SUPREME COURT OF NORWAY

O R D E R

issued on 30 June 2022 by a division of the Supreme Court composed of

Justice Aage Thor Falkanger
Justice Knut H. Kallerud
Justice Arne Ringnes
Justice Høgetveit Berg
Justice Erik Thyness

HR-2022-1314-A, (case no. 22-027874STR-HRET), (case no. 22-027879STR-HRET) and (case no. 22-027883STR-HRET)
Appeal against Borgarting Court of Appeal's order 19 January 2022

I.	
A	(Counsel Marius Oscar Dietrichson)
v.	
The Public Prosecution Authority	(Counsel Andreas Magne Alfoni Strand)
II.	
B	(Counsel Berit Reiss-Andersen)
v.	
The Public Prosecution Authority	(Counsel Andreas Magne Alfoni Strand)
III.	
C	(Counsel Øystein Ola Storrvik)
v.	
The Public Prosecution Authority	(Counsel Andreas Magne Alfoni Strand)

(1) Justice **Høgetveit Berg:**

Issues and background

(2) The case concerns a request for exclusion of evidence. The question is whether data read by foreign authorities from an encrypted communication network can be used as evidence in a Norwegian criminal case.

(3) A, B and C are charged with violation of section 232 subsection 2 first penal option cf. section 231 subsection 1 cf. section 15 of the Penal Code on dealings with a "very substantial quantity" of drugs. In addition, B and C are charged with violation of section 79 c of the Penal Code on criminal acts "perpetrated as part of the activities of an organised criminal group".

(4) The investigation was opened as a result of the acquisition of data from C's communication through EncroChat, described as follows in the Court of Appeal's order:

> "EncroChat is the name of one of several providers of encrypted communication solutions via the use of encrypted mobile phones. The phones have a modified operating system allowing specific communication applications. In practice, the phones only function in contact with other encrypted phones of the same type and enable communication with a high level of security. The EncroChat phones come with an international and prepaid SIM card. The phones cannot be bought in stores, but exclusively through EncroChat's websites or on Ebay.
>
> All traffic between such phones is encrypted and can therefore not be wiretapped during the transmission phase. The service also allows 'panic deletion', 'remote deletion' and automatic deletion of messages after a given time. These functions make the phones well suited for criminal communication."

(5) The reason why Norwegian police – represented by the National Criminal Investigation Service (Kripos) – were given access to the materials was that Dutch and French police, in 2018, had opened an investigation of EncroChat and succeeded in accessing a server located in Roubaix, France. Early in 2020, they also succeeded – with the assistance of Eurojust and Europol – in developing a technical solution for encryption of the data traffic in EncroChat that made it possible to read the content virtually in real time.

(6) On 30 January 2020, the first-instance court in Lille gave permission to read the logs on the server in Roubaix. Based on the grounds for suspicion stated in the request to access the logs and the court's ruling, the primary target of investigation were the persons and companies affiliated with EncroChat and the identified server in Roubaix as the service provider, not the subscribers of the service. Thus, the suspicion was directed at the service provider and included contribution to aggravated drug offences. The permission to read the logs applied for one month, but was extended several times. In a ruling of 12 February 2020, the permission was also extended to cover the terminals/phones of the subscribers.

(7) French police installed software on the server in Roubaix, with the result that the subscribers downloaded false updates enabling the police to bypass the encryption. The technical method for reading the data is classified information in France, which means that no details related to the procedure are available. Therefore, it is also unclear whether the data have in fact been

acquired from the server, from the phones or from both. The Court of Appeal found as follows:

> "After an overall assessment, the Court of Appeal finds, like the District Court, that it is more likely that the data were acquired from the server and/or the phones than from the server only. From information presented to the Court of Appeal, it appears more probable that the software installed made it possible to read data both from the server and from the relevant phones (the external units). The server, the phones and the other components appear jointly to constitute an electronic communication network – a 'computer system' as defined in Article 1 (a) of the Council of Europe's Convention on Cybercrime of 8 November 2001."

(8) On 27 March 2020, Kripos was offered access to data connected to subscribers in Norway, and accepted the offer. Data were received from 2 April 2020 and until EncroChat was shut down in July 2020. The materials were made available without French police or anyone else having gone through them first.

(9) Based on these materials, and other investigation materials, several phone users were identified and the grounds for suspicion were individualised. Kripos then obtained permission from Oslo District Court to monitor the communication between the three defendants in this case, among others. In June 2020, after the Oslo police district had acquired the materials from Kripos, the prosecution authority obtained the consent of French authorities to use them as evidence in the criminal case.

(10) During the preparatory proceedings, it was requested that the EncroChat materials be excluded as evidence. After an oral hearing, Oslo District Court ruled as follows on 2 November 2021:

> "The EncroChat materials can be presented as evidence in the criminal case against C, B and A."

(11) The District Court found that the evidence had been legally acquired in France, that the acquisition did not involve circumvention of the control mechanisms in Norwegian law, and that neither the acquisition nor the use of the materials as evidence conflicted with basic Norwegian values.

(12) A, B and C appealed to the Court of Appeal. On 19 January 2022, Borgarting Court of Appeal ruled as follows:

> "The appeals are dismissed."

(13) The Court of Appeal found that the materials could not have been acquired in the same manner under Norwegian law, but that it had been legally acquired in France. The materials were not acquired in manner that circumvented Norwegian law. Admitting the materials as evidence in the main hearing would not be in conflict with basic Norwegian values.

(14) A, B and C have appealed to the Supreme Court. The appeal challenges the Court of Appeal's application of the law and procedure. On 3 March 2022, the Supreme Court's Appeals Selection Committee unanimously ruled (in HR-2022-520-U) that the appeals against the procedure could clearly not succeed, see section 387 a subsection 1 of the Criminal Procedure Act. It also ruled that oral proceedings should be conducted to decide the appeals against the

application of the law, see section 5 subsection 1 second sentence and section 387 of the Criminal Procedure Act.

The parties' contentions

(15) *A* contends that the standard for using materials acquired by foreign authorities as evidence in a Norwegian criminal case, presented, *inter alia,* in the Supreme Court ruling in Rt-2002-1744, has not been correctly applied by the Court of Appeal. The materials were not legally acquired in France. French authorities' assessment of the legitimacy must be eligible for review in Norway when the question is whether the materials can be used as evidence in a Norwegian court. The Court of Appeal has also erred in its assessment of the circumvention requirement; decisive emphasis cannot be placed the prosecution authority's lack of knowledge of the method. In any case, the acquisition and possible use of the materials in a Norwegian criminal case are in conflict with Norwegian values.

(16) *B* contends that the evidence must be excluded because it in reality was acquired in Norway. Such coercive measures may thus only be taken under Norwegian law, in this case under section 216 o of the Criminal Procedure Act. As that was not done, the evidence was illegally acquired and must be excluded. In any case, the evidence was acquired by circumvention of Norwegian rules – and is therefore in conflict with Norwegian values.

(17) *C* contends that a similar coercive measure could not have been taken under Norwegian law. It is an error to consider data acquired from Norwegian phones as surplus information. The Court of Appeal was wrong in deciding the case based on the prosecution authority's lack of knowledge of the reading of data from a Norwegian phone. Overall, the operation appears as a circumvention of the requirements in the Criminal Procedure Act.

(18) *The Public Prosecution Authority* contends that the appeals must be dismissed. A similar acquisition of the materials would have been legal in Norway under section 216 o of the Criminal Procedure Act. In any event, the data were acquired by French authorities in accordance with French law. Using them as evidence is not in conflict with basic Norwegian values. Under any circumstances, exclusion may only take place in C's case, as materials have only been acquired from his phone.

My opinion

The law

(19) The main issue is whether data acquired by foreign authorities may serve as evidence in the criminal case. The basic starting point is that the parties may present any evidence they wish. Refusing a particular piece of evidence requires a legal basis or other special justification.

(20) The use of materials acquired by foreign authorities in a Norwegian criminal case is not regulated by law. As stated in the Appeals Selection Committee's order in Rt-2002-1744, investigation materials from another country, legally acquired there but not under Norwegian law, *may* serve as evidence in a Norwegian criminal case. The ruling concerned wiretapping of a Norwegian national in Spain. The method was legal in Spain, but would not have been so in Norway. The Appeals Selection Committee stated on page 1747:

> "The limitations on the use of communication control as an investigation measure are due to the individual's right to respect for privacy and personal integrity, see Proposition to the Odelsting no. 64 (1998–99), page 46. Opinions may vary as to the balancing of these considerations against the need to solve crimes, and various countries have chosen somewhat different solutions. If one chooses to take residence in a country that does not have the same limitations on communication control as we have, the Appeals Selection Committee finds that one cannot have any legitimate expectation that information acquired through legal communication control in the relevant country should be inadmissible as evidence Norway.
>
> Against this background, the Appeals Selection Committee finds that it should not be a condition for using information from legal communication control abroad as evidence in a criminal case in Norway that the information could have been acquired in the same manner here. If the communication control carried out abroad is in accordance with Norwegian values and the information is used as evidence for an offence that in the relevant country may justify the form of communication control from which it is acquired, the information must be admissible as evidence in a criminal case in Norway, provided that the defendant in the relevant case has access to it."

(21) The order concerned materials acquired during communication control, and is followed up in Rt-2005-1524, HR-2021-1336-U and HR-2021-1538-U.

(22) Rt-2005-1524 concerned materials acquired during communication control carried out by the police in Lithuania. The Supreme Court reiterated that Norwegian courts must admit evidence that has been legally acquired by foreign authorities, by other means and under other procedural rules, unless it conflicts with basic Norwegian values. The following was stated in paragraph 19:

> "I add that if it were a requirement that foreign police and prosecution authority follow Norwegian procedural rules in criminal cases, it would in practice obstruct international collaboration with regard to cross-border crime. That would not be acceptable."

(23) HR-2021-1336-U concerned use of summaries of basic materials acquired during the control of an encrypted communication platform in connection with remand in custody. The background was the FBI's establishment of a communication platform for encrypted information. The communication was monitored, and the operation was aimed at all subscribers regardless of suspicion of criminal activities. The materials were sent to the police in other countries, including Norway. Here, the Court of Appeal had assumed that the acquisition was legal under United States law. In the appeal to the Supreme Court, it was held that the method would not have been legal in Norway and that the use of the information was in conflict with basic Norwegian values. The majority of the Appeals Selection Committee disagreed, since the subscribers of such a platform "at least must know that that the police will assume that the encryption service is largely used by criminal networks, and that they may easily be subjected to monitoring and investigation", see paragraph 21. The minority found that "the threshold is higher for admitting as evidence information generated from another country's monitoring of a person residing in Norway than if the person had been present in the monitoring country", and that the Court of Appeal had failed to consider this aspect, see paragraph 31. It the light of the dissenting opinion, it is natural to understand the majority to have attached less importance to the monitored person's presence in Norway at the relevant time.

(24) The Supreme Court ruling HR-2021-1538-U concerned an extension of the remand in custody from HR-2021-1336-U. The Appeals Selection Committee based itself on the majority's view in the preceding order, and added that the communication form in itself – code words – further supported the result in HR-2021-1336-U.

(25) I cannot see any reason for departing from the standard laid down in Rt-2002-1744 and upheld in subsequent case law. The principle is technology-neutral, and there is no reason to distinguish between evidence acquired through communication control and evidence acquired through data reading. Data reading may be related to communication, but is not limited to it. It may also include text, film or images stored on a data unit.

(26) If the acquisition could not have been legally carried out in Norway, three criteria must be met in order for investigation materials acquired by foreign authorities in a Norwegian criminal case to be admissible: (i) they must have been acquired in accordance with applicable rules in the relevant country, (ii) the defendant must have access to all the acquired information, and (iii) the information must not have been acquired in a manner causing the use as evidence to conflict with basic Norwegian values. A prohibition against using materials acquired by foreign authorities as evidence would be particularly relevant where the acquisition is carried out by states in which criminal procedural traditions differ from ours.

(27) Thus, it is not a condition for using materials acquired by foreign authorities as evidence in a Norwegian criminal case that they could have been acquired in the same manner under Norwegian law. Further, the Office of the Public Prosecutor maintained in a letter of 20 January 2003, after the ruling in Rt-2002-1744, that the acquisition must not appear as a mere circumvention of the limits in Norwegian law. This is undoubtedly correct. In terms of method, this falls under criterion (iii), where the role of the Norwegian authorities is relevant.

(28) Also, it is not a condition for using the materials as evidence that they have been acquired upon the initiative of Norwegian authorities. In Rt-2002-1744, the investigation in Spain had been requested by the Norwegian prosecution authority. The request was both in form and content neutrally worded and contained no instructions for the Spanish investigation.

(29) If Norwegian authorities ask foreign authorities to use a method without a legal basis in Norway only to circumvent the hindrances in Norwegian criminal procedure, materials acquired in this manner are normally not admissible as evidence in a Norwegian criminal case. Such "jurisdiction shopping" may easily render the acquisition and use of the evidence in conflict with basic Norwegian values.

(30) Where Norwegian authorities have *not* initiated the investigation, and the foreign authorities have acted in accordance with their own country's legislation, Norwegian authorities' knowledge of the method may only exceptionally result in inadmissibility of the evidence in a Norwegian case.

Which rule on exclusion of evidence is applicable in the case at hand?

(31) B's defence counsel states that according to information provided, it must be assumed that the evidence at least partially was acquired in Norway. Since the conditions in the Criminal Procedure Act are not met, the ordinary doctrine on illegally acquired evidence, summarised in HR-2021-966-A, applies.

(32) I disagree. One may indeed argue in our case that the method established "sluiced" the materials more or less directly from C's phone in Norway to Norwegian authorities, although the traffic went via the server in Roubaix. But in this context, it is not decisive that C's phone was in Norway at the relevant time. In my view, the country from which the materials were acquired is less relevant. Today, electronic information flows unhindered across country borders. The key factor must be who acquired the materials.

(33) In the case at hand, the materials were acquired by French police according to a method established by French police, based on a permission from French courts. Thus, the principle established in Rt-2002-1744 and subsequent case law apply.

Use of evidence acquired by a foreign authority in a manner that would have been illegal under Norwegian law

Would a similar acquisition of evidence have been legal in Norway?

(34) The Public Prosecution Authority contends that the coercive measures, which involved reading of data from both the server and the phones, would in any case have been permitted under Norwegian law, see section 216 o of the Criminal Procedure Act, and that the materials without further qualification would have been admissible as evidence in a Norwegian criminal case. I agree that if the materials could have been acquired in a similar manner in Norway, there is no reason to preclude them as evidence.

(35) Our case seems to be covered by the wording of the law. However, it is not necessary for me to consider the scope of section 216 o and the hypothetic use of the provision, as the provision under any circumstances will be essential to the assessment of whether it would conflict with basic Norwegian values to present the materials as evidence. I will return to that.

Were the materials legally acquired under French law?

(36) In January 2020, French police asked the court's permission to read the logs on the server in Roubaix. The court granted such permission – which was extended and prolonged several times. The Court of Appeal found that the materials had been legally acquired under French law. The Supreme Court may normally not review the Court of Appeal's ruling on this point, see section 388 subsection 1 of the Criminal Procedure Act, see also HR-2021-1336-U paragraph 17 and Rt-2000-710.

(37) I mention nonetheless that the Court of Appeal was reluctant to review the issue, which means that its conclusion is also based on an assessment of Norwegian courts' competence to review the rulings of French courts. The Court of Appeal assumed that when determining the admissibility of investigation materials acquired by a foreign authority, it is – like in connection with surrender of criminals to countries outside the Nordics and the EU – neither necessary nor serviceable that Norwegian courts review the foreign authorities' compliance with respective laws, unless there are special reasons for investigating for instance violations of central rights in the European Convention on Human Rights (ECHR). I support this – and add that when the acquisition of evidence is based on rulings from a French court,

extraordinary circumstances are required for Norwegian courts to consider whether the French rules have been followed.

(38) Based on the information at hand, it must be concluded that the materials have been legally acquired under French law.

Would it be contrary to Norwegian values to admit the evidence?

(39) EncroChat was developed for confidential communication. Encryption in itself is neither criminal nor unwanted. On the contrary, the possibility of encryption and confidential communication is important for the freedom of expression and information, see, *inter alia,* the Council Resolution on Encryption of 24 November 2020 (13084/1/20). The Resolution stresses that the Member States' duty to respect and ensure the freedom of expression and the right to private life also implies a duty to protect encrypted data. At the same time, the Resolution sets out that encryption brings with it the potential for exploitation for criminal purposes. As emphasised in the Resolution, the consideration of protecting privacy and security of communications must be balanced against the possibility for competent authorities to fight serious crime. On the one hand, privacy protection is generally a strong value in Norway. Mass surveillance of citizens to uncover crime would easily conflict with Norwegian values. On the other hand, the investigation is aimed at solving serious crime.

(40) A ruling by the first-instance court in Lille 29 April 2020 sets out that the coercive measure revealed 32 477 subscribers in 121 countries. Among the 380 subscribers in France, French authorities estimated that 242 used the encrypted system for criminal purposes. The remaining 138 subscribers were, at that time, connected to inactive or non-analysed phones. The Court of Appeal ultimately supported the District Court's conclusion that it is "highly likely" that EncroChat is "mainly used by criminals for criminal communication".

(41) At the same time, the facts show that mass surveillance is not an adequate term in this case. I reference decisions by the Federal Supreme Court of Germany – Bundesgerichtshof – of 2 March 2022, case 5 StR 457/21, which concluded that the coercive measures taken against EncroChat did not have the characteristics of mass surveillance – but, ultimately, the suspicion was aimed at all the subscribers, see particularly paragraph 37. I support this characterisation.

(42) Therefore, I agree with the District Court and Court of Appeal that the use of an encrypted communication platform whose subscribers are mainly criminals is not eligible for protection. Persons who choose to use such a service must be aware of the possibility of surveillance and investigation. In such events, it would generally not disturb the Norwegian sense of justice if materials acquired in this manner are used as evidence in a criminal case. I add that, when Norwegian values did not hinder such use in HR-2021-1336-U, it is difficult to see how they can be a hindrance in the case at hand.

(43) As mentioned, exclusion of materials acquired by foreign authorities is particularly relevant where the acquisition is carried out by states whose criminal process is based on values different from ours. That is clearly not the case for France.

(44) Under any circumstances – in addition to the fact that we are not dealing with mass surveillance – it is of essence that the Storting, through the adoption of section 216 o of the

Criminal Procedure Act, has allowed for data acquisition in situations that, at least according to the provision's wording, are similar to the case at hand.

(45) As for the Norwegian authorities' role in the investigation, I mention that Kripos, on 27 March 2020, was offered to receive data materials from the foreign investigation. It was a condition that the Norwegian police accepted that the investigation methods had involved acquisition of data from units in Norway. It was also a condition that the materials could not be used in criminal cases in Norway without the investigating parties' consent. Kripos accepted the conditions on the same day and confirmed that the Norwegian police would be handed the materials from the operation. After having received the materials, Kripos concluded that the communication was of a criminal nature – and opened its own investigation. The Court of Appeal found no evidence that Kripos took an active part in the investigation together with foreign police. The Supreme Court is not to review this finding of fact. Kripos was only involved as a "passive recipient" of the materials. The nature of the materials – raw data virtually in real time – is not relevant.

(46) Against this background, I find that presenting the disputed investigation materials as evidence in the criminal case at hand is not in conflict with Norwegian values.

Conclusion

(47) I find that there is no basis for excluding the materials related to EncroChat as evidence. The appeal must therefore be dismissed. Based on the principle of free presentation of evidence, I find that the most appropriate would be to formulate a new conclusion.

(48) I vote for this

O R D E R :

The request for exclusion of materials acquired from EncroChat as evidence is dismissed.

(49) Justice **Kallerud:** I agree with Justice Høgetveit Berg in all material respects and with his conclusion.

(50) Justice **Ringnes:** Likewise.

(51) Justice **Thyness:** Likewise.

(52) Justice **Falkanger:** Likewise.

(53) The Supreme Court issued this

O R D E R :

The request for exclusion of materials acquired from EncroChat as evidence is dismissed.