

Danish data retention: Back to normal after major crisis

By IT-Pol

The Danish police and the Ministry of Justice consider access to electronic communications data to be a crucial tool for investigation and prosecution of criminal offences. Legal requirements for blanket data retention, which originally transposed the EU Data Retention Directive, are still in place in Denmark, despite the judgments from the Court of Justice of the European Union (CJEU) in 2014 and 2016 that declared general and indiscriminate data retention illegal under EU law.

In March 2017, in the aftermath of the Tele2 judgment, the Danish Minister of Justice informed the Parliament that it was necessary to amend the Danish data retention law. However, when it comes to illegal data retention, the political willingness to uphold the rule of law seems to be low – every year the revision is postponed by the Danish government with consent from Parliament, citing various formal excuses. Currently, the Danish government is officially hoping that the CJEU will revise the jurisprudence of the Tele2 judgment in the new data retention cases from Belgium, France and the United Kingdom which are expected to be decided in May 2020. This latest postponement, announced on 1 October 2019, barely caught any media attention.

However, data retention has been almost constantly in the news for other reasons since 17 June 2019 when it was revealed to the public that flawed electronic communications data had been used as evidence in up to 10000 police investigations and criminal trials since 2012. Quickly dubbed the “telecommunications data scandal” by the media, the ramifications of the case have revealed severely inadequate data management practices by the Danish police for almost ten years. This is obviously very concerning for the functioning of the criminal justice system and the right to a fair trial, but also rather surprising in light of the consistent official position of the Danish police that access to telecommunications data is a crucial tool for investigation of criminal offences. The mismatch between the public claims of access to telecommunications data being crucial, and the attention devoted to proper data management, could hardly be any bigger.

According to the initial reports in June 2019, the flawed data was caused by an IT system used by the Danish police to convert telecommunications data from different mobile service providers to a common format. Apparently, the IT system sometimes discarded parts of the data received from mobile service providers. During the Summer of 2019, a new source of error was identified. In some cases, the data conversion system had modified the geolocation position of mobile towers by up to 200 meters.

Based on the new information of involuntary evidence tampering, the Director of Public Prosecutions decided on 18 August 2019 to impose a temporary two-month ban on the use of telecommunications data as evidence in criminal trials and pre-trial detention cases. Somewhat inconsequential, the police could still use the potentially

flawed data for investigative purposes. Since telecommunications data are frequently used in criminal trials in Denmark, for example as evidence that the indicted person was in the vicinity of the crime scene, the two-month moratorium caused a number of criminal trials to be postponed. Furthermore, about 30 persons were released from pre-trial detention, something that generated media attention even outside Denmark.

In late August 2019, the Danish National Police commissioned the consultancy firm Deloitte to conduct an external investigation of its handling of telecommunications data and to provide recommendations for improving the data management practices. The report from Deloitte was published on 3 October 2019, together with statements from the Danish National Police, the Director of Public Prosecutions, and the Ministry of Justice.

The first part of the report identifies the main technical and organisational causes for the flawed data. The IT system used for converting telecommunications data to a common format contained a timer which sometimes submitted the converted data to the police investigator before the conversion job was completed. This explains, at least at technical level, why parts of the data received from mobile service providers were sometimes discarded. The timer error mainly affected large data sets, such as mobile tower dumps (information about all mobile devices in a certain geographical area and time period) and access to historical location data for individual subscribers.

The flaws in the geolocation information for mobile towers that triggered the August moratorium were traced to errors in the conversion of geographical coordinates. Mobile service providers in Denmark use two different systems for geographical coordinates, and the police uses a third system internally. During a short period in 2016, the conversion algorithm was applied twice to some mobile tower data, which moved the geolocation positions by a couple of hundred meters.

On the face of it, these errors in the IT system should be relatively straightforward to correct, but the Deloitte report also identifies more fundamental deficiencies in the police practices of handling telecommunications data. In short, the report describes the IT systems and the associated IT infrastructure as complex, outdated, and difficult to maintain. The IT system used for converting telecommunications data was developed internally by the police and maintained by a single employee. Before December 2018, there were no administrative practices for quality control of the data conversion system, not even simple checks to ensure that the entire data set received from mobile service providers had been properly converted.

The only viable solution for the Danish police, according to the assessment in the report, is to develop an entirely new infrastructure for handling telecommunications data. Deloitte recommends that the new infrastructure should be based on standard software elements which are accepted globally, rather than internally developed systems which cannot be verified. Concretely, the reports suggests using POL-INTEL, a big data policing system supplied by Palantir Technologies, for the new IT infrastructure. In the short term, some investment in the existing infrastructure will be necessary in order to improve the stability of the legacy IT systems and reduce the risk of creating new data flaws. Finally, the report recommends systematic

independent quality control and data validation by an external vendor. The Danish National Police has accepted all recommendations in the report.

Deloitte also delivered a short briefing note about the use of telecommunications data in criminal cases. The briefing note, intended for police investigators, prosecutors, defence lawyers and judges, explains the basic use cases of telecommunications data in police investigations, as well as information about how the data is generated in mobile networks. The possible uncertainties and limitations of telecommunications data are also mentioned. For example, it is pointed out that mobile devices do not necessarily connect to the nearest mobile tower, so it cannot simply be assumed that the user of the device is close to the mobile tower with almost “GPS level” accuracy. This addresses a frequent critique against the police and prosecutors for overstating the accuracy of mobile location data – an issue that was covered in depth by the newspaper Information in a series of articles in 2015. Quite interestingly, the briefing note also mentions the possibility of spoofing telephone numbers, so that the incoming telephone call or text message may originate from a different source than the telephone number registered by the mobile service provider under its data retention obligation.

On 16 October 2019, the Director of Public Prosecutions decided not to extend the moratorium on the use of telecommunications data. Along with this decision, the Director issued new and more specific instructions for prosecutors regarding the use of telecommunications data. The Deloitte briefing note should be part of the criminal case (and distributed to the defence lawyer), and police investigators are required to present a quality control report to prosecutors with an assessment of possible sources of error and uncertainty in the interpretation of the telecommunications data used in the case. Documentation of telecommunications data evidence should, to the extent possible, be based on the raw data received from mobile service providers and not the converted data.

For law enforcement, the October 16 decision marks the end of the data retention crisis which erupted in public four months earlier. However, only the most imminent problems at the technical level have really been addressed, and several of the underlying causes of the crisis are still looming under the surface, for example the severely inadequate IT infrastructure used by the Danish police for handling telecommunications data. The Minister of Justice has announced further initiatives, including investment in new IT systems, organisational changes to improve the focus on data management, improved training for police investigators in the proper use and interpretation of telecommunications data, and the creation of a new independent supervisory authority for technical investigation methods used by the police.



Denmark: Our data retention law is illegal, but we keep it for now (08.03.2017)
<https://edri.org/denmark-our-data-retention-law-is-illegal-but-we-keep-it-for-now/>

Denmark frees 32 inmates over flaws in phone geolocation evidence, The Guardian (12.09.2019)
<https://www.theguardian.com/world/2019/sep/12/denmark-frees-32-inmates-over-flawed-geolocation-revelations>

Response from the Minister of Justice to the reports on telecommunications data (in Danish only, 03.10.2019)
<http://www.justitsministeriet.dk/nyt-og-presse/pressemeddelelser/2019/justitsministerens-reaktion-paa-teledata-redegoerelser>

Can cell tower data be trusted as evidence? Blog post by the journalist covering telecommunications data for the newspaper Information (26.09.2015)
<https://andreas-rasmussen.dk/2015/09/26/can-cell-tower-data-be-trusted-as-evidence/>

(Contribution by Jesper Lund, EDRI member IT-pol, Denmark)