KKO:2023:14 – Admission of ANOM messages into evidence

Diary number R2022/712
Issued on 23 February 2023
ECLI:FI:KKO:2023:14

Background of the case and the issue before the Supreme Court

The US Federal Bureau of Investigation (FBI) and the Australian Federal Police had co-operated in a sting operation, codenamed Trojan Shield, where the FBI had established a messaging platform called ANOM. The ANOM smartphone app could be used for sending messages to another phone running the same app, with the service being touted as being fully secure. ANOM smartphones had been distributed especially among persons involved in organised or habitual crime. Unbeknownst to the users, the messages had been intercepted and stored on an FBI-operated server. The FBI had read and analysed the messages and on its own initiative forwarded them to countries to which it had assumed the messages to pertain, including to the Finnish police.

The public prosecutor brought charges against several defendants for aggravated narcotics offences and offered ANOM messages intercepted in the context of the FBI operation as evidence. The defendants argued that the messages should be ruled inadmissible as they had been obtained through unlawful means and their use would compromise the fairness of the trial. The District Court and the Court of Appeal rejected the inadmissibility argument.

The matter before the Supreme Court was whether the ANOM messages had been obtained through unlawful means and, if so, should they be ruled inadmissible as evidence.

Applicable law

According to the general rule in chapter 17, section 1 of the Code of Judicial Procedure, a party has the right to present the evidence that he or she wants to the court hearing the case. Section 25 of the same chapter contains provisions concerning the admissibility of unlawfully obtained evidence. Paragraphs (1) and (2) of the section cover the absolute inadmissibility of evidence obtained by means of torture or in breach of the protection against self-incrimination; these provisions were not at hand in the present case. The applicable provision appears in paragraph (3) of the section, according to which a court may in cases not covered by paragraphs (1) or (2) use also evidence that has been obtained unlawfully unless such use would endanger the conduct of fair proceedings, taking into consideration the nature of the matter, the seriousness of the violation of law in

obtaining the evidence, the significance of the manner of obtaining the evidence in relation to its credibility, the importance of the evidence for the resolution of the case, and the other circumstances.

The Supreme Court held that the general rule in such situations is that evidence obtained through unlawful means other than those referred to in paragraphs (1) and (2) may be used. The Supreme Court made reference to the preparatory works concerning the relevant legislation, which emphasised the primacy of the principle of free evaluation of evidence and the exceptional character of a ruling of inadmissibility. The Supreme Court referred also to the case-law of the European Court of Human Rights, according to which the utilisation of unlawfully obtained evidence, other than in cases of serious rights violations such as torture, does not constitute a violation of Article 6 ECHR, provided that the proceedings as a whole meet the criteria of a fair trial.

Assessment of unlawfulness

The FBI had carried out the interception by storing the messages sent by means of the ANOM app on a server in an undisclosed location. The FBI had not requested legal assistance from Finnish authorities so as to procure the evidence, nor had it applied for or been granted a warrant for covert surveillance under the Coercive Measures Act of Finland. However, the evidence had been lawfully provided to Finland on the FBI's own initiative and permission for the use of the messages as evidence had been granted by the competent authority of the United States.

The Supreme Court held that the assessment of the lawfulness or unlawfulness of the manner of obtaining evidence in Finland should proceed in accordance with the relevant Finnish legislation and with the human rights obligations binding on Finland.

According to section 10(2) of the Constitution of Finland, the secrecy of correspondence, telephony and other confidential communications is inviolable. Under paragraph (4) of the section, legislation may be enacted on necessary restrictions of this secrecy e.g. in the investigation of crimes that jeopardise the security of the individual or society or the sanctity of the home, at trials and security checks, and deprivation of liberty. According to Article 8 ECHR, everyone has the right to respect for private and family life, home and correspondence. Under para. 2 of the Article, there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The ANOM messages were confidential messages sent by persons in Finland to other persons in Finland. The interception of the messages had therefore constituted interventions in the rights of persons subject to the jurisdiction of Finland. This was not a messaging platform in general use, but rather a restricted and ostensibly secure platform intended for the use of a very limited group of individuals. That being said, the senders and the addressees of the messages were entitled to the protection of their privacy and the confidentiality of their communications. This secrecy could be breached only by means allowed by law. As a matter of fact, it had not even been claimed that the messages would have been obtained in accordance with the Coercive Measures Act or other Finnish legislation. The Supreme Court held that the messages had been obtained through unlawful means.

Assessment of inadmissibilitv

Assessment of inadmissibility

The Supreme Court noted that, in the application of the provision concerning admissibility, the relevant case-law of the European Court of Human Rights was of decisive significance. The threshold for admissibility was not to be set at a higher level than that set in that case-law. Hence, if the European Court of Human Rights, in view of its earlier case-law, would probably consider that the admission of the evidence constitutes a violation of the right to a fair trial or, in a case where EU law applies, the admission would be contrary to EU law as interpreted in the case-law of the European Court of Justice, the evidence must be ruled inadmissible. If not, the admissibility even of unlawfully obtained evidence was justified.

The Supreme Court noted that the Code of Judicial Procedure does not contain any specific provision on the admissibility of evidence obtained through criminal incitement, that is, in a way where the police or some other authority or a person acting on their behalf incites someone to commit an offence that they would not have committed had the incitement not taken place. According to the established case-law of the European Court of Human Rights the admission of evidence obtained through criminal incitement renders the proceedings unfair. Therefore, the Supreme Court held the general rule to be that evidence obtained through criminal incitement is inadmissible directly by virtue of the manner in which it has been obtained.

ANOM smartphones had been offered to persons identified as being linked to serious crime. There is no doubt that the messaging app had made it easier for its users to communicate among themselves and that it could have lowered the threshold for planning and committing criminal offences. That said, it had not even been alleged that the FBI had been in touch with the defendants or e.g. sought to buy drugs from them. The ANOM app had been one possible alternative for communication among the defendants; before being able to utilise the platform, they must have known the usernames of the other users in order to make contact to them. The FBI or any other authority had not established the contacts among the defendants or among other persons and there also otherwise was no indication that the FBI, any other authority or someone acting on their behalf would have incited the defendants to commit criminal offences. The Supreme Court held that there were no grounds for a ruling of inadmissibility on the basis of criminal incitement.

As regards the nature of the matter as an assessment criterion, the Supreme Court noted that regardless of the seriousness of the alleged offence, the defendant has the right to a fair trial. Accordingly, the seriousness of the alleged offence was to be given only relatively little weight in the assessment of admissibility. In the present case, the most serious charges pertained to aggravated narcotics offences, but the ANOM messages had been offered as evidence also relating to charges of regular narcotics offences, doping offences and illegal dealing with imported goods. That said, also these less serious charges were parts of the same whole and involved aggravating circumstances. The nature of the matter was not held to be an argument for the inadmissibility of the ANOM messages.

As regards the seriousness of the violation of law in obtaining the evidence, the Supreme Court noted first that the interception of the ANOM messages had constituted an essential violation of the rights to personal privacy and security of confidential communications, as enshrined in section 10 of the Constitution and in Article 8 ECHR. That being said, due note was to be given to the fact that ANOM smartphones had been offered to persons involved in organised crime. It could have been assumed that the messages to be intercepted would pertain mainly to the planning and commission of serious offences. In addition, users of ANOM smartphones ought to have been aware that they may be subject to police surveillance. The matter did not go to the core of personal privacy and the manner of obtaining the evidence had not been inhuman or degrading. Moreover

privacy and the manner of obtaining the evidence had not been inhuman or degrading. Moreover, the interception of the ANOM messages had been grounded on the purpose of preventing serious crime that is detrimental to public safety, which was a legitimate reason for restricting the protection of personal privacy as referred to in section 10(4) of the Constitution and in Article 8, paragraph 2 ECHR. Even though the unlawful interception of the ANOM messages had constituted a violation of the privacy of the defendants and of the secrecy of their confidential communications, these circumstances reduced the seriousness of the rights violation, with the result that the seriousness of the violation was according to the Supreme Court not an argument for the inadmissibility of the ANOM messages.

The defendants had alleged that the FBI had participated in the commission of narcotics offences by developing and providing the ANOM app. In this respect, the Supreme Court noted that the provision of the ANOM service was comparable to the provision of any other communications platform and that the provision of such service did not in itself mean complicity in a narcotics offence. However, the Supreme Court also noted that in view of the circumstances, the interception of the ANOM messages might meet the constituent elements of some of the data and communications offences governed by the Criminal Code of Finland. However, even where the manner of obtaining the evidence were criminalised, this would not mean that the evidence is directly inadmissible. Some arguments had been offered also on how the interception of the ANOM messages and the FBI sting operation in general should be assessed under US law. There were no indications that the operation would have been unlawful according to US law. In addition, there were no indications that the Finnish authorities would have acted unlawfully or attempted to exert undue influence on what kind of material would be sent in from the FBI. Accordingly, the accounts of the conduct of the US authorities or Finnish authorities were not an argument for the inadmissibility of the ANOM messages.

In conclusion relating to the seriousness of the violation of law in obtaining the evidence, the Supreme Court held that even though the interception of the messages had constituted a violation of the defendants' right to privacy and the secrecy of their confidential communications, the seriousness of the violation or the conduct of the authorities, when assessed as a whole, were not arguments for the inadmissibility of the messages as evidence.

As regards the significance of the manner of obtaining the evidence in relation to its credibility, the Supreme Court noted that the unlawfulness of the manner of obtaining the evidence had not bearing on whether the platform had worked reliably, that is, whether the messages offered as evidence were authentic and uncorrupted. There were no tangible indications that the FBI or someone else would e.g. have edited the contents of the messages or held back any relevant messages from among those provided to the Finnish authorities. There was no reason to believe that the messages would have been written by someone else than the person under whose name they appeared in the materials. Hence, the manner of obtaining the messages did not compromise their credibility as evidence and there was no argument for the inadmissibility of the messages as evidence.

As regards the importance of the evidence on the resolution of the case, as an assessment criterion, the Supreme Court made reference to case-law of the European Court of Human Rights, where note had been taken of whether also other evidence had been available and whether the unlawfully obtained evidence had lower probative value or supported other, lawfully obtained evidence. That said, even one piece of credible evidence with high probative value, even if obtained unlawfully, can under certain circumstances be taken as sufficient proof without this compromising the fairness of the trial. The Supreme Court noted that the ANOM messages were not the only

evidence in support of the charges, but that they had a lot of importance as proof. The messages constituted strong and credible evidence. As the defendants had not needed to use coded language, the course and internal consistency of the discussions could be assessed quite easily. In view of the credibility of the messages, their use as evidence did not compromise the fairness of the trial and hence was not an argument for the inadmissibility of the messages.

According to the law, also other circumstances could be taken into account in the assessment of admissibility. The Supreme Court noted that all defendants were represented by counsel, and they therefore had had the opportunity to contest the admissibility, credibility, and probative value of the messages with the help of a legal advisor. The defendants had had access to the same materials as the public prosecutor. There had not been any other violations of the rights of the defence either.

In conclusion, the Supreme Court held that no such circumstances had arisen that would indicate that the admissibility of the ANOM messages as evidence would compromise the fairness of the trial, and there therefore were no grounds for a ruling of inadmissibility. The Supreme Court upheld the decision of the Court of Appeal regarding admissibility.

Published 27.4.2023