Reports of Cases

Case C-670/22

Criminal proceedings
against
M.N. (EncroChat)

(Request for a preliminary ruling from the Landgericht Berlin)

Judgment of the Court (Grand Chamber) of 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)

1. *Judicial cooperation in criminal matters – European Investigation Order in criminal matters – Directive 2014/41 – Concept of issuing authority – European Investigation Order for obtaining evidence already in the possession of the competent authorities of the executing State – Public prosecutor able to order the transmission of such evidence in a purely domestic case – Included*
(European Parliament and Council Directive 2014/41, Arts 1(1) and 2(c)(i))

(see paragraphs 71-75, 77, operative part 1)

2. *Judicial cooperation in criminal matters – European Investigation Order in criminal matters – Directive 2014/41 – Conditions for issuing and transmitting a European Investigation Order – European Investigation Order for obtaining evidence already in the possession of the competent authorities of the executing State – Evidence acquired following the interception, on the territory of the issuing State, of encrypted telecommunications – Whether permissible – Compliance with conditions laid down by the law of the issuing State for transmission of such evidence in a purely domestic situation*
(Art. 82(1) TFEU; European Parliament and Council Directive 2014/41, recitals 2, 6 and 19 and Arts 1(1), 6(1)(a) and (b) and 14(7))

(see paragraphs 88-93, 99-101, 104-106, operative part 2)

3. *Judicial cooperation in criminal matters – European Investigation Order in criminal matters – Directive 2014/41 – Interception of telecommunications not requiring assistance from the Member State where the target is located – Concept – Independent and uniform interpretation –Infiltration of terminal devices for the purpose of gathering traffic, location*

and communication data of an internet-based communication service – Included – Notification of that Member State – Identification of the competent authority – Scope
(European Parliament and Council Directive 2014/41, recital 30 and Arts 31(1) to (3) and 33 and Annex C)

(see paragraphs 110-119, operative part 3)

4. *Judicial cooperation in criminal matters – European Investigation Order in criminal matters – Directive 2014/41 – Interception of telecommunications not requiring assistance from the Member State where the target is located – Notification of that Member State – Objectives – Protection of the rights of users affected – Included*
(Charter of Fundamental Rights of the European Union, Art. 7; European Parliament and Council Directive 2014/41, Art. 31)

(see paragraphs 123-125, operative part 4)

5. *Judicial cooperation in criminal matters – European Investigation Order in criminal matters – Directive 2014/41 – Respect for the rights of the defence and the fairness of the proceedings in the issuing State – Information and evidence obtained in breach of the directive – Obligations of the national court – Scope*
(European Parliament and Council Directive 2014/41, Art. 14(7))

(see paragraphs 128, 130, 131, operative part 5)

Résumé

In a reference from the Landgericht Berlin (Regional Court, Berlin, Germany) for a preliminary ruling, the Grand Chamber of the Court of Justice rules on the conditions under which a public prosecutor may issue a European Investigation Order (EIO) in criminal matters where the issuing authority of a Member State wishes to secure the transmission of intercepted telecommunications data already in the possession of another Member State. It also clarifies the consequences, so far as the use of the data is concerned, of a breach of the relevant EU legislation.

In the context of an investigation carried out by the French authorities, it appeared that accused persons were using mobile phones encrypted through the 'EncroChat' service in order to commit offences primarily related to drug trafficking. That service enabled encrypted communication, via a server in France, that could not be intercepted by conventional investigative means.

In the spring of 2020, with the authorisation of a French court, a piece of Trojan software developed by a French-Dutch investigation team was uploaded to that server and, from there, installed on the mobile phones of users in 122 countries, including approximately 4 600 users in Germany.

At a conference organised by Eurojust[1] in March 2020, the representatives of the French and Netherlands authorities informed the authorities of other Member States of their planned interception of data, including data from mobile phones located outside French territory. The representatives of the Bundeskriminalamt (Federal Criminal Police Office, Germany; 'the BKA')

[1] European Union Agency for Criminal Justice Cooperation.

and of the Generalstaatsanwaltschaft Frankfurt am Main (Public Prosecutor's Office, Frankfurt am Main, Germany; 'the Frankfurt Public Prosecutor's Office') signalled their interest in the data of the German users.

Between June 2020 and July 2021, in proceedings brought against X, the Frankfurt Public Prosecutor's Office issued EIOs for the purpose of requesting authorisation from the French authorities to use the data collected by them 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 were being committed in Germany with the aid of mobile phones equipped with the 'EncroChat' service, and that as yet unidentified persons were suspected of planning and committing such offences in Germany using encrypted communications. A French court authorised the transmission and use in judicial proceedings of the data intercepted from German users.

The Frankfurt Public Prosecutor's Office subsequently reassigned the investigations, inter alia, in respect of M.N., to local public prosecutor's offices. In one of the criminal proceedings brought before it, the referring court queries the lawfulness of those EIOs in the light of Directive 2014/41[2] and the consequences of a possible infringement of EU law for the use, in those proceedings, of the intercepted data. It therefore decided to refer questions to the Court of Justice for a preliminary ruling.

Findings of the Court

In the first place, the Court notes that the concept of 'issuing authority', within the meaning of Directive 2014/41, is not limited to judges. In fact the public prosecutor is included, in Article 2(c)(i) of that directive, among the authorities which are understood to be an 'issuing authority', subject to the sole condition that they should have competence in the case concerned. 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' 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.

In the second place, it follows from Article 6(1) of Directive 2014/41 that an EIO for the transmission of evidence acquired, such as that at issue in the main proceedings, which is already in the possession of the competent authorities of the executing State, must satisfy 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.

However, while 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, it does not require – including in a situation such as that at issue in the main proceedings, where the data in question were gathered 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

[2] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters (OJ 2014 L 130, p. 1).

the 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.

Moreover, in the light of the principle of mutual recognition of judgments and judicial decisions underpinning judicial cooperation in criminal matters, to which Directive 2014/41 relates, the issuing authority is not authorised to review the lawfulness of the separate procedure by which the executing Member State gathered the evidence already in the possession of that Member State and whose transmission is sought by the issuing authority.

The Court also makes clear that, first, Article 6(1)(a) of Directive 2014/41 does not require that the issuing of such an EIO 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 for the transmission of evidence between national public prosecutor's offices. Secondly, that provision does not, moreover, preclude an EIO from being issued where the integrity of the intercepted data cannot be verified at that stage because of the confidentiality of the technology underpinning the interception, 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.

In the third place, the Court notes that 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 Article 31(1) of Directive 2014/41, 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.

Under Article 31(3) of Directive 2014/41, the competent authority of the notified Member State may then, if the interception would not be authorised in a similar domestic case, indicate that the interception may not be carried out or is to be terminated, or that any material already intercepted may not be used, or may only be used under conditions which it is to specify. 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 protect the rights of persons affected by such an interception of telecommunications.

Finally, the Court points out that 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.

However, Article 14(7) of Directive 2014/41 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. Consequently, if a court takes the view that a party is not in a position to comment effectively on such 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 disregard that evidence.