 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.

2. The conditions referred to in paragraph 1 shall be assessed by the issuing authority in each case.

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

9 Article 14 of that directive, headed 'Legal remedies', is worded as follows:

'1. Member States shall ensure that legal remedies equivalent to those available in a similar domestic case, are applicable to the investigative measures indicated in the EIO.

…

7. The issuing State shall take into account a successful challenge against the recognition or execution of an EIO in accordance with its own national law. 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.'

10 Article 30 of that directive, headed 'Interception of telecommunications with technical assistance of another Member State', states:

'1. An EIO may be issued for the interception of telecommunications in the Member State from which technical assistance is needed.

…

7. When issuing an EIO referred to in paragraph 1 or during the interception, the issuing authority may, where it has a particular reason to do so, also request a transcription, decoding or decrypting of the recording subject to the agreement of the executing authority.

8. Costs resulting from the application of this Article shall be borne in accordance with Article 21, except for the costs arising from the transcription, decoding and decrypting of the intercepted communications which shall be borne by the issuing State.'

11 Article 31 of the directive, headed 'Notification of the Member State where the subject of the interception is located from which no technical assistance is needed', provides:

'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.

3. The competent authority of the notified Member States may, in case where the interception would not be authorised in a similar domestic case, notify, without delay and at the latest within 96 hours after the receipt of the notification referred to in paragraph 1, the competent authority of the intercepting Member State:

(a) that the interception may not be carried out or shall be terminated; and

(b) where necessary, that any material already intercepted while the subject of the interception was on its territory may not be used, or may only be used under conditions which it shall specify. The competent authority of the notified Member State shall inform the competent authority of the intercepting Member State of reasons justifying those conditions.

…'

12 Article 33 of Directive 2014/41, headed 'Notifications', sets out in paragraph 1 the information that must be notified and made available to all the Member States and to the European Judicial Network (EJN) created by Joint Action 98/428/JHA of 29 June 1998 adopted by the Council on the basis of Article K.3 [EU], on the creation of a European Judicial Network (OJ 1998 L 191, p. 4).

### *German law*

13 The interception of telecommunications for the purposes of criminal prosecution is governed by the Strafprozessordnung (StPO) (Code of Criminal Procedure) ('the StPO').

14 The first, second and third sentences of Paragraph 100a(1) of the StPO permit, respectively, the monitoring of ongoing communications through 'conventional' monitoring of telecommunications, the surveillance of ongoing communications through the installation of spyware on terminal devices (interception of telecommunications at source) and the capture of communications transmitted and already stored on a device at the time when the decision of the Landgericht (regional court, Germany) ordering the measure concerned (limited online surveillance) is issued. Under Paragraph 100b of the StPO, it is possible to read all the data stored on a terminal device (online surveillance).

15 All of those measures presuppose the existence of a concrete suspicion that a criminal offence has been committed, albeit that the category of offences covered is limited to those listed in Paragraph 100a(2) and Paragraph 100b(2) of the StPO.

16 Under Paragraph 100e(1) and (2) of the StPO, those measures may, moreover, be ordered by the competent Landgericht (regional court) only upon the application of the relevant public prosecutor's office. In accordance with Paragraph 100e(2) of the StPO, in conjunction with Paragraph 74a(4) of the Gerichtsverfassungsgesetz (GVG) (Law on the organisation of the courts) of 12 September 1950 (BGBl. 1950 I, p. 455), online surveillance comes within the exclusive competence of a special chamber of that Landgericht (regional court).

17 The Gesetz über die internationale Rechtshilfe in Strafsachen (IRG) (Law on international mutual legal assistance in criminal matters) of 23 December 1982 (BGBl. 1982 I, p. 2071), in the version applicable to the dispute in the main proceedings ('the IRG'), does not expressly determine the authority that is competent to issue EIOs. By reference to Paragraph 161 of the StPO, an EIO for the monitoring of telecommunications in a foreign country may thus be issued by the public prosecutor's office in the course of the investigation prior to a person being charged.

18 Paragraph 91g(6) of the IRG, which transposes Article 31 of Directive 2014/41 into German law, provides that the competent authority, to which a Member State is to notify its intention to carry out an interception measure on German territory, must prohibit the implementation of that measure, or the use of any material already intercepted, at the latest within 96 hours or attach conditions to the use of those data if that measure would not be authorised in a similar domestic case. However, the IRG does not specify whether that measure must be notified to the competent Landgericht (regional court) or to the relevant public prosecutor's office. Paragraph 92d of the IRG governs only the territorial competence of the competent authority.

## The dispute in the main proceedings and the questions referred for a preliminary ruling

19 In the context of an investigation carried out by the French authorities, it appeared that accused persons were using encrypted mobile phones that operated under an 'EncroChat' licence in order to commit offences primarily related to drug trafficking. Those mobile phones had special software and modified hardware that enabled end-to-end encrypted communication, via a server in Roubaix (France), that could not be intercepted by conventional investigative means ('the EncroChat service').

20 With the authorisation of a judge, the French police were able to secure data from that server in 2018 and 2019. Those data enabled a joint investigation team, which included experts from the Netherlands, to develop a piece of Trojan software. With the authorisation of the tribunal correctionnel de Lille (Criminal Court, Lille, France), that software was uploaded to the server in the spring of 2020 and, from there, was installed on those mobile phones via a simulated update. Of a total of 66 134 subscribed users, 32 477 users in 122 countries are said to have been affected by that software, including approximately 4 600 users in Germany.

21 On 9 March 2020, representatives of the Bundeskriminalamt (Federal Criminal Police Office, Germany) ('the BKA') and of the Frankfurt Public Prosecutor's Office, as well as representatives, inter alia, of the French, Netherlands and United Kingdom authorities, participated in a videoconference organised by the European Union Agency for Criminal Justice Cooperation (Eurojust). During that videoconference, the representatives of the French and Netherlands authorities informed the representatives of the other Member States' authorities of their investigation of an encrypted mobile phone operating company and of their planned interception of data, including data from mobile phones located outside French territory. The representatives of the German authorities signalled their interest in the data of the German users.

22 In a note dated 13 March 2020, the BKA announced that it was opening an investigation in respect of all unknown users of the EncroChat service, on suspicion of engaging in organised trafficking in substantial quantities of narcotic drugs and of forming a criminal association. The BKA justified the opening of that investigation by explaining that the use of the EncroChat service in itself gave rise to a suspicion that serious criminal offences were being committed, in particular the organisation of drug trafficking.

23 On the basis of that note, on 20 March 2020, the Frankfurt Public Prosecutor's Office opened an 'urgent' investigation in respect of X ('the UJs proceedings').

24 On 27 March 2020, the BKA received, via the Secure Information Exchange Network Application (SIENA) of the European Union Agency for Law Enforcement Cooperation (Europol), a message from the joint investigation team addressed to the police authorities of the Member States interested in the EncroChat service data. The competent authorities of those Member States were requested to confirm in writing that they had been informed of the methods used to gather data from mobile phones in their territory. They were also required to ensure that data transmitted would be transmitted, in principle, initially only for analysis purposes and would be used for ongoing investigations only after approval by the Member States of the joint investigation team. According to the referring court, the requested confirmations were transmitted by the BKA in agreement with the Frankfurt Public Prosecutor's Office.

25 Between 3 April and 28 June 2020, the BKA retrieved the data which were made available on the Europol server on a daily basis relating to mobile phones used in Germany.

26 On 2 June 2020, within the framework of the UJs proceedings, the Frankfurt Public Prosecutor's Office requested authorisation from the French authorities, by way of an initial EIO, to use the data from the EncroChat service without restriction in criminal proceedings. It justified its request by explaining that the BKA had been informed by Europol that a large number of very serious criminal offences, including the import and trafficking of a substantial quantity of narcotic drugs, were being committed in Germany with the aid of mobile phones equipped with that service, and that as yet unidentified persons were suspected of planning and committing very serious offences in Germany using encrypted communications.

27 Following that request, the tribunal correctionnel de Lille (Criminal Court, Lille) authorised the transmission and use in judicial proceedings of the data from German users' mobile phones that were equipped with the EncroChat service. Further data were transmitted subsequently on the basis of two supplementary EIOs dated 9 September 2020 and 2 July 2021, respectively (together with the EIO of 2 June 2020, 'the EIOs').

28 The Frankfurt Public Prosecutor's Office subsequently divided the UJs proceedings and reassigned the investigations in respect of certain users, including M.N., to local public prosecutor's offices. It is against that background that the Landgericht Berlin (Regional Court, Berlin, Germany), which is the referring court, queries the lawfulness of the EIOs in the light of Directive 2014/41.

29 By the first set of three questions, the referring court seeks to determine which authority was competent to issue the EIOs.

30 In that regard, it states that, in an order of 2 March 2022 made in Case 5 StR 457/21 (DE:BGH:2022:020322B5STRT457.21.0), the Bundesgerichtshof (Federal Court of Justice, Germany) ruled that the Frankfurt Public Prosecutor's Office, which was investigating in the UJs proceedings, was competent to issue EIOs for the transmission of evidence ('the order of the Federal Court of Justice of 2 March 2022'). The referring court does not agree with that interpretation. It prefers the view that, under Article 6(1) of Directive 2014/41, in conjunction with Article 2(c) of that directive, only a court could have made the EIOs.

31 The referring court invokes, in that regard, the judgments of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)* (C-746/18, EU:C:2021:152), and of 16 December 2021, *Spetsializirana prokuratura (Traffic and location data)* (C-724/19, EU:C:2021:1020). It relies, more specifically, on the statements made by the Court, in the case-law arising from those judgments, 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. According to the referring court, that case-law can be applied to the interpretation of Article 6(1)(a) of Directive 2014/41.

32 The German prosecuting authorities' access to the EncroChat service data by means of the EIOs should be subject to the same criteria as those governing access to data retained pursuant to Article 15(1) of Directive 2002/58. The fact that the EncroChat service data were not secured by a telecommunications operator under an administrative order, but were collected directly by the French prosecuting authorities, does not, in its view, warrant a different assessment. On the contrary, that fact reinforces the interference with the fundamental rights of the persons concerned.

33 Furthermore, according to the referring court, it is apparent from Article 2(c) of Directive 2014/41 that an EIO for the purposes of criminal prosecution should, irrespective of the national rules of jurisdiction in a similar domestic situation, always be issued by a judge who is not responsible for specific investigative measures, where the assessment of proportionality under Article 6(1)(a) of that directive calls for a complex balancing of the interests involved and concerns serious interference with fundamental rights.

34 The second and third sets of questions raised by the referring court concern the substantive conditions to which the issuing of an EIO is subject.

35 The referring court considers, in the first place, that an EIO seeking access to data from the interception of telecommunications for the purposes of criminal prosecution does not satisfy the conditions of necessity and proportionality set out in Article 6(1)(a) of Directive 2014/41 unless there is, in respect of each person concerned, a suspicion, based on concrete facts, of that person's involvement in a serious criminal offence.

36 The referring court does not, in that respect, agree with the conclusion of the order of the Federal Court of Justice of 2 March 2022, according to which the mere – unspecified – suspicion of multiple criminal offences is sufficient for EIOs to be issued. Its doubts stem from the case-law of the Court relating to the legality of the retention of data, in particular the findings as to proportionality, for the purposes of Article 15(1) of Directive 2002/58, and it relies in that regard on the judgments of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)* (C-746/18, EU:C:2021:152, paragraphs 39, 40 and 50), and of 5 April 2022, *Commissioner of An Garda Síochána and Others* (C-140/20, EU:C:2022:258, paragraph 44). It cannot, in that respect, be countered that the national rules of criminal procedure provide sufficient safeguards for the protection of the fundamental rights of the persons concerned in the context of the national proceedings.

37 The issue of the proportionality of an EIO has also prompted the referring court to raise questions with regard to the right to a fair trial guaranteed in the second paragraph of Article 47 of the Charter and Article 6(1) of the Convention for the Protection of Human Rights and Fundamental Freedoms, signed in Rome on 4 November 1950. It states that that right requires that a party to judicial proceedings should have a real opportunity to comment on a piece of evidence. This is particularly the case where the evidence pertains to a technical field in which the competent court and the party to the proceedings have no expert knowledge.

38 In the second place, the referring court recalls that, in accordance with Article 6(1)(b) of Directive 2014/41, the issuing authority must review the measure indicated in the EIO in the light of national law.

39 However, in the order of the Federal Court of Justice of 2 March 2022, that provision was found to be inapplicable in the case in the main proceedings. It was found to cover only an EIO aimed at gathering evidence which had yet to be executed, and was not applicable to an EIO that merely sought a transfer of evidence that had already been gathered. The review of the measure in the light of national law was therefore superfluous.

40 The referring court considers, on the contrary, that the issuing authority in respect of an EIO must, in that situation, review the investigative measure underlying the data collection in the light of national law. In other words, the issuing authority may request, by way of an EIO, evidence gathered in the executing State only if the investigative measure by which that evidence was gathered would have been authorised in the issuing State in a similar domestic case.

41 The fourth set of questions raised by the referring court concerns the interpretation of Article 31 of Directive 2014/41.

42 The referring court considers that where a Member State wishes to intercept the telecommunications of persons who are located in Germany, it must, in accordance with that article, notify the planned interception to the competent German authority before starting to implement the measure or immediately after becoming aware of where those persons are located.

43 In the order of the Federal Court of Justice of 2 March 2022, doubt was cast on the fact that the French data-extraction measure constituted an 'interception of telecommunications' within the meaning of Article 31(1) of Directive 2014/41. The referring court takes a different view. It considers that the French investigating authorities should have notified the infiltration of German mobile phones equipped with the EncroChat service to the competent German authority before proceeding with the infiltration.

44 However, while German legislation determines the territorial competence of that authority, it does not specify whether any such notification is to be addressed to a Landgericht (regional court) or to the relevant public prosecutor's office. There is some disagreement on this point in German case-law and academic writings. The referring court would favour interpreting the concept of 'competent authority' in Article 31(1) of Directive 2014/41 as designating only an independent body that has no interest in the data for investigative purposes, that is to say, a court.

45 In the case of cross-border measures that are carried out at EU level and implemented in the interests of several Member States at the same time, the concepts of an 'EIO', within the meaning of Article 2(c) of Directive 2014/41, and of 'notification' as referred to in Article 31 of that directive, are largely interchangeable, according to the referring court. That would therefore militate in favour of the competences of the authorities responsible for those measures being aligned.

46 The referring court also raises questions concerning the objective of protecting the Member States' sovereignty, which is said to be pursued in Article 31 of Directive 2014/41, in view of the particular sensitivity of covert interference with communications.

47 The fifth set of questions raised concerns the consequences of a possible infringement of EU law in the light of the principles of equivalence and effectiveness.

48 The referring court notes that the national decisions delivered in respect of data derived from the use of the EncroChat service assume that the data can be used and that, in so far as infringements of EU law are conceivable, priority must nevertheless be given to criminal prosecutions in view of the seriousness of the offences identified on the basis of those data.

49 It expresses doubts, however, as to the conformity of that approach with EU law, in particular with the principles of equivalence and effectiveness.

50 As regards the principle of equivalence, the referring court notes that, under the German rules of criminal procedure, data collected by means of a phone-tapping measure adopted in disregard of the competence reserved to the relevant judge and in the absence of a concrete suspicion of a listed offence would have been unusable.

51 As regards the principle of effectiveness, the referring court observes that it is apparent from the judgment of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)* (C-746/18, EU:C:2021:152, paragraph 43), that the objective of preventing information and evidence obtained unlawfully from unduly prejudicing a person who is suspected of having committed criminal offences could be achieved not only by prohibiting the use of such information and evidence, but also by factoring in whether that material is unlawful when assessing the evidence or determining the sentence.

52 According to the referring court, the prohibition on using that evidence derives directly from the principle of the effectiveness of EU law. That prohibition applied in the case in the main proceedings since the general principle of a right to a fair trial was undermined in several respects, in particular by the fact that the data requested by way of the EIOs could not be examined by a technical expert because of the 'defence secrets' classification conferred on them by the French authorities.

53 Moreover, the referring court infers from the judgments 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 141); of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)* (C-746/18, EU:C:2021:152, paragraph 50); and of 5 April 2022, *Commissioner of An Garda Síochána and Others* (C-140/20, EU:C:2022:258, paragraph 65), that the objective of combating serious crime cannot justify a general and indiscriminate retention of personal data. Personal data that are retained unlawfully and without a reason cannot subsequently be accessed by prosecuting authorities, even if the data must serve to shed light on serious offences in a specific case.

54 In those circumstances, the Landgericht Berlin (Regional Court, Berlin) decided to stay the proceedings and to refer 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 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?'

**Procedure before the Court**

55 The referring court requested that the present reference for a preliminary ruling be dealt with pursuant to the expedited procedure under Article 105 of the Rules of Procedure of the Court of Justice.

56 In support of its request, it states that the case in the main proceedings calls for particular urgency. Although the national arrest warrant issued in respect of M.N. is not currently being executed, any avoidable delay in the proceedings that is attributable to the State could result in the cancellation of that arrest warrant. The decision of the Court is, moreover, relevant to a large number of similar pending proceedings.

57 Article 105(1) of the Rules of Procedure provides that, at the request of the referring court or tribunal or, exceptionally, of his own motion, the President of the Court may, where the nature of the case requires that it be dealt with within a short time, after hearing the Judge-Rapporteur and the Advocate General, decide that a reference for a preliminary ruling is to be determined pursuant to an expedited procedure derogating from the provisions of those rules.

58 It must be borne in mind, in that regard, that such an expedited procedure is a procedural instrument intended to address matters of exceptional urgency (judgment of 21 December 2021, *Randstad Italia*, C-497/20, EU:C:2021:1037, paragraph 37 and the case-law cited).

59 In the present case, the President of the Court decided, on 16 November 2022, after hearing the Judge-Rapporteur and the Advocate General, to refuse the request referred to in paragraph 55 of the present judgment.

60 First, since M.N. is not deprived of his liberty, the fact that the referring court is required to do everything possible to ensure that the case in the main proceedings is resolved swiftly is not sufficient to justify the use of an expedited procedure under Article 105(1) of the Rules of Procedure (see, to that effect, orders of the President of the Court of 7 October 2013, *Rabal Cañas*, C-392/13, EU:C:2013:877, paragraph 15, and of 20 September 2018, *Minister for Justice and Equality*, C-508/18 and C-509/18, EU:C:2018:766, paragraph 13, and also judgment of 13 July 2023, *Ferrovienord*, C-363/21 and C-364/21, EU:C:2023:563, paragraph 46).

61 Secondly, the importance of the questions or the fact that a large number of persons or legal situations are potentially concerned by those questions is not, as such, a reason that establishes exceptional urgency, which is, however, necessary to justify an expedited procedure (order of the

President of the Court of 21 September 2004, *Parliament* v *Council*, C-317/04, EU:C:2004:834, paragraph 11, and judgment of 21 December 2023, *GN (Ground for refusal based on the best interests of the child)*, C-261/22, EU:C:2023:1017, paragraph 30).

62 However, the President of the Court decided that the present case would be given priority, pursuant to Article 53(3) of the Rules of Procedure.

**Admissibility of the request for a preliminary ruling**

63 The Staatsanwaltschaft Berlin (Public Prosecutor's Office, Berlin, Germany) and a number of the governments that lodged observations with the Court submit that certain questions are inadmissible since they are, in essence, either hypothetical or too general or concern an assessment of the facts or of national legislation.

64 According to settled case-law, in proceedings under Article 267 TFEU, it is solely for the national court before which the dispute has been brought, and which must assume responsibility for the subsequent judicial decision, to determine in the light of the particular circumstances of the case both the need for a preliminary ruling in order to enable it to deliver judgment and the relevance of the questions which it submits to the Court (see, to that effect, judgment of 16 December 1981, *Foglia*, 244/80, EU:C:1981:302, paragraph 15). Consequently, where the questions submitted by the national court concern the interpretation of EU law, the Court of Justice is, in principle, bound to give a ruling (judgment of 20 September 2022, *VD and SR*, C-339/20 and C-397/20, EU:C:2022:703, paragraph 56).

65 The Court may refuse to rule on a question referred for a preliminary ruling by a national court only where it is quite obvious that the interpretation of EU law that is sought bears no relation to the actual facts of the main action or its purpose, where the problem is hypothetical, or where the Court does not have before it the factual or legal material necessary to give a useful answer to the questions submitted to it (see, to that effect, judgments of 15 December 1995, *Bosman*, C-415/93, EU:C:1995:463, paragraph 61, and of 20 September 2022, *VD and SR*, C-339/20 and C-397/20, EU:C:2022:703, paragraph 57).

66 In the present case, it is, admittedly, apparent from the order for reference that some of the concerns of the referring court do indeed arise from national law and that certain findings of fact have yet to be made by that court.

67 However, it follows from settled case-law that national courts are free to exercise the discretion to refer matters to the Court at whatever stage of the proceedings they consider appropriate. The choice of the most appropriate time to refer a question for a preliminary ruling lies within their exclusive jurisdiction (see, to that effect, judgment of 5 July 2016, *Ognyanov*, C-614/14, EU:C:2016:514, paragraph 17 and the case-law cited).

68 Moreover, it must be noted that the questions referred for a preliminary ruling concern the interpretation of provisions of EU law that are clearly identified and to which, according to the referring court, the resolution of the dispute in the main proceedings is subject. In those circumstances, given that the arguments relied on by the Berlin Public Prosecutor's Office and the governments referred to in paragraph 63 of the present judgment are not sufficient to

establish that it is quite obvious that that interpretation bears no relation to the actual facts of the main action or its purpose, a reply from the Court to the questions raised appears necessary for the purposes of the decision to be given in the main proceedings.

## Consideration of the questions referred

### *Question 1*

69 By Question 1, the referring court asks, in essence, whether Article 2(c) and Article 6(1) of Directive 2014/41 must be interpreted as meaning that an EIO for the transmission of evidence already in the possession of the competent authorities of the executing State must necessarily be issued by a judge where, under the law of the issuing State, the initial gathering of that evidence would have had to be ordered by a judge in a purely domestic case in the issuing State.

70 As a preliminary point, it must be noted that while Article 6(1) of Directive 2014/41 helps to define the conditions for issuing an EIO, it does not determine the nature of the authority that may issue such an order.

71 In that regard, it follows from Article 1(1) of Directive 2014/41 that an EIO may be issued in two situations. An EIO may thus seek, first, to have one or several specific investigative measures carried out in another Member State to obtain evidence or, secondly, to obtain evidence that is already in the possession of the competent authorities of the executing State, that is to say, to have that evidence transmitted to the competent authorities of the issuing State. In both cases, it is apparent from that provision that an EIO must be issued or validated by a 'judicial authority'.

72 The concept of 'judicial authority' used in that provision is not, however, defined there. According to the case-law of the Court, in that context, Article 1(1) of Directive 2014/41 should be read in conjunction with Article 2(c) thereof, which defines, for the purposes of that directive, the concept of 'issuing authority' (see, to that effect, judgment of 2 March 2023, *Staatsanwaltschaft Graz (Düsseldorf Tax Office for Criminal Tax Matters)*, C-16/22, EU:C:2023:148, paragraphs 27 and 28).

73 In that regard, it is clear from its wording that Article 2(c)(i) of that directive expressly provides that a public prosecutor is included among the authorities which, like a judge, court or investigating judge, are understood to be an 'issuing authority'. That provision makes classification as an 'issuing authority' subject to the sole condition that the court and the persons acting as judge, investigating judge or public prosecutor should have competence in the case concerned (judgment of 8 December 2020, *Staatsanwaltschaft Wien (Falsified transfer orders)*, C-584/19, EU:C:2020:1002, paragraphs 50 and 51).

74 Accordingly, in so far as, under the law of the issuing State, a public prosecutor is competent, in a purely domestic situation in that State, to order an investigative measure for the transmission of evidence already in the possession of the competent national authorities, that public prosecutor is covered by the concept of 'issuing authority', within the meaning of Article 2(c)(i) of Directive 2014/41, for the purposes of issuing an EIO for the transmission of evidence that is already in the possession of the competent authorities of the executing State (see, by analogy, judgment of 8 December 2020, *Staatsanwaltschaft Wien (Falsified transfer orders)*, C-584/19, EU:C:2020:1002, paragraph 52).

75 However, where, under the law of the issuing State, a public prosecutor is not competent to order such a measure for the transmission of evidence already in the possession of the competent national authorities – and therefore in particular where, in a purely domestic situation, such transmission would have to be authorised by a judge because it involves serious interference with the fundamental rights of the person concerned – the public prosecutor cannot be regarded as a competent issuing authority, within the meaning of that provision (see, by analogy, judgment of 16 December 2021, *Spetsializirana prokuratura (Traffic and location data)*, C-724/19, EU:C:2021:1020, paragraph 39).

76 In the present case, the German Government states that Paragraph 100e(6)(1) of the StPO permits the transmission of evidence, at a national level, from one national investigative authority to another. Furthermore, that legal basis, which differs from that used for the initial collection of data, would not require such transmission to be authorised by a judge. It is for the referring court, which alone has jurisdiction to interpret national law, to determine whether that is the case.

77 In the light of all the above considerations, the answer to Question 1 is that Article 1(1) and Article 2(c) of Directive 2014/41 must be interpreted as meaning that an EIO for the transmission of evidence already in the possession of the competent authorities of the executing State need not necessarily be issued by a judge where, under the law of the issuing State, in a purely domestic case in that State, the initial gathering of that evidence would have had to be ordered by a judge, but a public prosecutor is competent to order the transmission of that evidence.

### *Questions 2 and 3*

78 According to settled case-law, in the procedure laid down by Article 267 TFEU providing for cooperation between national courts and the Court of Justice, it is for the latter to provide the national court with an answer which will be of use to it and enable it to determine the case before it. To that end, the Court should, where necessary, reformulate the questions referred to it. It is for the Court to extract from all the information provided by the national court, in particular from the grounds of the order for reference, the points of EU law which require interpretation, having regard to the subject matter of the dispute (see, to that effect, judgments of 13 December 1984, *Haug-Adrion*, 251/83, EU:C:1984:397, paragraph 9, and of 18 May 2021, *Asociația 'Forumul Judecătorilor din România' and Others*, C-83/19, C-127/19, C-195/19, C-291/19, C-355/19 and C-397/19, EU:C:2021:393, paragraph 131).

79 It should be observed in that regard that, by the EIOs at issue in the main proceedings, the Frankfurt Public Prosecutor's Office sought to obtain from the French investigating authorities data collected from mobile phones equipped with the EncroChat service that were being used by German users. The French investigating authorities had collected those data after being authorised to do so by a French judge.

80 The situation envisaged by Questions 2 and 3 therefore relates exclusively – as the wording of those questions also makes clear – to the second situation referred to in Article 1(1) of Directive 2014/41, that is to say, where an EIO is issued for the transmission of evidence that is already in the possession of the competent authorities of the executing State.

81 In that regard, it is apparent from the request for a preliminary ruling that, by Questions 2 and 3, the referring court is querying the substantive conditions for issuing such EIOs as set out in Article 6(1)(a) and (b) of Directive 2014/41, specifically where the authorities of a Member State have collected data from mobile phones which, through special software and modified hardware, enable end-to-end encrypted communication.

82 Thus, by Question 2(a), the referring court queries whether, in order to meet the requirements of Article 6(1)(a) of Directive 2014/41 as to necessity and proportionality, the issuing of an EIO for the transmission of evidence already in the possession of the competent authorities of the executing State must be subject, in particular, to the existence, at the time when that EIO is issued, of concrete evidence of a serious offence against each person concerned, or whether indicia of multiple offences committed by as yet unidentified persons may suffice in that regard.

83 By Question 2(b), the referring court also queries whether, in the light of the right to a fair trial, the principle of proportionality precludes an EIO from being issued where the integrity of the data gathered by the interception measure cannot be verified because of the confidentiality of the technology underpinning that measure and the accused party might, for that reason, not be able to comment effectively on those data in the subsequent criminal proceedings.

84 With regard to Article 6(1)(b) of Directive 2014/41, the referring court queries, in Question 3(a) and (b), whether – generally or, at the very least, where those data have been gathered by the competent authorities of the executing State on the territory of the issuing State and in its interest – the issuing of an EIO for the transmission of evidence already in the possession of the competent authorities of the executing State is subject to the same substantive conditions as those that apply, in the issuing State, in relation to the gathering of that evidence in a purely domestic situation.

85 In those circumstances, it must be concluded that, by Questions 2 and 3, which it is appropriate to consider together, the referring court asks, in essence, whether, and if so under what conditions, Article 6(1) of Directive 2014/41 precludes a public prosecutor from issuing an EIO for the transmission of evidence already in the possession of the competent authorities of the executing State where that evidence has been acquired following the interception, by those authorities, on the territory of the issuing State, of telecommunications of all the users of mobile phones which, through special software and modified hardware, enable end-to-end encrypted communication.

86 In that regard, it should be recalled that the purpose of Directive 2014/41, as is apparent from recitals 5 to 8 thereof, is to replace the fragmented and complicated existing framework for the gathering of evidence in criminal cases with a cross-border dimension and that it seeks, by the establishment of a simplified and more effective system based on a single instrument called the European Investigation Order, to facilitate and accelerate judicial cooperation with a view to contributing to the attainment of the objective set for the European Union to become an area of freedom, security and justice, and has as its basis the high level of trust which must exist between the Member States (judgment of 8 December 2020, *Staatsanwaltschaft Wien (Falsified transfer orders)*, C-584/19, EU:C:2020:1002, paragraph 39).

87 In accordance with Article 6(1) and (2) of Directive 2014/41, the issuing of an EIO is subject to two cumulative conditions, which are to be assessed by the issuing authority. First, under Article 6(1)(a), the issuing authority must satisfy itself that the issuing of the EIO is necessary and proportionate for the purpose of the proceedings referred to in Article 4 of that directive, taking

into account the rights of the suspected or accused person. Secondly, under Article 6(1)(b), that authority must check whether the investigative measure(s) indicated in the EIO could have been ordered under the same conditions in a similar domestic case.

88 Article 6(1)(a) of Directive 2014/41 thus requires a review of the necessity and proportionality of the issuing of the EIO by reference to the purpose of the proceedings referred to in Article 4 of that directive. The latter article, which determines the types of proceedings for which an EIO can be issued, provides, in point (a), that an EIO may be issued 'with respect to criminal proceedings that are brought by, or that may be brought before, a judicial authority in respect of a criminal offence under the national law of the issuing State'. Since that provision refers to the national law of the issuing State, the necessity and proportionality of the issuing of an EIO must be assessed only in the light of that law.

89 In that regard, in view of the referring court's queries as set out in paragraphs 82 and 83 of the present judgment, it should be made clear that, first, Article 6(1)(a) of Directive 2014/41 does not require that the issuing of an EIO for the transmission of evidence already in the possession of the competent authorities of the executing State is necessarily subject to the existence, at the time when that EIO is issued, of a suspicion, based on specific facts, of a serious offence in respect of each person concerned, if no such requirement arises under the national law of the issuing State.

90 Secondly, that provision does not, moreover, preclude an EIO from being issued where the integrity of the data gathered by the interception measure cannot be verified because of the confidentiality of the technology underpinning that measure, provided that the right to a fair trial is guaranteed in the subsequent criminal proceedings. Indeed, the integrity of the evidence transmitted can, in principle, be assessed only when the competent authorities actually have the evidence in question at their disposal and not at the earlier stage of the issuing of the EIO.

91 It then follows from the wording of Article 6(1)(b) of Directive 2014/41 and from the distinction made in Article 1(1) of that directive, referred to in paragraph 71 of this judgment, that where 'the investigative measure indicated in the EIO' consists in the obtaining of evidence already in the possession of the competent authorities of the executing State, that is to say, the transmission of that evidence to the competent authorities of the issuing State, such an EIO can be issued only if that transmission 'could have been ordered under the same conditions in a similar domestic case'.

92 Through the use of the words 'under the same conditions' and 'in a similar domestic case', Article 6(1)(b) of Directive 2014/41 makes the determination of the precise conditions required in order for an EIO to be issued dependent on the national law of the issuing State alone.

93 It follows that, when an issuing authority wishes to obtain evidence already in the possession of the competent authorities of the executing State, that authority must ensure that an EIO satisfies all the conditions laid down by the national law of its own Member State for a similar domestic case.

94 That means that the lawfulness of an EIO such as the EIOs at issue in the main proceedings, seeking transmission of data in the possession of the competent authorities of the executing State that can provide information concerning the communications of a user of a mobile phone which, through special software and modified hardware, enables end-to-end encrypted communication, is subject to the same conditions as those which may be applicable to the transmission of such data in a purely domestic situation in the issuing State.

95 Consequently, if, under the law of the issuing State, that transmission is subject to there being concrete evidence that the accused person has committed serious offences or to the evidence in the form of the data at issue being admissible, the issuing of an EIO is subject to all of those conditions.

96 By contrast, Article 6(1)(b) of Directive 2014/41 does not require – including in a situation such as that at issue in the main proceedings, where the data in question were collected by the competent authorities of the executing State on the territory of the issuing State and in its interest – that the issuing of an EIO for the transmission of evidence already in the possession of the competent authorities of the executing State should be subject to the same substantive conditions as those that apply in the issuing State in relation to the gathering of that evidence.

97 Admittedly, Article 6(1)(b) of Directive 2014/41 seeks to ensure that the rules and guarantees provided for by the national law of the issuing State are not circumvented. However, in the present case, it does not appear that that gathering of evidence and the transmission, by means of an EIO, of the evidence thus gathered would have had the aim or effect of such circumvention, which it is for the referring court to ascertain.

98 Furthermore, in the absence of any rule in Directive 2014/41 that might vary the regime applicable to an EIO for the transmission of evidence that is already in the possession of the competent authorities of the executing State depending on where that evidence has been gathered, the fact that, in this case, the executing State gathered evidence on the territory of the issuing State and in its interest is, in that respect, irrelevant.

99 Moreover, it should be noted that it follows in particular from recitals 2, 6 and 19 of Directive 2014/41 that the EIO is an instrument falling within the scope of judicial cooperation in criminal matters referred to in Article 82(1) TFEU, which is based on the principle of mutual recognition of judgments and judicial decisions. That principle, which constitutes the 'cornerstone' of judicial cooperation in criminal matters, is itself based on mutual trust and on the rebuttable presumption that other Member States comply with EU law and, in particular, fundamental rights (judgment of 8 December 2020, *Staatsanwaltschaft Wien (Falsified transfer orders)*, C-584/19, EU:C:2020:1002, paragraph 40).

100 It follows that where the issuing authority wishes to secure, by means of an EIO, the transmission of evidence already in the possession of the competent authorities of the executing State, the issuing authority is not authorised to review the lawfulness of the separate procedure by which the executing Member State gathered the evidence sought to be transmitted. In particular, any other interpretation of Article 6(1) of that directive would result, in practice, in a more complicated and less effective system, which would undermine the objective of that directive.

101 It must also be pointed out that Directive 2014/41 guarantees a judicial review of compliance with the fundamental rights of the persons concerned.

102 First, Article 14(1) of Directive 2014/41 requires Member States to ensure that legal remedies equivalent to those available in a similar domestic case are applicable to the investigative measure to which an EIO relates. As it is, in that context, it is for the competent court to check that the conditions for issuing an EIO, which are set out in Article 6(1) of that directive and recalled in paragraphs 87 to 95 of the present judgment, are satisfied.

103 Therefore, if the transmission of evidence already in the possession of the competent authorities of another Member State were to appear either disproportionate for the purpose of the criminal proceedings brought against the person concerned in the issuing State, because, for example, of the gravity of the breach of that person's fundamental rights, or to have been ordered in breach of the legal regime applicable to a similar domestic case, the court seised of the action brought against the EIO ordering that transmission would have to draw the appropriate conclusions from this as required under national law.

104 Secondly, Article 14(7) of Directive 2014/41 requires Member States to ensure that, in the criminal proceedings initiated in the issuing State, the rights of the defence and the fairness of the proceedings are respected when assessing evidence obtained through that EIO.

105 However, as regards specifically the right to a fair trial, it must be noted in particular that if a court takes the view that a party is not in a position to comment effectively on a piece of evidence that is likely to have a preponderant influence on the findings of fact, that court must find an infringement of the right to a fair trial and exclude that evidence in order to avoid such an infringement (see, to that effect, judgment of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)*, C-746/18, EU:C:2021:152, paragraph 44).

106 In the light of all the above considerations, the answer to Questions 2 and 3 is that Article 6(1) of Directive 2014/41 must be interpreted as not precluding a public prosecutor from issuing an EIO for the transmission of evidence already in the possession of the competent authorities of the executing State where that evidence has been acquired following the interception, by those authorities, on the territory of the issuing State, of telecommunications of all the users of mobile phones which, through special software and modified hardware, enable end-to-end encrypted communication, provided that the EIO satisfies all the conditions that may be laid down by the national law of the issuing State for the transmission of such evidence in a purely domestic situation in that State.

### *Question 4(a) and (b)*

107 By Question 4(a) and (b), the referring court asks, in essence, whether Article 31 of Directive 2014/41 must be interpreted as meaning that a measure entailing the infiltration of terminal devices for the purpose of gathering traffic, location and communication data of an internet-based communication service constitutes an 'interception of telecommunications', within the meaning of that article, which must be notified to a judge of the Member State on whose territory the subject of the interception is located.

108 Article 31(1) of that directive covers cases in which, for the purpose of carrying out an investigative measure, the competent authority of one Member State has authorised the interception of telecommunications of a target whose communication address is being used on the territory of another Member State from which no technical assistance is needed to carry out the interception. In that scenario, the first of those Member States, referred to as 'the intercepting Member State', must notify that interception to the competent authority of the second of those Member States, referred to as 'the notified Member State'.

109 As regards, in the first place, the concept of 'telecommunications' used in that provision, it must be borne in mind that, according to the Court's settled case-law, it follows from the need for a uniform application of EU law and the principle of equality that the terms of a provision of EU law which makes no express reference to the law of the Member States for the purpose of

determining its meaning and scope must normally be given an independent and uniform interpretation throughout the European Union, having regard not only to the wording of that provision but also to the context in which it occurs and the objectives pursued by the rules of which it is part (see, to that effect, judgments of 18 January 1984, *Ekro*, 327/82, EU:C:1984:11, paragraph 11, and of 8 December 2020, *Staatsanwaltschaft Wien (Falsified transfer orders)*, C-584/19, EU:C:2020:1002, paragraph 49).

110 In view of the fact that Directive 2014/41 does not include any definition of the concept of 'telecommunications' used in Article 31(1) of that directive, or any express reference to the law of the Member States for the purpose of determining the meaning and scope of that concept, it must be held that that provision must be given an independent and uniform interpretation in EU law, in accordance with the methodology referred to in the preceding paragraph.

111 First, as regards the wording of Article 31(1) of Directive 2014/41, the term 'telecommunications' refers, in its ordinary meaning, to all processes for the remote transmission of information.

112 Secondly, as regards the context in which Article 31(1) of Directive 2014/41 occurs, it should be noted that paragraph 2 of that article provides that the notification referred to in paragraph 1 of that article is to be made by using the form set out in Annex C to that directive. Under the heading 'Target of the interception', point B (III) of that annex envisages a telephone number and an Internet Protocol address ('IP number') or email address. That the term 'telecommunications' is to be understood in its broad sense is further confirmed by Article 31(3) of Directive 2014/41 which envisages, generally, 'any material' already intercepted.

113 Thirdly, so far as the objective of Article 31 of Directive 2014/41 is concerned, it is apparent from recital 30 thereof that the possibilities for cooperating on the basis of that directive on the interception of telecommunications should not be limited to the content of the telecommunications, but could also cover collection of traffic and location data associated with such telecommunications.

114 It follows that the infiltration of terminal devices for the purpose of gathering communication data, but also traffic or location data, from an internet-based communication service constitutes an 'interception of telecommunications' within the meaning of Article 31(1) of Directive 2014/41.

115 In the second place, as regards the authority to which the notification prescribed in that article must be addressed, it is apparent, first of all, from the wording of Article 31(1) of that directive that the EU legislature merely referred to the 'competent authority of the notified Member State', without specifying whether that authority or its functions should be administrative or judicial in nature.

116 Secondly, it should also be noted that that authority is not included in the information listed in Article 33 of Directive 2014/41 of which the European Commission was to be notified by Member States. Moreover, it is apparent from the form in Annex C to that directive, which, as indicated in paragraph 112 of the present judgment, must be used in order to notify the 'interception of telecommunications', within the meaning of Article 31(1) of that directive, that the only piece of information that must be provided in that respect on that form is the 'notified Member State'.

117 It follows that it is for each Member State to designate the authority that is competent to receive the notification referred to in Article 31(1) of Directive 2014/41. Should the intercepting Member State not be in a position to identify the competent authority of the notified Member State, that notification could be submitted to any authority of the notified Member State that the intercepting Member State considers appropriate for that purpose.

118 In that regard, it must nevertheless be made clear that the competent authority within the meaning of Article 31(1) of Directive 2014/41 may, pursuant to Article 31(3) of that directive, inter alia, give notice that the interception may not be carried out or is to be terminated, if the interception would not be authorised in a similar domestic case. It follows from this that if the authority which receives the notification is not the competent authority under the law of the notified Member State, it must, for the purposes of ensuring the effectiveness of Article 31 of Directive 2014/41, on its own initiative forward the notification to the competent authority.

119 In the light of all the above considerations, the answer to Question 4(a) and (b) is that Article 31 of Directive 2014/41 must be interpreted as meaning that a measure entailing the infiltration of terminal devices for the purpose of gathering traffic, location and communication data of an internet-based communication service constitutes an 'interception of telecommunications', within the meaning of that article, which must be notified to the authority designated for that purpose by the Member State on whose territory the subject of the interception is located. Should the intercepting Member State not be in a position to identify the competent authority of the notified Member State, that notification may be submitted to any authority of the notified Member State that the intercepting Member State considers appropriate for that purpose.

***Question 4(c)***

120 By Question 4(c), the referring court asks, in essence, whether Article 31 of Directive 2014/41 must be interpreted as being intended to protect the rights of users affected by a measure for the 'interception of telecommunications' within the meaning of that article, and that that protection would extend to the use of the data thus collected in the context of a criminal prosecution initiated in the notified Member State.

121 First of all, unlike the 'interception of telecommunications with technical assistance of another Member State', governed by Article 30 of Directive 2014/41, the 'interception of telecommunications' referred to in Article 31 of that directive, that is to say, interceptions which do not require technical assistance from the Member State on whose territory the subject of the interception is located, is not covered by an EIO. It follows that the various conditions and guarantees that circumscribe an EIO do not apply to that interception.

122 Next, as has been noted in paragraph 118 of the present judgment, it is apparent from the terms of Article 31(3) of Directive 2014/41 that the competent authority of the notified Member State may, where the interception would not be authorised in a similar domestic case, notify the competent authority of the intercepting Member State that that interception may not be carried out or is to be terminated, or, where appropriate, that any material already intercepted may not be used, or may only be used under conditions which it is to specify.

123 The use of the verb 'may' in that provision implies that the notified Member State has a discretion which comes under the assessment to be made by the competent authority of that State; the exercise of that discretion must be justified by the fact that such an interception would not be authorised in a similar domestic case.

124 Article 31 of Directive 2014/41 is thus intended not only to guarantee respect for the sovereignty of the notified Member State but also to ensure that the guaranteed level of protection in that Member State with regard to the interception of telecommunications is not undermined. Therefore, in so far as a measure for the interception of telecommunications amounts to an interference with the right to respect for the private life and communications – enshrined in Article 7 of the Charter – of the target of the interception (see, to that effect, judgment of 17 January 2019, *Dzivev and Others*, C-310/16, EU:C:2019:30, paragraph 36), it must be held that Article 31 of Directive 2014/41 is also intended to protect the rights of persons affected by such a measure, an objective which extends to the use of the data for the purposes of criminal prosecution in the notified Member State.

125 In the light of all the above considerations, the answer to Question 4(c) is that Article 31 of Directive 2014/41 must be interpreted as being intended also to protect the rights of those users affected by a measure for the 'interception of telecommunications' within the meaning of that article.

### *Question 5*

126 By Question 5, the referring court asks, in essence, whether the principle of effectiveness requires national criminal courts to disregard, in criminal proceedings against a person suspected of having committed criminal offences, information and evidence obtained in breach of the requirements of EU law.

127 As a preliminary point, it must be stated, first, that there is no need for this question to be answered unless the referring court comes to the conclusion, on the basis of the replies to Questions 1 to 4, that the EIOs were made unlawfully.

128 Secondly, as EU law currently stands, it is, in principle, for national law alone to determine the rules relating to the admissibility and assessment in criminal proceedings of information and evidence obtained in a manner contrary to EU law (see, to that effect, 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 222).

129 The Court has consistently held that, in the absence of EU rules on the matter, it is for the national legal order of each Member State to establish, in accordance with the principle of procedural autonomy, procedural rules for actions intended to safeguard the rights that individuals derive from EU law, provided, however, that those rules are no less favourable than the rules governing similar domestic actions (the principle of equivalence) and do not render impossible in practice or excessively difficult the exercise of rights conferred by EU law (the principle of effectiveness) (see, to that effect, judgments of 16 December 1976, *Rewe-Zentralfinanz and Rewe-Zentral*, 33/76, EU:C:1976:188, paragraph 5, and 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 223).

130 However, as is apparent from paragraphs 104 and 105 of the present judgment, the fact cannot be overlooked that Article 14(7) of Directive 2014/41 expressly requires Member States to ensure, without prejudice to the application of national procedural rules, 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, which means that evidence on which a party is not in a position to comment effectively must be excluded from the criminal proceedings.

131 In the light of all the above considerations, the answer to Question 5 is that Article 14(7) of Directive 2014/41 must be interpreted as meaning that, in criminal proceedings against a person suspected of having committed criminal offences, national criminal courts are required to disregard information and evidence if that person is not in a position to comment effectively on that information and on that evidence and the said information and evidence are likely to have a preponderant influence on the findings of fact.

## Costs

132 Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the referring court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.

On those grounds, the Court (Grand Chamber) hereby rules:

1. **Article 1(1) and Article 2(c) 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**

   **must be interpreted as meaning that a European Investigation Order (EIO) for the transmission of evidence already in the possession of the competent authorities of the executing State need not necessarily be issued by a judge where, under the law of the issuing State, in a purely domestic case in that State, the initial gathering of that evidence would have had to be ordered by a judge, but a public prosecutor is competent to order the transmission of that evidence.**

2. **Article 6(1) of Directive 2014/41**

   **must be interpreted as not precluding a public prosecutor from issuing an EIO for the transmission of evidence already in the possession of the competent authorities of the executing State where that evidence has been acquired following the interception, by those authorities, on the territory of the issuing State, of telecommunications of all the users of mobile phones which, through special software and modified hardware, enable end-to-end encrypted communication, provided that the EIO satisfies all the conditions that may be laid down by the national law of the issuing State for the transmission of such evidence in a purely domestic situation in that State.**

3. **Article 31 of Directive 2014/41**

   **must be interpreted as meaning that a measure entailing the infiltration of terminal devices for the purpose of gathering traffic, location and communication data of an internet-based communication service constitutes an 'interception of telecommunications', within the meaning of that article, which must be notified to the authority designated for that purpose by the Member State on whose territory the subject of the interception is located. Should the intercepting Member State not be in a position to identify the competent authority of the notified Member State, that notification may be submitted to any authority of the notified Member State that the intercepting Member State considers appropriate for that purpose.**

4. **Article 31 of Directive 2014/41**

**must be interpreted as being intended also to protect the rights of those users affected by a measure for the 'interception of telecommunications' within the meaning of that article.**

5. **Article 14(7) of Directive 2014/41**

**must be interpreted as meaning that, in criminal proceedings against a person suspected of having committed criminal offences, national criminal courts are required to disregard information and evidence if that person is not in a position to comment effectively on that information and on that evidence and the said information and evidence are likely to have a preponderant influence on the findings of fact.**

[Signatures]