Supreme Court's DECISION

Case no.

delivered in Stockholm on 30 March 2023

Ö 5686-22

PARTIES

Appellant

HO

Counsel and Public Defender: Attorney SB

Respondent

Prosecutor General

Box 5553

114 85 Stockholm

THE MATTER

Remote search order

RULING APPEALED

Judgment of the Göta Court of Appeal of 01/09/2022 in case Ö 3245-22

_____

SUPREME COURT
Riddarhustorget 8

Postal address
Box 2066
103 12 Stockholm

Telephone +46 8 561 666 00
Fax -
E-mail:
hogsta.domstolen@dom.se
www.hogstadomstolen.se

Office hours
08:00–12.00
13:15–16.00

THE SUPREME COURT'S DECISION

The Supreme Court declares that it has been possible to order a remote search, even though the requested search concerns information that may be stored abroad.

The Supreme Court, which denies leave to appeal in the remainder of the case, dismisses the case.

SB shall receive compensation from public funds for the defence of HO in the Supreme Court in the amount of SEK 36,050. Of the amount, SEK 28,840 relates to work and SEK 7,210 relates to value added tax. The State shall bear the cost.

CLAIMS IN THE SUPREME COURT

HO has requested that the Supreme Court annul the Court of Appeal's remote search order.

The Prosecutor General has opposed modification of the decision of the Court of Appeal.

The Supreme Court has granted the leave to appeal referred to in para. 6.

REASONS FOR THE DECISION

Background

1. HO is suspected of aggravated money laundering and aggravated accounting offences. During the preliminary investigation, the prosecutor requested that the District Court order a remote search for documents that could be relevant to the investigation of the offences.

2. According to the prosecutor, the documents were stored in readable information systems, which were accessible on mobile phones and computers seized from the HO. The prosecutor stated that it was unclear on which cloud service, and where in the world, the information being sought was stored.

3. The District Court, concluding that the conditions for ordering a remote search were met, granted the request. The order was limited to a search of documents stored in readable information systems that can be accessed outside of certain mobile phones and computers stated in the decision. The order stated, in particular, that the search could only be carried out by means of authentication in the readable information systems, and that it could not encompass documents covered by the prohibition of seizure in Chapter 27, Section 2 of the Code of Judicial Procedure.

4. The Court of Appeal upheld the District Court's decision.

5. Execution of the contested decision has been concluded.

6. The Supreme Court has granted leave to appeal as regards the question whether it has been possible to order a remote search, even when the search relates to information that may be stored abroad. A stay in proceedings has been issued as regards leave to appeal in the remainder of the case. (See "*Den verkställda genomsökningen*", Supreme Court decision of 17 March 2023, in the present case.)

Precedential matter

7. The matter of precedent in the case regards whether a remote search can be ordered even when the information sought may be stored abroad.

Remote search order

What is meant by a remote search

8. A remote search is a coercive measure enabling access to electronic data that may be relevant as evidence and that is stored, for example, on external servers or cloud-based internet services during a criminal investigation. This coercive measure is regulated in Chapter 28, Sections 10 a—10 i of the Code of Judicial Procedure.

9. A remote search order allows for the search of documents stored in a readable information system outside the electronic communication device (e.g., mobile phone or computer) used to conduct the search (see Chapter 28, Section 10 a). The measure can be carried out using equipment that has been seized or found during a search of premises or a body search, but it can also be carried out using the equipment of the public authority (see Govt. bill 2021/22:119 pp. 76 & 178). A readable information system refers to an electronic communications device or a user account for, or a correspondingly delimited part of, a communications service, storage service or similar service (cf. Section 1, second paragraph *Lagen om hemlig dataavläsning*, 2020:62). Documents found during the search can be copied for perpetuation of evidence.

10. A remote search thus gives the executing authority access to information stored outside the equipment to which it has access. For example, the authority may access information in internet-based applications, including messaging services and social media accounts, where the information is stored outside the mobile phone or tablet used to access the information.

Preconditions for remote searches

11. Under Chapter 28, Section 10 b of the Code of Judicial Procedure, a remote search may be carried out to search for documents that may be of importance for the investigation of a criminal offence or for the investigation of whether there are grounds for confiscation under Chapter 36, Section 1 b of the

Criminal Code. There must be reason to believe that an offence punishable by imprisonment has been committed. As a general rule, the measure may only be carried out in a readable information system that the person reasonably suspected of the offence can be assumed to have used. Even in other cases, however, the measure may be taken if there is particular reason to believe that it is possible to find documents that may be of importance to the investigation of the offence. In these respects, the preconditions for the measure are essentially the same as the preconditions for a search of premises (cf. Chapter 28, Section 1).

12. The measure may only be carried out through authentication in the readable information system (see Chapter 28, Section 10 b, third paragraph). This means that law enforcement authorities may not use other means to access system content than those available to the user of the service. Thus, if access to the content requires, for example, a username and password, biometric authentication or login with a personalised code, the authorities must have access to what is required. The provisions do not allow the installation of software or hardware or the use of other methods to circumvent the necessary authentication.

13. In addition, remote searches require *that* the measure does not encompass information that, according to Chapter 27, section 2 of the Code of Judicial Procedure, prevents seizure; *that* the person affected by the measure may, under certain circumstances, be present at the search or otherwise informed of the measure; *and that* the measure is proportionate (see Chapter 28, Sections 10 c, 10 e, 10 g and 10 i).

14. Remote searches are, by design, of an instantaneous nature, and it is therefore not possible to use the coercive measures for continuous surveillance. The measure may not be extended pending the arrival and

storage of additional documents. (Govt. bill 2021/ 22:119 pp. 78 et seq. & 177.)

Decision-making procedure

15. A remote search is ordered by the leader of the preliminary investigation, the prosecutor or the court. If the search is likely to be extensive, or to cause serious inconvenience to the person affected by the measure, the measure should not be taken without a court order, unless delay entails risk. (See Chapter 28, Section 10 d.)

16. If a search order has been issued by the court, it can be appealed in accordance with the general rules on appeals. However, the order is immediately enforceable (see Chapter 30, section 12, first paragraph, item 3). If the order is issued by the preliminary investigation supervisor or prosecutor, there is no possibility of appeal (cf. Govt. bill 2021/ 22:119 p. 91). However, to the extent that documents found have been copied, the person affected by the measure, regardless of who ordered the search, always has certain possibilities to request the court to destroy the copies (see further Chapter 27, Section 17 e).

Remote searches involving or potentially involving foreign servers

The provisions on remote searches are not limited to searching for information located in Sweden

17. When executing a remote search order, Swedish authorities may come across electronic documents stored abroad or in an unknown location. At issue is whether this circumstance constitutes an impediment to the measure, either in the sense that a remote search order cannot be issued in the first place or that the order cannot be executed.

18. The provisions on remote searches are, with their wording, not limited to searches of information stored in Sweden. Nor does anything in the legislative history of the provisions indicate that such a limitation was intended. On the contrary, it is clear that a restriction of this kind would significantly counteract the purpose of the legislation, as Swedish authorities would then regularly be obliged to request legal assistance from foreign authorities. The negative impact of such a restriction would be of particular significance when it is not known where the information is stored (a so-called "loss of location"), as Swedish authorities would then, in practice, lack the possibility to request legal assistance.

19. There is no reason to assume otherwise than that the relevant interests with regards to legal certainty and protection of privacy — e.g., the interests in protecting certain particularly sensitive information (cf. Chapter 27, Section 2 of the Code of Judicial Procedure) — can be satisfied just as satisfactorily when the information sought is located abroad.

20. Against this background, it is clear that a remote search involving information stored abroad is compatible with the provisions of Chapter 28 of the Code of Judicial Procedure. The decisive issue is rather whether public international law or any international agreement binding on Sweden precludes such an application.

Enforcement jurisdiction

21. According to Chapter 2, Section 12 of the Criminal Code, a court shall observe the limitations that follow from public international law or an international agreement that is binding on Sweden. The provision primarily refers to limitations on judicial jurisdiction, i.e., limitations on the Swedish court's jurisdiction to judge a specific offence. The limitations arise mainly from international law rules on immunity, but other international law standards

must also be taken into account. Limitations on the competence of Swedish courts that are based on international law also, in principle, entail an impediment to the use of coercive measures (cf. Govt. bill. 1984/ 85:156 p. 5). The limitation on the use of coercive measures is thus derived from the limitation imposed on the court's jurisdiction.

22. However, even where a Swedish court clearly has jurisdiction over a particular offence, there are restrictions under international law regarding the use of coercive and other enforcement measures. In particular, the executive jurisdiction of a state is limited to the territory of that state, and the state is thus prohibited from taking enforcement measures in the territory of other states. This is an application of the "territoriality principle" vis-à-vis enforcement measures. Application of that principle here should be distinguished from cases where the jurisdiction of the Swedish court to judge a particular offence is to be assessed. That the limitation of Swedish enforcement jurisdiction to Swedish territory must be taken into account can be said to follow from Chapter 2, Section 12 of the Criminal Code, or from the grounds for that provision.

23. In order for international law to constitute an impediment to Swedish jurisdiction or Swedish enforcement jurisdiction, it is required, according to Chapter 2, Section 12, that there be an established norm in international law limiting national jurisdiction in the individual case. Thus, no positive support under international law for the exercise of jurisdiction in accordance with Swedish provisions is required. (See "*The Universality Principle*" Supreme Court decision of 10 November 2022 in case Ö 1314-22, paragraphs 12–14.)

24. As indicated above, it is a general principle of international law that the executive jurisdiction of a state is limited to its own territory. This principle is an outgrowth of the international law principle of state sovereignty. If a law enforcement authority carries out a criminal procedural measure, such as an

arrest or search, in another state without the authorisation of that state, this is typically considered a violation of the territorial sovereignty of the other state. However, the principle of territoriality was developed in an era when enforcement measures typically required the physical presence of representatives of the authorities at the site of enforcement. It is not always clear how the principle is to be understood when such a representative carries out a measure affecting another state without entering the territory of that state.

The Swedish discussion

25. Swedish legislation on coercive measures has no provisions regarding when Swedish authorities can exercise executive jurisdiction. However, it must be considered presumed that the Swedish legislation on coercive measures, including Chapter 28 of the Code of Judicial Procedure, can only be applied if the Swedish courts have jurisdiction in the case. It is also clear that the principle of territoriality must be respected. If Swedish authorities lack the jurisdiction to execute a coercive measure that concern another state and there is no agreement with that state, they are required to request legal assistance from the authorities of the other state. (See para. 21 and 22.)

26. However, views differ regarding whether this also prevents Swedish authorities from accessing electronic documents that are stored abroad but accessible through equipment located in Sweden.

27. The issue has been addressed in the preparatory works for the provisions on remote searches. The inquiry report preceding the legislation noted that, in the Swedish preparatory works and the legal doctrine, it is generally assumed that Swedish authorities are prevented from accessing electronic information stored abroad, and that this applies even when the owner of the information is in Sweden. However, the inquiry stated that there

are persuasive reasons for adopting a different approach, and that the issue should be left to case law. (See Swedish Government Official Reports 2017:100 p. 362 et seq., also Swedish Government Official Reports 2017:89 p. 443 et seq. See also Ministry Publications Series 2005:6 p. 282.)

28. In the resulting bill, the Government stated that it is vital, in the interests of effective law enforcement, that the rules regarding access to electronic evidence can be practically applied, even in cases where the information is located outside Sweden or where its location is unknown. However, the Government did not consider that it had a basis for considering the issue of executive jurisdiction outside Sweden more thoroughly. (Govt. bill 2021/22:119 p. 85 et seq.)

29. The question of what limitations arise from international law is not in itself determined by the the Swedish legislator. However, it can be noted that there is, at present, no generally accepted Swedish view of the implications of international law in this matter.

Treaty limitations?

30. The issue of whether, and under what conditions, it is acceptable for law enforcement authorities of one state to access information stored on a server in another state, or in an unknown location, is the subject of international attention and debate. In both the Council of Europe and the EU, extensive work has been done to reach common solutions.

31. The main international regulation in this area is the Council of Europe Convention on Cybercrime (ETS No. 185). The Convention, commonly known as the Budapest Convention, was adopted in 2001 and entered into force in 2004. Sweden has been a party to the Convention since 1 August 2021.

32. One purpose of the Convention is to lay the groundwork for swift and effective international cooperation in combatting cybercrime. Under Article 32 of the Convention, a state that is party to the Convention may, without the authorisation of another such party state, access stored computer data that is publicly available, irrespective of its geographical location. It is also permissible for a state to access data, held by another state, through a computerised system in its territory if the former state obtains the lawful and voluntary consent of the person legally entitled to disclose the data to the state through the computerised system.

33. When the Convention was drawn up, it was not possible to reach an agreement on what would apply in other situations. However, Article 32 does not preclude a state that is a party to the Convention from obtaining access to information stored abroad in situations other than those listed in the Article. (See Council of Europe, Explanatory Report to the Convention on Cybercrime, 2001, p. 53, para. 293 with reference to Article 39(3) of the Convention.)

34. Sweden is not bound by any other international agreement regulating the jurisdiction of law enforcement authorities in accessing information stored abroad or in an unknown location. Overall, this means that treaty law imposes no restrictions for Swedish authorities to obtain such access.

Customary law limitations?

35. The question is then whether such limitations follow from the general rules developed in international law (customary international law). It is usually considered that such a rule exists if a general practice of states has developed (state practice) and this has been accepted as law.

36. Several international reports have noted that the absence of a clear, effective and practicable international regulatory framework has led states to

increasingly opt for unilateral means of accessing electronically stored information in cloud-based services. In several countries, criminal investigation authorities are permitted to access information on external servers in the course of a criminal investigation, if the storage medium is open during the investigation or the law enforcement authority has legally obtained login details, even if the information is known to be stored in another country. However, in other counties this is forbidden. (See, e.g., *Transborder access and jurisdiction: What are the options? Report of the Transborder Group, Cybercrime Convention Committee (T-CY*), Council of Europe, 2012, and *Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY.* Final report of the T-CY Cloud Evidence Group, Council of Europe, 2016.)

37. In this respect, it can be particularly noted that, in both Denmark and Norway, it has been considered permissible for law enforcement authorities to gain access to electronically stored information held abroad (see the decision of the Danish Højesteret, UfR 2012 p. 2614 [H.K. 10 May 2012 in Case 129/2011] and the decision of the Norwegian Høyesterett, HR-2019-610-A).

38. Against this background, it is clear that there is no existing state practice that might form the basis of a customary international law rule preventing public authorities from accessing electronic information that is or may be stored on servers outside the territory of their own state.

Conclusion

39. The provisions of the Code of Judicial Procedure regarding remote searches are designed to allow for the search of information stored outside Sweden (see para. 17–20). There are no international law obstacles to such searches (see para. 21–38). Whether it is known in which country the information is stored, or whether the location of the information being stored is unknown, is of no consequence.

40. The above applies provided that the measure is taken in the context of a Swedish criminal investigation and is thus prompted by a suspicion of an offence that falls within Swedish jurisdiction (cf. para. 21); in this context, a case of legal assistance to a competent foreign authority may be equated with a Swedish criminal investigation. It must also be assumed that the measure is taken using equipment available in Sweden and that it is carried out in such a way that the information sought is not deleted or otherwise affected in terms of its content. However, given the formulation of the provisions on remote searches, these conditions usually exist when the coercive measure is ordered and executed. Further, there is no reason to impose any special requirement for a connection to Sweden, e.g., that the suspect be domiciled in this country or that the storage be provided by a company established in Sweden.

41. A remote search can therefore be ordered, under the conditions set out above, even if the information sought may be stored abroad.

The assessment in this case

Assessment of the issue on which leave to appeal has been granted

42. The search in question was intended to be carried out in the context of a preliminary investigation conducted in Sweden and using equipment available in Sweden. It has not been likely to affect the content of the information in the storage site. Under these circumstances, the fact that the information sought may be stored abroad does not constitute an impediment to the measure (see para. 39 and 40).

The issue of leave to appeal in the remainder of the case

43. With the contested decision, the Court of Appeal has found that the measure is compatible with the conditions set out in Chapter 28 of the Code of

Judicial Procedure. No grounds for granting leave to appeal have emerged in these respects.

The case shall be dismissed

44. Execution of the remote search order has now been concluded. This entails that the Supreme Court's position on the matter shall not result in a decision to reject the appeal. Instead, the case shall be dismissed. (See "*Den verkställda genomsökningen*", cf. para. 6 above.)

_____

_____ _____ _____

_____ _____

Justices of the Supreme Court Anders Eka, Agneta Bäcklund, Sten Andersson (reporting Justice), Petter Asp and Johan Danelius participated in the ruling. Judge referee: Hanna Hallonsten