Case law on the data retention of electronic communications and its impact on national legislation and criminal proceedings

Andres Parmas, Prosecutor General, Estonia

Current situation and issues arisen in Estonian domestic law:

- Recent years have presented Estonia with a set of acute and critical problems concerning gathering evidence obtained via data retention of electronic communications and using this kind of evidence in criminal proceedings.

- In June 2021, the Supreme Court of Estonia decided[1] that electronic communication data, which telecommunication companies were obliged to gather and retain based on Art 111[1] of the Electronic Communications Act, cannot be requested for the purpose of investigating crimes, because the data storage and use procedure in force in Estonia is contrary to the European Union law, taking into account the European Court of Justice preliminary ruling from 2nd March 2021[2].

    - More precisely, the Supreme Court concluded that Art 15(1) of the E-Privacy Directive (2002/58/EC), in conjunction with Articles 7, 8, 11 and 52(1) 11 of the EU Charter of Fundamental Rights must be interpreted as contradicting domestic legal provisions according to which telecommunication companies are obliged to gather and retain proactively in a general and indiscriminate manner the communications data and the Prosecutor's Office has the right to make inquiries to obtain this data.

    - The Supreme Court decided that the aforementioned EU law provisions are in contradiction with the Estonian domestic regulation which allows the Prosecutor's Office to make requests to telecommunication companies in order to obtain data related to telephone call traffic, as well as location data, which are stored for criminal proceedings under the Electronic Communications Act, for the purpose of investigating crimes.

- The paradigm shift regarding the lawfulness of data retention of electronic communications for the purpose of investigating crimes has led to a legally unclear and unpredictable situation.

    - Telecommunication companies currently continue to retain certain communications data for their business purposes. Also, the norm obliging Telecoms to gather and retain data is still in force and for the time being it seems

[1] Case No. 1-16-6179
[2] Case No. C-746/18

that Telecoms must retain data for other purposes than criminal investigation (most notably for internal or external security purposes).

- The Prosecutor's Office has abstained to request for retained data based on the quashed obligation in Art 111^1 of Electronic Communications Act but has requested the same data as something that the Telecoms possess notwithstanding this obligation for billing purposes (based on Art 102 of the Electronic Communications Act).
  - Statistically, the number of requests has significantly decreased however since the referred decision of the Supreme Court:
  - In the period from 01.10.2020 to 30.04.2021, the prosecutor's office granted around **1024** permits to request communication data.
  - In 2022 the prosecutor's office submitted **less than 350 requests** to the pre-trial judge to grant access to the communication data. In 2023 the number of requests has remained approximately the same.

- The alternative investigative approach to obtaining evidence by requesting access to communications data is obtaining data using covert investigative measures. While the former involves accessing metadata like call logs or location history with telephone mast accuracy, the latter entails immensely more invasive measures such as wiretapping, covert monitoring or gaining access to the entire content of the communication device. Despite the significantly larger intrusion on personal rights that surveillance entails, current court practice paradoxically suggest a trend towards favoring this approach.

- The real issue arising from Estonian case law lies in the fact that it is unpredictable and often not consistent. Moreover, a recent district court ruling from mid-May this year, although not yet in force, concluded that since the legal obligation to general and indiscriminate proactive retention of the communications data was quashed, using such data obtained from the telecommunications companies is unlawful and is inadmissible as evidence. Yet, the district court failed altogether to address the fact that recently only communication data that the Telecoms possess because of billing purposes has been requested. Hence the question remains open. The situation is further complicated because Telecoms do not have different databases for data stored on different legal bases. Hence, the differentiation of the source of data is only imaginary anyway.

- A further problem is that in many cases, initiation of the use of covert measures is based on the evidence gathered from the communications data. Therefore, if the communications data is declared inadmissible as evidence, this renders evidence gathered by covert measures also inadmissible. This presents a significant concern for numerous ongoing criminal proceedings, severely threatening the prosecution of many types of crimes.

- At the same time, it is profoundly paradoxical that the legal framework permits social media companies to function, allowing them to store vast amounts of personal data. These business models are designed to capitalize on user data. Conversely, states are restricted from using similar data to fulfill their fundamental aims and obligations of

investigating and deterring crimes, as well as aiding victims. This contradiction raises critical questions about the balance between privacy and security, highlighting the controversy over allowing commercial exploitation of data while limiting its use for public safety and justice.

Way forward:

- The ECJ's recommendations regarding selective data gathering are impractical, particularly in terms of proposed geographic limitations. Regarding telecommunications, the strength of signal coverage and whether the telecommunication device is in the range of a particular mast is influenced by weather conditions, further complicating the issue. The ECJ's recommendation to target specific individuals amounts to mass profiling, which is inherently discriminatory and, in that sense, incomprehensible. Apart from ethical concerns that such practices raise, it could lead to disastrous consequences to members of targeted groups (such as suspected pedophiles) should a database be breached. Therefore, it is preferable to treat everyone equally and to find a way to store the communications metadata in an indiscriminatory fashion.

- In the current European context, the approach preached by the ECJ may be dangerous due to evolving security challenges such as ongoing war in Europe, growing sabotage, and terrorism. On that background the Estonian Ministry of the Interior is working on a draft legislation, which aims to further justify an indiscriminate regime of data retention under the guise of security considerations. However, this would not alleviate the concerns of criminal investigation in most cases not directly related to national security.

- Moving forward, if the European Union is aware of the associated risks, it would be more effective to implement regulations at the EU level. The European Commission could introduce a new regulation to address these concerns comprehensively. Moreover, the way forward should not only involve the continued debate over the retaining and use of telecommunications data such as data about telephone calls and SMS messages. Instead, we must shift our focus to contemporary communication methods, such as internet calls (e.g., WhatsApp) and messaging services, which predominantly include platforms like FaceTime. These forms of communication are fundamentally different in terms of data storage requirements and regulations, for which there are currently no comprehensive rules. Our existing frameworks, related to traditional phone infrastructure, are outdated. We should prioritize developing new regulatory frameworks for obtaining evidence in criminal proceedings that address the current landscape of digital communication.