CASE TRANSLATION: DENMARK

CASE CITATION:
U 2012.2614 H

NAME AND LEVEL OF COURT:
Højesteret (Supreme Court)

DATE OF DECISION:
10 May 2012

MEMBERS OF THE COURT:
Peter Blok, Poul Søgaard, Marianne Højgaard Pedersen, Thomas Rørdam and Jens Peter Christensen

Social media; publicly available information; police obtaining information of social media; interception of communications; jurisdiction; Denmark

Closed doors

SUPREME COURT ORDER

delivered on Thursday 10 May 2012

Case 129/2011

Prosecution

against

T

(Advocate Lars Lindhard, appointed)

In previous instances, the district court in Esbjerg and the High Court of Western Denmark Second Department handed down rulings on 20 October 2010 and 8 February 2011 respectively. On 15 April 2011, leave to appeal was granted by the Appeals Permission Board, allowing the High Court's ruling to be brought before the Supreme Court.

Five judges participated in the adjudication: Peter Blok, Poul Søgaard, Marianne Højgaard Pedersen, Thomas Rørdam and Jens Peter Christensen.

Allegations

T has reiterated his claim before the High Court that the police are not authorised to carry out data acquisition of T's Facebook profile (X @ X) and Messenger profile (Y @ Y), and that the police's data reading on 19 October 2010 of T's profile on Facebook should not be approved.

The prosecution has argued that the High Court ruling be upheld, however, provided that the interventions are approved in accordance with the Administration of Justice Act's rules on repeated secret searches; in the alternative, as determined by the High Court in accordance with the Administration of Justice Act's rules on data reading.

Pleas

Concerning the Administration of Justice Act § 791 b relating to the reading of data, T has submitted that the rule cannot be applied because his Facebook profile and Messenger profile cannot be considered to be information systems, i.e. a computer or other data processing system.

The conditions for search are not met, since there does not exist anything that can be searched, because the information resides on a server. The conditions for the interception of communications are also not met.

Although the crime under investigation is subject to Danish criminal jurisdiction, a clear legal basis and a license from the country's authorities are required for the police to undertake action outside its borders. Neither the statutory authority nor the permission exists.

The fact that the police can actually gain access to these profiles from Denmark, does not mean that the profiles are necessarily subject to Danish jurisdiction when the holder of the profiles resides in another country and uses the profiles from there, and when the servers are located in other countries.

It is clear from the rules for Facebook, that Facebook is based in Santa Clara County, California, that all data are stored on a server in the United States, and that Californian law applies to the relationship between Facebook and the profile owner. The Messenger profile is domiciled in Luxembourg. The authorities in these countries should therefore have been involved. In addition, he has had to connect to these services via a Canadian telecommunications provider, when he stayed in Canada, so the Canadian authorities should have approved the police actions.

The rules on criminal procedural measures must necessarily be subject to a strict interpretation. Analogies and expanded interpretations cannot be considered.

The prosecution contends that the measure is similar in nature, or equivalent to repeated secret searches, and

that the conditions laid down in accordance with the Administration of Justice Act § 799, see § 793 paragraph 1, no. 1, for doing so are met. The police have, by using the correct username and password subsequent to the ruling of the District Court, repeatedly logged on T's Facebook and Messenger profiles for the purpose of examination of the information and messages that were to be found during the respective investigation times, including messages received and sent (e-mails, chat, etc.). The information on T's wall on Facebook, which for example can contain status updates, can most accurately be compared with a bulletin board found in a house by the police in connection with a search. The police have therefore obtained access to a 'snapshot' similar to that which the police can achieve by a physical search. The intervention did not include information in transit, and therefore the rules on the interception of communications are not applicable.

In support of it being a question of search, see Report no 1023/1984, page 55, and Report no 1377/1999 section 6.1 and the preparatory work for Law no 465 of 7 June 2001 on receiving stolen goods and other subsequent complicity and for IT investigations, see Bill no 194, the parliamentary year 2000-01, the general comments section 4.2. It is also supported by the preparatory work for Act no 378 of 6 June 2002, where, amongst other things, the rules on reading data were inserted.

In relation to the search rules, it is immaterial that the data in question was not stored on a computer belonging to T, but on servers affiliated with Facebook and Messenger, given that the information can be accessed by using the correct username and password and without the involvement of the provider of Facebook and Messenger or other third parties.

The intervention must be assumed to be of crucial importance to the investigation of the case, hence this condition is complied with, both as regards the search rules and data reading rules.

If assumed that the intervention is fully or partially covered by the Administration of Justice Act's rules on the interception of communications, these conditions are also satisfied, see Administration of Justice Act § 781, paragraph 1.

According to the preparatory work for the Administration of Justice Act § 791 b, paragraph 1, it seems the rules on reading data are directed, in particular, at cases in which the police by installing sniffer programs or other items of equipment on a computer to be able to gain access to information residing in the computer in question. In the present situation, it is hardly a question of the reading of the data being done with the assistance of 'programs or other equipment.'

The criminal procedural measure is carried out as part of a criminal investigation conducted by the Danish authorities with a view to possible prosecutions in Denmark. The investigation of the case, including the implementation of the criminal procedural measures, must therefore be carried out in accordance with the rules in the Administration of Justice Act. The court shall only consider whether the conditions for the interventions are fulfilled in accordance with rules in the Administration of Justice Act; not whether the implementation of the action in that case will require assistance from foreign authorities, or whether it could be implemented by Danish police on their own.

The legal basis

On the limitations of a search with respect to other coercive procedural measures, reference is made to the Bill's general explanatory notes on report 1159/1989, see FT 1996/1997, appendix A, sp. 2488. In the explanatory notes the following is stated regarding the report:

> 'It follows, amongst other things, that the concept of search also includes the examination of e.g. electronic media in the same manner as paper is likely to be a carrier of semantic content. It will thus constitute a search, if you read a floppy disk found during a search, or information that is stored in the memory on a computer. It is also deemed to be a search to play a message that was previously recorded on an answering machine.
>
> Conversely, the interception of correspondence between the computer of the accused and a computer in another location or the interception of a telephone conversation is an intervention in the confidentiality of communications, which is regulated by the rules of the Administration of Justice Act Chapter 71.'

Reasoning of the Supreme Court and decision

The police may gain access to T's Facebook and Messenger profiles from any computer with internet access using only the codes that the police became familiar with through telephone intercepts.

The information that the police can learn from such interventions is – in the same way as e-mails that are sent and received – not information in transit. The information is stored in profiles and available using the codes.

The Supreme Court finds that the interventions have the characteristics of repeated secret searches that can be made on the basis of the Administration of Justice Act § 793.1, subparagraph 1, pursuant to § 799.

Since the crime with which T is charged is subject to Danish criminal jurisdiction, as the matter is under investigation by the Danish authorities, and as the interventions can be made without involving foreign authorities, it cannot lead to a different result, that T from February 2010 to February 2011 was abroad, and that the information contained in the profiles reside on servers abroad.

Accordingly – and since the other conditions for approving the interventions in the Administration of Justice Act § 794 are found to be fulfilled – the Supreme Court upholds that the police are permitted to read T's Facebook and Messenger profiles.

For the reasons stated by the district court, the Supreme Court also upholds that the police's reading on 19 October 2010 is approved in accordance with the Administration of Justice Act § 796, paragraph 3.

It is held:

The police are allowed to take readings of T's Facebook profile (X @ X) and Messenger profile (Y @ Y) as repeated secret searches, and the police's reading on 19 October 2010 of T's Facebook profile is approved.

With thanks to Helena Lybæk Guðmundsdóttir for her help with this translation.

Helena Lybæk Guðmundsdóttir is a PhD student at the department of law at Aalborg University. Her main area of research is cybercrime law. Other interests include data privacy law and European Union law.

helena@law.aau.dk

Commentary

By Lars Bo Langsted

The fact that Supreme Court finds that Facebook and Messenger profiles are subject to the rules of search in the Administration of Justice Act is hardly surprising. Given that the preparatory work of the rules of search expressly mentions that reading the content of a computer or listening to messages left in an answering machine is a search, it would be more surprising had Supreme Court reached another conclusion regarding this question.

The really interesting item in this ruling is the question of jurisdiction. There are two sub-questions involved of which Supreme Court, however, only seem to address one. The first sub-question is the issue of criminal jurisdiction: whether the acts of the defendant come within Danish criminal jurisdiction. The answer is – undoubtedly – yes. The crime that was under investigation was a drug related crime and since the defence counsel does not doubt that there is criminal jurisdiction for the alleged crime, it is safe to assume that it has been committed on Danish territory or had the necessary connection to Denmark. The second sub-question is the hardest: whether Danish police are allowed to use investigative measures that involve foreign territory and thus foreign jurisdiction.

As a rule, the police are not allowed to investigate in territories other than that of Denmark. To a limited extent, some European Union legislation[1] allows the police to continue a pursuit after a criminal when trying to escape arrest. Any other investigative measure, however, is to be taken by the foreign, local police authority if they are asked to assist. In the physical world this means that any kind of search – or seizure for that matter – can only be carried out by the local police. The Danish police are able to search computers and the like within Danish territory. If the Danish police suspect that a computer with compromising content is to be found in Germany or Russia, they have to ask the German or Russian authorities for their assistance to carry out the search.

In the case at hand, the 'computer', meaning the content of the Facebook and Messenger profiles, were undoubtedly physically located on a server in California,

1 *Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, OJ 197, 12.07.2000, pp 0001–0002; Protocol established by the Council in accordance with Article 34 of the Treaty on European Union to the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, OJ C 326, 21.11.2001, pp 2–8; European Convention on Mutual Assistance in Criminal Matters and Protocols (Strasbourg, 20.IV.1959); Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (Strasbourg, 17.III.1978); Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (Strasbourg, 8.XI.2001).*

USA. Under normal circumstances this would mean that the Danish police should ask for the assistance from the American police authorities to carry out a search of the content. But in this case, the Danish police were able to carry out the search from their own office in Denmark since they were in possession of the necessary username and password and because the content of the computer in question was linked to the internet, which meant it was accessible from the entire world.

The Danish rules on criminal jurisdiction do not cover acts that have no direct connection to Denmark. In brief: attacks or intrusions carried out from abroad against computers on Danish territory are under Danish jurisdiction. This is the same for content on web pages that are directed at Danish relations or to Danish consumers. Any other content stored in computers (physically placed outside Danish territory) or of web pages – regardless of whether they are accessible from Denmark – fall without Danish jurisdiction (unless of course the content was written in the Danish territory).

Returning to the question of investigative jurisdiction, the rules on criminal jurisdiction would lead to the assumption that if – and only if – the content of a computerized system was accessible from Denmark and had some linkage to Denmark in way of content or language or was created in Danish territory, it would be admissible for the Danish police to carry out the necessary investigation under Danish legislation and without being bound to have admission from the local police authorities. The Supreme Court, however, seems to have taken a shortcut. The Court does not mention that the content of the profiles in question have a specific link to Denmark, other than the fact that the suspected 'original' criminal acts were covered by Danish criminal jurisdiction and that the Danish police were undertaking the investigation. But this misses the point, since it would most likely be the case every time the Danish police conduct an investigation and that does not – as referred above – give Danish police any authority to take investigative measures on a foreign territory. It seems as if the Supreme Court has simply stated that the search was legal because it was possible.

Perhaps that is the message from Supreme Court. And maybe that is the rational way of rethinking investigative jurisdiction when it comes to the internet. The users of the internet do not know – and could not know – where the servers they are using, passing or visiting are situated. And the point is: they do not care. The physical positions of the servers are irrelevant to the users, and Supreme Court says: it is irrelevant to us and to the police. One might say that Danish Supreme Court with this ruling has accepted cyberspace as a place of its own, but at the same time part of the investigative jurisdiction of Denmark (and any other country?).

Lars Bo Langsted is professor of law in the department of law at Aalborg University, Denmark. His research interests include economic crime, corporate crime and professional negligence. He has been a member of several committees on criminal legislation as well as of the Appeals Permission Board.

http://www.langsted.dk

lbl@law.aau.dk