January 12, 2016

Panoptykon Foundation

POLICE AND SECRET SERVICE ACCESS TELECOMMUNICATION AND ONLINE DATA: Current Status, Human Rights Standards, Latest Proposals and Conclusions

1. Introduction and Key Terms

Telecommunication data are data referred to in Article 180c of the Telecommunication Law of 16 July 2004 (hereinafter called "TL") and include:

- Subscriber data, i.e. subscriber name and address (conf. Article 180c Paragraph 1 Item 1 of TL);

- Billing data (date, time and duration of call, conf. Article 180c Paragraph 1 Item 2 Letter a of TL);

- Mobile phone location (conf. Article 180c Paragraph 1 Item 2 Letter c of TL);

- Other data such as IP number (conf. Article 180c Paragraph 1 and 2 of TL).

Online data are data referred to in Article 18 Paragraph 1-5 of the Electronic Service Provision Law of 18 July, 2002 (hereinafter called "ESPL"). They include information that is essential for the provision of electronic service, i.e. delivery address for online purchase, (conf. Article 18 Paragraph 1) and data that 'characterise the usage method of electronic service", i.e. usage data including information about each instance of service use, i.e. scope, start and end time (conf. Article 18 Paragraph 5 of ESPL). The concept of online data is fuzzy. It covers such items as the IP number, personalised information about the operating system and browser. Some experts believe the concept also covers the content of email correspondence (see the legal opinion published by Helsinki Foundation for Human Rights[1]).

Entities that have access to telecommunication and online data include: Police, Border Guards, Internal Security Agency (ABW), Central Anti-corruption Bureau (CBA), Military Police, Military Counterintelligence Service (SKW) Tax Audit Service and Customs Service (hereinafter: **authorised entities**).

2. Terms and Conditions of Access to Telecommunication and Online Data by Authorised Entities

a. Access to Telecommunication Data

[1] http://www.hfhr.pl/uwagi-hfpc-do-projektu-zmian-w-uprawnieniach-sluzb/

Poland has implemented the Retention Directive (Directive 2006/24/EC) and has granted access to telecommunication data to authorised entities under the following terms and conditions:

- Access to data is authorised in respect of any criminal case the given entity is authorised to investigate (conf. Article 20c Paragraph 1 of the Police Law), and in respect of analytics (conf. Article 18 Paragraph 1 Item 1 of the CBA Law);

- Access to data is subject to no external scrutiny by a court or external agency;

- No safeguards have been adopted to ensure that information about the use of telecommunication data can be obtained by the person whose data are being used;

- Access to data to achieved via the telecommunication network and does not involve employees of the telecommunication provider at hand (conf. Article 20c Paragraph 2a of the Police Law)

According to annual reports submitted by the Office of Electronic Communication to the European Commission, authorised entities submit approximately 2 million queries to telecommunication providers per year.

b. Access to Online Data

- Authorised entities have access to online data "to support pending investigations" (conf. Article 18 Paragraph 6 ESPL);

- There is no external scrutiny whatsoever over such use of online data by authorised entities;

- According to Panoptykon Foundation research[2], access to data is achieved by way of written queries to internet service providers;

- The total number of online data access queries is not known. The said research suggests that the Internal Security Agency made 692 queries in 2012 (meanwhile, ABW made 115,652 queries for telecommunication data in the same year).

3. What Are the Guidelines of the Case Law

In its ruling of 30 July 2014 (ref. K 23/11) The Constitutional Tribunal ascertained that the legislation that gives authorised entities access to telecommunication data is unconstitutional "in that it does not provide of independent scrutiny over access to telecommunication data". The Tribunal also stated that enabling legislation on ABW, SKW and CBA is unconstitutional because it does not stipulate an obligation to destroy data that are irrelevant for investigations. The ruling of the Tribunal enters into force 18 months after the sentence, i.e. on 6 February, 2016. On this date, the legislation on access to telecommunication data becomes ineffective. The Tribunal has indicated that courts or

---

[2] *Access of public authorities to the data of Internet service users*: https://panoptykon.org/sites/default/files/publikacje/transparency_report_pl_1.pdf)

other independent bodies must be given the right to exercise control over access to data. In principle, such control should be ex-ante with some exceptions allowed by the Tribunal.

Meanwhile, on 8 April 2014, the European Court of Justice stated (joined cases C-293/12 and C-594/12) that the Retention Directive (Directive 2006/24/EC) was null and void because it violated Article 7 and 8 of the Fundamental Rights Charter. ECJ stated that the following were measures were required to achieve compliance with EU legislation:

- Access to telecommunication data should be limited exclusively to "serious crime" cases;

- A prior consent of a court must be obtained each time access telecommunication data is sought;

- A mechanism must be introduced whereby the individual whose telecommunication data have been accessed (retrieved) must be informed (ex-post, with possible exceptions)

4. What Are the Amendments in the Bill

Key amendments include:

- Equal terms and conditions for retrieval of telecommunication and online data are introduced. Retrieval will be authorised for the purpose of "detection, acquisition, investigation and prosecution of crimes" (conf. proposed Article 20c of the Police Law) and , in some cases, also for the purpose of analytical work (conf. proposed Article 18 Paragraph 1 Item 1 of the CBA Law);

- Retrieval of online data is allowed via ICT networks;

- Control over the retrieval of telecommunication and online data (conf. proposed Article 20c of the Police Law). Under the proposed terms and conditions, authorised entities will report the total number of queries to the court every 6 months. The court may (not an obligation) perform random checks of such queries. Data deemed by the court as unlawfully retrieved will not have to be deleted.

- Data will have to be examined to assess whether they are essential for further investigation, redundant data are to be deleted.

5. Evaluation and Key Areas of Concern

The Bill is not compliant with the Polish Constitution and EU legislation, i.e. personal data and privacy protection in accordance with the Charter of Fundamental Rights[3]. It fails to comply with the rulings of the Constitutional Court and ECJ because it does not provide for external control over access to telecommunication data. The proposed control mechanism is not genuine:

- Control is to be exercise ex-post rather than ex-ante

[3] Conf. opinion of the Sejm Analytics Office re the Bill (Polish version): http://sejm.gov.pl/Sejm8.nsf/druk.xsp?documentId=B30BB05699C73CE8C1257F310040516D

- Control is optional. Given there will be no additional judge positions opened in Polish courts, judges will not take these measures.

- Data will not be deleted if found to be in violation.

The Bill extends and facilitates options to retrieve online data. Today, online data can be accessed as part of ongoing investigations. In contrast, the Bill provides that this will be possible for the purpose of "detection, acquisition, investigation and prosecution of crimes". The Bill authorises the retrieval of telecommunication data via telecommunication networks (secure link). This creates a risk of a radical increase in the number of online data queries. Given a similar level of privacy intrusion, access to online data should be subject to similar controls as are provided for telecommunication data.

The Bill fails to solve the issue of the deletion (destruction) of telecommunication/online data. There will be no regular checks of the relevance of retried data. In effect, such citizen information can be retained for ever.