SUPREME COURT OF NORWAY

On 28 March 2019, the Supreme Court composed of the justices Webster, Kallerud, Falch, Høgetveit Berg and Lindsetmo gave an order in

HR-2019-610-A, (case no. 19-010640STR-HRET), criminal case, appeal against order:

Tidal Music AS	(Counsel Fredrik Berg)
v.	
The public prosecution authority	(Counsel Henrik Horn)

(1) Justice **Kallerud:** The case concerns a third-party search at the Norwegian company Tidal Music AS in Oslo in accordance with section 192 subsection 3 (3) of the Criminal Procedure Act. The question is whether the police, from data terminals at the company's office in Oslo may download digital material that the company has stored abroad, or whether such a coercive measure falls outside the jurisdiction of Norwegian authorities.

(2) Tidal is a group of companies domiciled among other places in the USA and several European countries that offers music streaming to subscribers. Tidal Music AS is a Norwegian company in this group, and will mostly be referred to as Tidal.

(3) On 3 December 2018, *Økokrim* (Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime) requested a warrant from Oslo District Court to conduct a third-party search at Tidal's office in Oslo. The request sets out that the suspicion is against an "unknown perpetrator", and that it concerns computer fraud in the form of manipulation of the numbers for some tracks in order to influence the calculation of royalties to certain right holders. According to information provided, Tidal Music AS is not charged with or suspected of anything unlawful. The police want to access information assumed to shed light on criminal acts suspected to have been committed. If information that may serve as evidence happens to be stored electronically, the request also includes "the relevant data carriers and electronically stored information to which the person in question has access", including "online data carriers in the form of servers etc.".

(4) On 5 December 2018, Oslo District Court granted Økokrim's request.

(5) The search was commenced on 17 December 2018 at the company's office in Oslo. Tidal opposed the search and any seizure involving downloading from the company's terminals in Norway of data stored by Tidal on servers abroad.

(6) More specifically, the dispute concerns "source codes" that during the search – assisted by the technical director of Tidal – were downloaded from a server in the USA belonging to Amazon Web Services. The material was stored on a USB stick currently in Økokrim's custody.

(7) The second issue of dispute is the extraction of emails from the technical director's Google account. This data is stored on servers in the Netherlands, Finland, Belgium and/or Iceland. In which of these countries the data in question is stored is unknown. The downloading was commenced upon the police's order, but the process turned out to be lengthy. Økokrim therefore asked the owner of the email account to copy the data onto a hard drive that Økokrim could pick up at Tidal's office later. Due to the disagreement with regard to the search, the data has not been surrendered Økokrim.

(8) Tidal appealed the district court's decision to Borgarting Court of Appeal, which dismissed the appeal on 18 January 2019 as it found that the conditions for a search were met under section 192 subsection 3 (3) of the Criminal Procedure Act. The court also found that there was a reasonable cause for suspicion and highly probable that evidence could be secured by a search in Tidal's data. The measure was not disproportionate. Tidal did not dispute that these conditions were met.

(9) As for the issue at stake – whether the search could be conducted despite the data being stored abroad – the court of appeal found that this coercive measure had to be considered taken in Norway, by a Tidal employee – upon an order – giving the police access to servers abroad from the company's office in Norway. Hence, we are not dealing with an intrusion into the server abroad. The court also emphasised that any seizure of data on the server would be executed from Norway.

(10) Tidal has appealed against the court of appeal's order to the Supreme Court. In the Supreme Court's Appeal Selection Committee's decision of 7 February 2019, it was determined that the appeal be heard by a division of five justices, see section 5 subsection 1 second sentence of the Courts of Justice Act.

(11) *Tidal Music AS* contends:

(12) It is not in itself disputed that the conditions for search under section 192 subsection 3 (3) of the Criminal Procedure Act, cf. section 192 subsection 1, are met. However, the "storage place" that Økokrim wishes to search are servers on which Tidal's data is stored, and these servers are not in Norway. The data is stored in a territory over which other states have exclusive enforcement jurisdiction. In other words, it is outside of Norwegian territorial jurisdiction. The search allowed by the court of appeal is effective in the state in which the servers are present in the form of a data flow through a physical grid abroad. Hence, the search is a violation of the sovereignty of these states.

(13) Norway is not party to any treaties making exemptions from this principle of sovereignty in a case like this. State practice varies, and no customary international law exists that may form the necessary legal basis.

(14) If a search is allowed in the case at hand, there is a risk of disclosure of information that is vital for the storage state to protect, e.g. for privacy reasons. Norway would then have to be prepared for other states allowing their police to conduct searches in servers on Norwegian soil. This could be critical.

(15) Tidal Music AS has submitted this prayer for relief:

> **«The court of appeal's order is to be set aside.»**

(16) *Økokrim* contends:

(17) The legal basis in internal law is clear. Norway is not bound by any treaty or international customary law preventing a search in the case at hand. The coercive measure is taken here as the police are allowed to search a Norwegian company's storage place for possible evidence by legally accessing that company's computer system from its office in Norway. This does not violate the sovereignty of another state.

(18) The police are only present on Norwegian soil, the coercive measure is taken exclusively against a company domiciled in Norway, and no physical traces are left in the state in which the data is stored. The police are only doing what the company itself could do at the place of storage abroad.

(19) Possible objections to the police gaining access to downloaded material must be resolved document-by-document under the rules governing what can be seized.

(20) When evaluating this, one should also emphasise the need for efficient combat of international cybercrime.

(21) Økokrim has submitted this prayer for relief:

> **«The appeal is to be dismissed.»**

(22) *My view on the case*

(23) The Supreme Court's jurisdiction is limited to reviewing the court of appeal's procedure and general interpretation of a statutory provision, see section 388 subsection 1 of the Criminal Procedure Act.

(24) *Legal basis in internal law*

(25) The invoked and applied legal basis for the search is section 192 subsections 1 and 3 of the Criminal Procedure Act. The relevant parts of section 192 read:

> **"If a person is with just cause suspected of an act punishable pursuant to statute by imprisonment, a search may be made of his residence, premises or storage place … to look for evidence or objects that may be seized … .**
> **…**
> **A search may be made on any other person's premises when there is just cause for suspecting such an act, and**
> **…**
> **3) there are otherwise special grounds to assume that … there may be found evidence or objects that may be seized … ."**

(26) The court of appeal has established that both the general requirement for a search under subsection 1 of the provision and the special requirement for a third-party search in subsection 3 are met. The court of appeal also concluded that the measure is not disproportionate, see section 170 a of the Criminal Procedure Act. Tidal has not disputed the court of appeal's interpretation of the wording in section 192, and the company accepts that a legal basis exists in internal law.

(27) In my view, no interpretation issues arise in the case at hand with regard to section 192 of the Criminal Procedure Act. Like the court of appeal, I interpret section 192 subsection 3 (3) to mean that, in a third-party search, the same places may be searched as under subsection 1, including the

"storage place". This may include a data grid, such as a server located abroad.

(28) However, Tidal contends that the court of appeal, when referring to section 199 a of the Criminal Procedure Act in its grounds of judgment, must be deemed to conclude that this provision extends the right to search abroad. That is not how I read the court of appeal's order, but I agree with Tidal that section 199 a does not extend the right to search. When it comes to searches in a computer system – the provision constitutes a legal basis for "[ordering] everyone who is dealing with the said system to provide the information necessary for gaining access to the system". Yet, the requirements for a search, for instance under section 192 subsection 3 (3), considered in conjunction with subsection 1, must be met before an order under section 199 a may be given.

(29) Although the conditions under section 192 of the Criminal Procedure Act are met, Tidal has pointed out that the provision is not formulated clearly enough to cover searches in servers abroad. I cannot see that the principle of legality complicates anything. The wording – "storage place" – undoubtedly covers media for storage of digital material, and nothing suggests that certain devices are excluded.

(30) As I will revert to shortly, coercive measures may only be taken within the territorial jurisdiction of Norwegian authorities. This is essential for all coercive measures in criminal procedure, and not only when it comes to searches in computer systems. I cannot see why, in such matters, the scope of Norwegian jurisdiction should be stated in particular with regard to the principle of legality. A further demarcation must be based on principles under international law and after an individual assessment of the coercive measure and its planned use.

(31) Against this background, I conclude that nothing in the general interpretation of section 192 of the Criminal Procedure Act – based on Norwegian internal law – prevents the search from being conducted in the manner accepted by the lower instances.

(32) *Limitation of the right to search under international law*

(33) The rules in the Criminal Procedure Act apply, according to section 4, “subject to such limitations as are recognised in international law or which derive from any agreement made with a foreign state”.

(34) *Treaties*

(35) Before the Supreme Court, the parties have discussed in particular the Convention on Cybercrime from 2001 to which the member states of the Council of Europe are bound, and which has been ratified also by the USA.

(36) The Convention imposes the states to adopt any measures necessary to combat cybercrime. For instance, Article 18 sets out that each state must ensure the same access as that established in Norwegian law under section 199 a of the Criminal Procedure Act. Articles 29 et seq. contain provisions relating to mutual assistance. However, the Convention only establishes minimum obligations for the states, see Norwegian Official Report 2007: 2 Legislative measures to combat cybercrime, page 47. As none of the articles directly deals with a measure like that in the case at hand, I will not address this Convention any further.

(37) Nor are there other treaty provisions specifically preventing the relevant type of search. In fact, no legal basis is established under any treaty for conducting a search in a case like the one we are dealing with.

(38) As a matter of form, I mention that no information has been presented suggesting that the European

Convention on Human Rights (the ECHR) prevents the use of coercive measures in this particular case, nor has this been contended by any of the parties.

(39) *Limitations recognised in international law – the principle of sovereignty*

(40) The clear starting point under international law is that the states may exercise coercion only in their own territory. The enforcement jurisdiction is exclusive; no state may use coercive measures in the territory of another state without the consent of that state. Norwegian legislation is based on this principle. For instance, it is clear that the Norwegian police and prosecution authority cannot make arrests abroad or search a house in another country. In such cases, the enforcement authorities are dependent on assistance from – or agreements with – other countries.

(41) However, these general starting points are less instructive when it comes to search and seizure of digitally stored information. In addition to being stored on the user's personal storage media – including computers, USB sticks or hard drives – such information may be stored in "the cloud". This is often the case for storage services provided by foreign companies, such as Google and Amazon in the case at hand. However, this type of storage, too, implies that the data exists on one or several physical storage media – often referred to as servers. According to information provided, it is not easy to tell on which server a Norwegian user's data is stored, and the storage place may be changed over time without the user knowing or being able to control it. Although one agrees that the physical storage place is not in Norway, the state in which the data is stored at any given time may – as demonstrated in this case – be unknown.

(42) The legal issues brought to life by technological development and the use of coercion to obtain data stored in "the cloud" have not been clarified, neither under Norwegian nor under international law.

(43) *Norwegian case law*

(44) No Supreme Court judgment exists discussing the scope of Norwegian enforcement jurisdiction in a case like the one at hand.

(45) According to information provided, the Norwegian police and prosecution authority assumes that it has a right to search servers abroad when the procedure is as described. Special attention is given to Norwegian Official Report 1997: 15, stating that "it concerns a search in Norway when access to the data is gained from a terminal located in Norway", see section 4.2.1.3. According to the Report, one must be able to investigate "which data are available on the relevant terminal, irrespective of whether the particular piece of information is stored abroad".

(46) I also mention that Norwegian case law in other areas is probably based on some of the same ideas. For example, it has not been discussed whether communication can be controlled despite one of the parties to the conversation being present in another country. In practice, according to information provided, a surrender order under section 210 of the Criminal Procedure Act, also applies if the object deemed to be significant as evidence should be present abroad.

(47) The views expressed in Norwegian Official Report 1997: 15 did not result in amendments, and the practice described seems to have been followed without the question of jurisdiction having been dealt with earlier.

(48) *Case law of other countries – international reports*

(49) The case law of other countries varies. I mention some examples and reports for illustration purposes.

(50) On 10 May 2012, the Supreme Court of Denmark decided that the police could access a defendant's

Messenger and Facebook profiles, despite data pertaining to the profiles being stored on servers abroad. The police had received the necessary codes to gain access through wiretapping.

(51) Under Swedish law, however, the dominant view has been that the territorial principle prevents the police to access internet-based communication and storage services if the supplier's servers may be located outside of Sweden. This applies even if the police has obtained the necessary login credentials. I refer to the comprehensive report in Swedish Official Report 2017: 89 Secret data reading – an important tool in the combat against serious crime, page 444. The Report points out however that there are "strong reasons for nuancing the prevailing Swedish attitude", see the summary on page 28 of the report and pages 465 et seq. In the final remarks of the Report, the following is stated on 482:

> **"As concerns the practical reasons for changing the Swedish attitude, the strongest argument must be that, when a criminal investigation (or an intelligence case) is being conducted in Sweden directed at a person who is here and involves a crime committed (or planned) in the country, it seems odd that Swedish law enforcement authorities should not be able to collect electronically stored data that, in any case, can be made available in Sweden without any risk, considering the fact that information security issues arise in the state (or, where appropriate, the states) where the data is stored. This is even more remarkable because the storage place in most cases should be both irrelevant and unknown to the person who owns or disposes of the information, which thus exists in Sweden, as long as that person can obtain the information on his or her own. With so many similarities to a Swedish report, it is hard to see why the storage place in these cases should determine the executive jurisdiction issue."**

(52) As for other European countries, I confine myself to referring to case law reviews by expert groups of the Council of Europe in 2012 and 2016, and a working group under the EU Commission in 2018.

(53) The result of the review of the expert group of the Council of Europe in 2012 is thoroughly presented in Swedish Official Report 2017: 89 on pages 469 et seq. This presentation shows that it is not unusual that the state deems itself entitled to conduct a search like that in the case at hand, also if it is clear that the data is stored on a foreign server. Another expert group of the Council of Europe submitted a report on 16 September 2016 titled "Criminal justice access to electronic evidence in the cloud …". As regards practice, the following is stated on page 16 in paragraph 45:

> **"It seems to be widespread practice that law enforcement in a specific criminal investigation access data not only on the device of the suspect but also on connected devices such as email or other cloud service accounts if the device is open or the access credentials have been obtained lawfully even if they know that they are connecting to a different, known country."**

(54) The inquiry carried out by the EU group leaves the same impression. The following is stated on page 11 of the report called SWD (2018) 112, dated 17 April 2018:

> **"The national law in at least 20 Member States empowers authorities, subject to judicial authorisation, to seize and search a device and remotely stored data accessible from it …"**

(55) The report continues by stating that the relevance of this is increasing as data are now regularly stored "… on servers in a different location, possibly outside of the Member State concerned or even outside of the EU."

(56) From international literature, I mention only "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations" from 2017. The manual is prepared with the participation of a number of international experts upon invitation by "the NATO Cooperative Cyber Defence Centre of Excellence". Under the explanatory text to "Rule 11 – Extraterritorial enforcement jurisdiction", it is emphasised that resolving jurisdiction issues may be complex "in the cyber context», see paragraph 12. As I see it, the report expresses that the experts – in favour of accepting territorial

jurisdiction – emphasise whether the relevant data «is meant to be accessible from the State concerned», see paragraph 13, and whether access to the data can be obtained by exercising the state's enforcement jurisdiction over individuals or private entities domiciled in the country, see paragraphs 16 and 17.

(57) *Summary of case law*

(58) This review shows that no custom under international law exists in this area. According to information provided, case law that may serve as guidance is scarce.

(59) Yet, it is interesting that many states, in practice, seem to accept a search like that in the case at hand. Also, there is no information on inter-state reactions to a country's authorities accessing data stored in another state through coercive measures against legal entities in its own territory.

(60) *Starting point for the assessment whether the principle of sovereignty has been violated*

(61) As long as there is no international consensus or applicable provisions in any convention or treaty, Norwegians who apply the law must consider independently whether the use of coercive measures violates the sovereignty of another state. When assessing whether the enforcement jurisdiction of Norwegian authorities is limited by the principle of sovereignty in connection with a search in data stored on devices abroad, the following superior question should be asked: Is the relevant search an interference with another state's exclusive enforcement jurisdiction in a way that it violates the sovereignty of that state?

(62) The ultimate assessment must be specific and adjusted to the situation calling for the relevant measure.

(63) The factual circumstances set out in the court of appeal's judgment, which the court seems to have emphasised, are in my view relevant. The grounds given show that the court of appeal has applied a correct interpretation of the law. I will briefly summarise the central aspects.

(64) *The search in Tidal's data – aspects of the assessment*

(65) The court of appeal emphasised that the coercive measure – the decision to conduct a search in Tidal's data and the order to give access to the company's computer system – is initiated on Norwegian soil, at Tidal's office in Oslo.

(66) As the proceedings have demonstrated, the decision to allow a search is made by Norwegian courts while maintaining general rule of law guarantees.

(67) Also, it is clear that the data is made available through a coercive measure against a Norwegian company with an office in Norway, which means that Norwegian authorities are not, on their own, intruding into data stored abroad.

(68) In this respect, I add that it is clear that Norwegian authorities have enforcement jurisdiction over the Norwegian company and its employees present in this country. On these grounds, Norwegian authorities may order the company and these persons to provide the information necessary for Norwegian authorities to access the data. On a national level, the legal basis in this regard is section 1999 a of the Criminal Procedure Act. The relevant search was carried out by using the access credentials the company had given to Økokrim.

(69) The court of appeal's ruling sets out that the search only involves access to information the company itself has stored. And the company is at any time free to retrieve the data from the foreign storage place.

(70) Finally, it is clear that the data remains on the server abroad. Also, no changes are made to the stored information, for instance in the form of deletion or encryption. A possible seizure is carried out by copying the data onto storage media in Norway.

(71) At any rate, in a situation is like the one at hand, I cannot see that the search will affect another state to an extent that it constitutes a violation of the principle of sovereignty.

(72) Consequently, the court of appeal has correctly applied the relevant legal standards, and the appeal should be dismissed.

(73) I add that questions with regard to limitations to the possibility to seize information found in the search – here as in other situations – must be decided under the relevant rules in the Criminal Procedure Act, in particular section 204 that deals with the protection of lawyer-client correspondence and trade secrets. Any dispute concerning the access to evidence may be brought before the court as usual, see section 205 subsections 2 and 3 and section 208. Also, submissions that a seizure will result in a violation of the defendant's rights – for instance under the Norwegian Constitution and ECHR on the right to privacy and the right to a fair trial – may be legally tried in this manner.

(74) I vote for this

O R D E R :

The appeal is dismissed.

(75) Justice **Falch:** I agree with the justice delivering the leading opinion in all material respects and with his conclusion.

(76) Acting Justice **Lindsetmo:** Likewise.

(77) Justice **Høgetveit Berg:** Likewise.

(78) Justice **Webster:** Likewise.

(79) Following the voting, the Supreme Court gave this

O R D E R :

The appeal is dismissed.