Strasbourg, 27 May 2016 **CDL(2016)019***

Opinion No. 839/ 2016 Engl. only

EUROPEAN COMMISSION FOR DEMOCRACY THROUGH LAW

(VENICE COMMISSION)

POLAND

DRAFT OPINION

ON THE ACT OF 15 JANUARY 2016 AMENDING THE POLICE ACT AND CERTAIN OTHER ACTS

ON THE BASIS OF COMMENTS BY

Mr Iain CAMERON (Member, Sweden)
Ms Regina KIENER (Member, Switzerland)
Mr Ben VERMEULEN (Member, the Netherlands)

**This document has been classified restricted on the date of issue. Unless the Venice Commission decides otherwise, it will be declassified a year after its issue according to the rules set up in Resolution CM/Res(2001)6 on access to Council of Europe documents.*

TABLE OF CONTENTS

I. Introduction

1. By letter of 29 January 2016, the Chair of the Parliamentary Assembly's Monitoring Committee[1] requested the opinion of the Venice Commission on the law of Poland called "Act of 15 January 2016 amending the Police Act and certain other acts". According to its Article 17, the Amendments came into force on 7 February 2016.

2. Mr Iain Cameron, Ms Regina Kiener and Mr Ben Vermeulen were invited to act as rapporteurs on this opinion. On 28 and 29 April 2015, a delegation of the Venice Commission visited Warsaw and held meetings with the State authorities, politicians, lawyers and NGO representatives. The Venice Commission expresses its gratitude to the Ministry of Foreign Affairs of Poland for the excellent organisation of the visit.

3. The present opinion was prepared on the basis of the comments submitted by the rapporteurs based on the English translation of the Police Act and other relevant legislation (see CDL-REF(2016)036). This translation may not always accurately reflect the original version in Polish on all points; therefore, certain issues raised may be due to problems of translation.

4. *The present opinion was adopted by the Venice Commission at its … Plenary Session, in Venice (… 2016).*

II. Scope of the analysis

5. The purpose of the 2016 amendments was to regulate various methods of secret surveillance[2] employed by various law-enforcement and intelligence agencies. State agencies may obtain information by various means: through witnesses or informants, by searching premises, conducting "classical" surveillance (following a person on the street), etc. However, the main reason why the amendments attracted so much public attention and criticism[3] was the power of State agencies to obtain information by monitoring the *means of communication* and other tools including: computers, telephones, databases, e-mails, social networks, etc. Hence, in analysing the amendments the Venice Commission will concentrate on the legislative provisions regulating those methods of surveillance.[4]

6. The focus of the present opinion will be on the "regular" law-enforcement action which involves surveillance for the purposes of combatting crime within the country. The Venice Commission will not analyse surveillance by the external intelligence services, military counter-intelligence and alike. The Venice Commission is aware that the line between classical law-enforcement surveillance and intelligence gathering conducted for national security purposes is

[1] Committee on the Honouring of Obligations and Commitments by Member States of the Council of Europe

[2] The term "surveillance" is used in this opinion in two meanings: as a general term denoting all kinds of secret information gathering, and in a more narrow sense, as covert monitoring of the *content* of private communications (as opposed to the "metadata collection" – about this distinction see paragraphs 15 et seq. below).

[3] Within Poland, the amendments to the Police Act and other acts were strongly criticised by, among others, the Polish Ombudsman, the Inspector General for Data Protection, the National Council for the Judiciary, the Polish Bar Council as well as members of the parliamentary opposition. Some authoritative civil society organisations claimed that while the purpose of the new legislation ostensibly was to implement the Constitutional Court judgment from July 2014, it further expands surveillance powers in many areas and conflicts with Poland's international human rights obligations. On 13 January 2016, the European Union expressed its will to launch a Structured Dialogue with Polish authorities under the Rule of Law Framework in order to assess the necessity of making use of Article 7 TEU to safeguard European values and standards, with regard to several laws recently adopted in Poland, including, among others, the amendments to the Police Act.

[4] In addition, the opinion will also touch upon the covert interception of live conversations – see the analysis of Article 19 of the Police Act below (paragraph 14 below).

blurred.[5] However, the latter remains a very complex and delicate sphere which deserves a separate analysis.[6]

7. The 2016 amendments modified several laws regulating activities of different law-enforcement and intelligence agencies.[7] All those laws basically employ the same model of surveillance (with some minor exceptions).[8] The Venice Commission will concentrate on the Police Act, which may serve, *mutatis mutandis*, as an illustration of regulations concerning other agencies.[9]

8. Finally, the Venice Commission observes that following an application lodged by Mr Bodnar, the Commissioner for Human Rights, the Constitutional Tribunal of Poland is now examining the constitutionality of the 2016 amendments (case no. K 9/16). In deference to the Constitutional Tribunal the Venice Commission will avoid commenting on the compatibility of the 2016 amendments with the Polish Constitution. Instead, it will base its analysis on the international standards applicable in this area and on the examples from other countries illustrating these international standards.

9. In sum, this opinion is not a comprehensive evaluation of all aspects of the amendments. It outlines a number of problematic areas, which attracted attention both domestically and internationally, and which, in the opinion of the Venice Commission, need a revision by the Polish legislator as a matter of priority.

III. Background to the amendments to the Police Act and other Acts

10. The amendments aimed to amend the Polish legal system according to the judgement of the Constitutional Tribunal of Poland of 30 July 2014 (No. K 23/11). In that judgement the Constitutional Tribunal concluded that certain provisions of the original Police Act of 1990 (and several other acts) were incompatible with the Polish Constitution. The Constitutional Tribunal proceeded to a careful and convincing analysis of the domestic constitutional framework and of the international norms regulating surveillance.[10] There is no need to reproduce the reasoning of the Tribunal in detail. It suffices to recall the most essential principles formulated in para. 5.3 of the judgment, which had to be reflected in the process of revision of the legislation on secret surveillance. These principles may be summarised as follows:

---

[5] See the analysis of the EU law by the EU Fundamental Rights Agency Report of 2015 on "Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU; Mapping Member States' legal frameworks", paras. 10-11.

[6] Similarly, the Venice Commission will not touch upon such issues as extraterritorial surveillance and information exchanges between security services of different countries (see, in the Polish context, Article 20 para. 2ab of the Act). The Venice Commission is aware that these are amongst the techniques which are sometimes used to circumvent domestic rules on surveillance; however, these issues do not appear to be at the heart of the domestic discussion over the recent amendments and will not be analysed.

[7] (1) The Act of 6 April 1990 on Police; (2) the Act of 12 October 1990 on the Border Guard, (3) the Act of 28 September 1991 on Fiscal Controls, (4) the Act of 21 Au-gust 1997 on the Military Court System, (5) the Act of 27 July 2001 on the Common Court System, (6) the Act of 24 August 2001 on the Military Police and Military Law Enforcement Units, (7) the Act of 24 May 2002 on the National Security Agency and the Intelligence Agency, (8) the Act of 18 July 2002 on the provision of services supplied by electronic means, (9) the Telecommunications Act of 16 July 2004, (10) the Act of 9 June 2006 on the Military Counterintelligence Service and the Military Intelligence Service, (11) the Act of 9 June 2006 on the Central Anti-Corruption Bureau and (12) the Act of 27 August 2009 on the Customs Office.

[8] The Act not only amends those acts that relate to the different agencies which may implement covert surveillance, but also several other acts relating to the implementation of surveillance measures.

[9] Namely the Police, the Border Guard, the Fiscal Control Service, the Military Police, the National Security Agency and the Intelligence Agency, the Military Counterintelligence Service and the Military Intelligence Service, the Central Anticorruption Bureau, and the Customs Office.

[10] An English translation of the judgment can be found on the web-site of the Constitutional Tribunal: http://trybunal.gov.pl/en/hearings/judgments/art/7004-okreslenie-katalogu-zbieranych-informacji-o-jednostce-za-pomoca-srodkow-technicznych-w-dzialani/

- The law should contain explicit and precise provisions with regard to its material scope, and define which bodies are entitled to collect and process information through secret surveillance;
- The law should determine the types of offences which may warrant the use of such measure of information gathering as secret surveillance; those offences should be "serious" enough to warrant the use of the secret surveillance;
- The law should define the maximum duration of surveillance measures and, where possible, the definition of technical means envisaged to obtain information; [11]
- The law should define the procedure for authorisation of such measures by an independent authority, and provide for independent oversight of the process of obtaining and handling of data related to individuals;
- The law should include an obligation to destroy material which is immaterial or inadmissible and describe a procedure for it; there should be safeguards against unauthorised access to the information collected through secret surveillance;
- The law should provide for the right of the monitored person to be informed, within reasonable time, about surveillance once it is finished, and the right to initiate the judicial review thereof; however, in exceptional circumstances the departure from the notification rule should be possible;
- The relevant services should disclose statistical data on secret surveillance, in order to enable the analysis of its intensity;
- The law may introduce specific rules regulating secret surveillance by the State security and intelligence services (as opposed to the police) and collecting data in respect of non-Polish citizens.

11. In order not to create a legal vacuum, the Constitutional Tribunal gave the legislator 18 months to amend the relevant laws (that is until 7 February 2016). However, the previous legislature was unable to pass the necessary amendments. The new Parliament was formed in November 2015 and thus had limited time to implement the judgement of 30 July 2016. Eventually, the amendments were voted by means of accelerated procedure.

IV. Short description of the Police Act

12. In the following paragraphs the relevant provisions of the amended Police Act are briefly summarised. The Venice Commission will focus on two provisions of the Act: Article 19 (which regulates "classical" surveillance measures) and Article 20c (which describes collection of metadata – the meaning of this term is explained in paragraph 15 below).

13. Article 19 sets out the rules for secret surveillance (named in the official English translation of the Police Act "operational control") ordered "in case of preliminary investigation" with regard to crimes (including potential crimes) listed in para. 1, sub-paras. (1) to (8). As was explained to the rapporteurs of the Venice Commission in Warsaw, secret surveillance under Article 19 is not governed by the formal rules of evidence gathering set by the Criminal Procedure Code – these are two different legal regimes.[12] In general, secret surveillance usually *precedes* opening of a criminal case, providing justification to initiate it. However, not every secret surveillance operation results in the opening of a criminal case.[13] On the other hand, materials obtained

[11] The relevant part of para. 5.3 states that it is "desirable" to indicate those technical means; it follows that this is not a strict requirement but rather a recommendation.

[12] The Criminal Procedure Code contains Chapter 26 which governs the process of gathering evidence through secret surveillance for the purposes of conducting criminal proceedings which are already in place.

[13] In his petition of 18 February 2016 before the Constitutional Tribunal of Poland with regard to the unconstitutionality of the amendments to the Police Act, the Commissioner for Human Rights described it as follows (on pp. 7 and 8): "[…] [The] discussed provisions [Article 19 et al.] do not apply to the issue of operational and investigative activities conducted in the framework of criminal proceedings, in the manner laid down in the Code of Criminal Procedure […]. [The] provisions that are the subject of this application govern activities outside of the scope of criminal procedure,

through secret surveillance may be introduced in evidence in criminal proceedings.[14] Secret surveillance shall be ordered for a period not exceeding 3 months (para. 8); it may, however, be prolonged to a maximum of 18 months (para. 9).

14. According to Article 19 para. 6, secret surveillance includes such measures as listening to and recording of the contents of telephone conversations and correspondence conducted via telecommunications networks (e-mails, messengers, etc.), in ordinary letters, recording "live" conversations with listening devices, etc. Therefore, "classical" secret surveillance under Article 19 allows the police to know the *content* of communications which were supposed by the interlocutors to be private.[15]

15. Article 20c of the Police Act deals with *metadata*. Simply put, metadata is all data connected to and regarding a (tele-)communication. It may include information about phone calls placed or received, numbers dialled, duration of the calls, geographical location of mobile devices at a given moment, web-sites visited, log-ins, personal settings, addresses of e-mail correspondence, etc. Access to metadata does not reveal the *content* of private communications (Article 20c para. 1), at least not in the same way as the "classical" surveillance under Article 19 does. At the same time, as explained further below, the content/form distinction is no longer so clear, and metadata may reveal considerable information about a person's private life. The meaning of "metadata" is further developed in the relevant legislation (Telecommunications Act, Act on Electronic Services, and Postal Act).[16]

16. Secret surveillance under Article 19 and metadata collection under Article 20c are ordered on different grounds and implemented within different procedures. As to the grounds, Article 19 contains a closed list of crimes which may warrant surveillance.[17] The legal framework for collecting metadata under Article 20c is much wider. It is done "in order to prevent or detect crimes or in order to save human life and health, or in order to support rescue and find missions". In essence, police may collect metadata for any useful purpose related to the very broad mandate of the police to maintain peace and order.

17. As to the procedure, secret surveillance governed by Article 19 is performed, as a rule, with the prior consent of a district court (see paras. 1 and 2). However, in "cases of the utmost urgency, where any delay could result in the loss of information or the obliteration or destruction of the evidence of a crime", police may start surveillance without prior consent of the court. But, if consent is not granted within the following 5 days, surveillance must be suspended and the material gained should be destroyed (para. 3).

18. By contrast, under Article 20c metadata may be collected *without* prior consent of a court. Article 20ca only establishes a system of *ex-post* review: every six months the police are obliged to pass to a competent court for review a statistical report on metadata collection (para. 2). Finally, Article 20cb sets out the rules for processing and obtaining certain data, that is not subject to any controls, even *ex-post*. In sum, the Police Act establishes two separate, fundamentally different legal regimes: one for "classical" secret surveillance of communications, and another for metadata collection.

---

which could lead to criminal proceedings, but do not involve such a necessity. The literature emphasizes that operational surveillance plays a subsidiary role in relation to criminal proceedings, they precede preparatory proceedings, providing justification to initiate preparatory proceedings […]".

[14] See, for example, Article 19 para. 15g which describes conditions in which materials containing "privileged communications" may be lawfully used in criminal proceedings.

[15] The Venice Commission stresses that Article 19 of Act speaks of the *secret* access to the content of the correspondence, letters, e-mails etc. In many jurisdictions law-enforcement bodies may also implement *open* monitoring of communications in respect of some groups of persons, most often prisoners. The present opinion will not discuss limitations to privacy which may result from that type of the monitoring.

[16] See CDL-REF(2016)036 which contains the extracts from the relevant legislation in English.

[17] This list is very long to be quoted in its entirety; for more details see CDL-REF(2016)036

19. It appears that metadata collection on the basis of Article 20c is a widely used method of investigation, while "classical" secret surveillance of communications is much rarer. According to the figures provided by the Ministry of Interior, in 2015 the police was investigating 833,361 cases, out of which 215,561 cases related to the crimes mentioned in Article 19 para. 1. In respect of that group of cases secret surveillance was ordered on 8,000 occasions (which represents 0,9% of the overall amount of all pending cases, and 3,7% of the number of listed cases, i.e. cases referred to in Article 19 p. 1). Prosecutor refused police requests for surveillance in 178 cases, the courts refused such requests in 19 cases.

20. As to metadata monitoring, in 2015 various law-enforcement agencies made 1,497,174 queries, of which about 1,3 million related to telecommunications data and 0,2 million to Internet data. In the latter category the law-enforcement agencies requested information inter alia on "www addresses" and "email addresses, internet communicators, blogs, chats" (902 and 4,913 times respectively). Itemized billings (that is information on numbers dialled, date, hour and length of the connections) are the main type of information requested (703,819 queries in 2015). About 330,000 requests related to the less sensitive data (i.e. the subscriber data - name and address of the user of the communication device). The Venice Commission recalls that the population of Poland is over 38 million people.

21. Before passing to a more detailed examination of the Police Act, the Venice Commission would like to stress that the 2016 amendments involve several improvements, if compared to the previously existing system. Thus, for example, the Act now specifies more precisely the means of secret surveillance (Article 19, para. 6),[18] regulates the equipment interference, and sets time-limits for the duration of the continued secret surveillance (see Article 19 para. 9); the Police Act requires the police to keep registers describing secret surveillance operations (Article 19 para. 16a and para. 16b); there is a procedure for *ex-post* judicial control of metadata collection (Article 20ca); the Act provides for the destruction/limited use of materials covered by the professional privilege obtained as a result of surveillance (see Article 19 paras. 15f et seq.); it describes in more details the powers of the relevant services in the sphere of internet metadata collection (Article 20c et seq.), and it imposes the obligation to destroy irrelevant data (Article 20c para. 7).[19]

V. To what extent measures provided by Articles 19 and 20c of the Act amount to an interference with privacy?

22. Article 8 of the European Convention on Human Right (the Convention or the ECHR) protects, *inter alia*, private life and secrecy of communications. Over the years, the notion of "private life" has been developed by the European Court on Human Rights (the ECtHR or the Court); it now includes the right to keep certain information of personal character secret.

23. There can hardly be a simple and comprehensive definition of what sort of information is private. "Privacy" is a complex social construct which develops over time and varies from country to country.[20] It is clear, however, that the *content* of private communications was

[18] Before, Article 19 para. 6 (3) allowed the "use of technical measures, which facilitate obtaining information and evidence in secret as well as recording thereof, especially the content of telephone conversations and other information submitted via the telecommunications networks". This formula was given a broad interpretation in the judgement of the Constitutional Tribunal of 30 July 2014, para. 6.1.2: "[The] Tribunal assumes that the challenged provisions – as this arises from the linguistic interpretation thereof – make it possible inter alia: to conduct audio surveillance of persons and premises, which includes the interception of conversations held via landline, mobile and Internet telephony; to intercept text and multimedia messages sent via telephone devices as well as other equipment used for distant communication; to apply devices that register the location of persons and objects and which rely on satellite navigation; or to intercept electromagnetic emanations".

[19] Special rules apply for the surveillance measures implemented by the Military Counter-intelligence and the Internal Security Agency.

[20] In *Uzun v. Germany* the European Court of Human Rights held as follows: "Private life is a broad term not susceptible to exhaustive definition" (no. 35623/05, § 43, ECHR 2010 (extracts)).

originally and remains at the core of the protection provided by Article 8 of the Convention. Moreover, some of the secret surveillance measures described in the Act may also involve interference with the home (see Article 19 para. 6 (2) which speaks of "obtaining and recording image or sound of persons from rooms", which clearly involves "bugging" of living premises). Consequently, surveillance measures set out in Article 19 the Act constitute an interference with Article 8 rights.[21]

24. As to the *metadata* collection, the situation is less clear. Until relatively recently, metadata was regarded as being of less sensitivity from the perspective of personal integrity as compared to the content of a communication.[22]

25. However, the advent of the internet, smartphones and other mobile devices changed the perception of metadata. The digital footprint one leaves often results in a great deal of personal information being obtainable by collecting metadata, and by the combined analysis of communications patterns. Oversight bodies have in fact noted a decrease in police agencies' use of intrusive methods of intelligence collection (telephone tapping, etc.) because the same type of information can now be obtained by accessing social media.[23] In addition, there is a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life":[24] thus, for example, information about the circle of close friends may be worth protecting.

26. One may try to distinguish between different types of metadata, depending on their potential to interfere with privacy. A less sensitive type of metadata is, for example, subscriber data, i.e. information which simply indicates which person has which telephone number. Other types of metadata are very close to the information about content of private communications, and can be called "content-related" metadata (for example, the information which reveals the websites a person has visited). Information about geographical location of mobile devices may be more or less sensitive, depending on the circumstances. Thus, the physical location of a person at a given moment of time may sometimes be established by merely observing that person in a public place, which arguably reduces the "privacy expectation" attached to this information. At the same time systematic tracking of all movements of a particular person during a certain period of time, or even real-time, constitutes a much deeper penetration into his or her private life.[25]

27. That being said, the Venice Commission observes that the continuous technological innovations in the field probably argue against making too many distinctions based on the category of data. It is in any event clear that *combining* different types of metadata (for example, comparing content-related data, such as the web-logs, with continuous location data) allows a relatively full picture to be built of a person's habits, interests, connections etc., as was

[21] In addition, surveillance measures might also indirectly affect other human rights the realisation of which depends on the right to privacy, notably the freedom of expression (Article 10 of the Convention – in particular in relation to the right of the journalists not to disclose their sources; see *Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands*, no. 39315/06, 22 November 2012). As far as surveillance practices lead to the interception of confidential communications with lawyers or priests, the Act might also infringe upon the right to a fair trial (Article 6 of the Convention) and freedom of religion (Article 9 of the Convention).

[22] *PG and JH v. UK*, No. 44787/98, 25 September 2001. In this case the Court noted, in particular, as follows: "The information obtained concerned the telephone numbers called from B.'s flat between two specific dates. It did not include any information about the contents of those calls, or who made or received them. The data obtained, and the use that could be made of them, were therefore strictly limited."

[23] See e.g. the Annual Report of the UK Chief Surveillance Commissioner to the Prime Minister and to Scottish Ministers for 2011-2012, at 5.17. "A frequent response to my Inspectors' enquiries regarding a reduction in directed surveillance is that 'overt' investigations using the Internet suffice. My Commissioners have expressed concern that some research using the Internet may meet the criteria of directed surveillance. This is particularly true if a profile is built by processing data about a specific individual or group of individuals without their knowledge."

[24] *Uzun v. Germany*, cited above, § 43

[25] See the ECtHR reasoning in *Uzun v. Germany*, cited above, where the Court analysed effects of the secret surveillance of movements of a person by a GPS-tracker in-built in a car he was regularly using.

shown by an experiment when a German politician installed spyware on his own phone for a month.[26]

28. In *Digital Rights Ireland v Minister for Communications & Others*,[27] the Court of Justice of the European Union (CJEU) examined the compatibility of the European Directive on data retention with Article 7 ("Respect for private and family life") and Article 8 ("Protection of personal data") of the Charter. The CJEU held as follows:

> *"26. […] [The] data which [Internet or telephone providers] must retain, pursuant to Articles 3 and 5 of Directive 2006/24, include data necessary to trace and identify the source of a communication and its destination, to identify the date, time, duration and type of a communication, to identify users' communication equipment, and to identify the location of mobile communication equipment, data which consist, inter alia, of the name and address of the subscriber or registered user, the calling telephone number, the number called and an IP address for Internet services. Those data make it possible, in particular, to know the identity of the person with whom a subscriber or registered user has communicated and by what means, and to identify the time of the communication as well as the place from which that communication took place. They also make it possible to know the frequency of the communications of the subscriber or registered user with certain persons during a given period.*
>
> *27. Those data,* ***taken as a whole*** [emphasis added] *may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them."*

29. Thus, according to the CJEU the disclosure of that kind of information, given its cumulative effect, clearly constitutes an interference with privacy, protected by Article 7 of the Charter. In that case the CJEU annulled the EU Directive on data retention, and several courts in the EU countries have followed, stressing the need for improved controls over metadata collection.[28]

30. The ECtHR also interprets the applicability of Article 8 of the ECHR to such kind of data quite broadly. The use of information relating to the date and length of telephone conversations and in particular the numbers dialled can give rise to an issue under Article 8 as such information constitutes an "integral element of the communications made by telephone".[29] Furthermore, systematic collection and storing of data by security services on particular individuals, even without the use of covert surveillance methods, constituted an interference with these persons' private lives.[30]

---

[26] See https://www.bof.nl/2014/07/30/how-your-innocent-smartphone-passes-on-almost-your-entire-life-to-the-secret-service/

[27] Cases C-293/12 and C-594/12, 8 April 2014

[28] See, e.g. Austrian Constitutional Court, decision G 47/2012 and others of 27 June 2014. In some cases, the negative judgments preceded that of the CJEU; see in particular, the judgment of the German Federal Constitutional Court in 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08 of 2 March 2010 regarding the data retention directive.

[29] *Copland v. the United Kingdom*, no. 62617/00, §43, ECHR 2007-I; see also *Malone v. the United Kingdom*, 2 August 1984, § 84, Series A no. 82; see also the separate opinion by Judge Pinto de Albuquerque in the case of *Bărbulescu v. Romania, no. 61496/08, 12 January 2016*, where he concluded that protection provided by Article 8 "includes not only the content of the communications, but also the metadata resulting from the collection and retention of communications data, which may provide an insight into an individual's way of life, religious beliefs, political convictions, private preferences and social relations".

[30] See *Rotaru v. Romania* [GC], no. 28341/95, §§ 43-44, ECHR 2000-V; *Amann v. Switzerland* [GC], no. 27798/95, §§ 65-67, ECHR 2000-II, where the storing of information about the applicant on a card in a file was found to be an interference with private life, even though it contained no sensitive information and had probably never been consulted

31. Turning to Poland, the Venice Commission observes that the data collected under Article 20c of the Act[31] may disclose social connections of the person, his or her habits, preferences and interests. *Combined* analysis of various types of metadata (which is not excluded by the law) and processing of large volumes of information derived from it may be even more intrusive and give insight into very intimate aspects of the person's private life. Such data are collected *secretly* by *law-enforcement agencies* and may be *used against* this person in criminal proceedings, or against other individuals. In such circumstances it would be more plausible if the Polish legislator started from the assumption that the collection of *most of the types* of metadata under Article 20c of the Act must be seen as an interference with the privacy of the persons concerned.[32]

VI. Substantive and procedural safeguards against abusive surveillance

A. International standards

32. According to international human rights standards, and in particular the ECHR, any measures aimed at obtaining private information should pursue legitimate aims, should be lawful and "necessary in a democratic society" (Article 8 § 2 of the ECHR). As to the first prong of the test (legitimate aim), there is no doubt that the aims of secret surveillance under Article 19 and of the collection of metadata under Article 20c of the Police Act are in compliance with Article 8 § 2 in this respect.[33]

33. Next, any interference should be lawful ("provided by law"). The "lawfulness" requirement implicitly contains the criteria of clarity and foreseeability of the law.[34] In its Grand Chamber judgement in the case of *Roman Zakharov v. Russia*,[35] the Court summarised its jurisprudence on the notion of "foreseeability" in the context of interception of communications as follows: "The domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures". Moreover, the Court held that "since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the discretion granted to the executive or to a judge to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference" (see §§ 243 and 230).

34. Finally, the most complex test under Article 8 is that of "necessity". The analysis of "necessity" includes *inter alia* the examination of the procedure in which particular surveillance measures are ordered, implemented and the way in which data so obtained is used. Those procedural safeguards will vary depending on the type and intensity of the interference. Yet, any procedural safeguards should be sufficiently effective to prevent possible abuses of the system. The ECtHR in its *Klass* judgement has laid down the following test: "The Court must be satisfied that, whatever system of surveillance is adopted, there exist adequate and effective guarantees against abuse. This assessment has only a relative character: it depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures,

[31] On the exact description of what falls into the concept of metadata under the Polish law see in the CDL-REF(2016)036; see also the analysis in paragraphs 60 et seq. of the present opinion.
[32] See, as an example, *Copland*, cited above, §§41-44.
[33] Such measures should be "in the interests of national security, public safety or the economic well-being 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."
[34] See, for example, *Heglas v. Czech Republic*, No. 5935/02, 1 March 2007, § 74. In addition, the ECtHR jurisprudence also discusses the question of accessibility of the legislation to the persons concerned; however, it doesn't seem to be an issue *in casu*.
[35] *Roman Zakharov v. Russia* [GC], no. 47143/06, ECHR 2015

the grounds required for ordering such measures, the authorities competent to permit, carry out and supervise such measures and the kind of remedy provided by the national law".[36] In a later judgement on surveillance measures the Court indicated that the law should specify "[the] nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration [of telephone tapping]; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed".[37]

35. In the above-cited *Roman Zakharov* case, the Grand Chamber of the Court summarised the ECtHR case-law on the question whether an interference was "necessary in a democratic society" in the following way:[38]

> *"[The] Court has acknowledged that, when balancing the interest of the respondent State in protecting its national security through secret surveillance measures against the seriousness of the interference with an applicant's right to respect for his or her private life, the national authorities enjoy a certain margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security. However, this margin is subject to European supervision embracing both legislation and decisions applying it. In view of the risk that a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there are adequate and effective guarantees against abuse. The assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law. The Court has to determine whether the procedures for supervising the ordering and implementation of the restrictive measures are such as to keep the 'interference' to what is 'necessary in a democratic society'".*

36. The CJEU, in the above-sited case of *Digital Rights Ireland and Seitlinger and Others* held, in particular, that Directive 2006/24 on data retention did not set out clear and precise rules regarding the extent of the interference, that it did not require a relationship between the data retained and the seriousness of the crime or public security issue. The CJEU criticised the Directive in that it didn't set substantive or procedural conditions (like review by an administrative authority or a court prior to access) which would determine the limits of access to and use of the data retained by competent national authorities. Nor did the Directive determine the time period for which data are retained on the basis of objective criteria. Not least, the Directive did not set out clear safeguards for the protection of retained data (see §§ 56 et seq.).

37. The argument can be made that the judgment should be interpreted so as to forbid totally the blanket retention of data. Even if such an extensive interpretation is not followed, it is clear that the blanket retention of data is a major contributor to public concerns. These can only be met by the creation of a strong independent oversight system (see further below, paragraphs 111 et seq.).

---

[36] *Klass and others v. Germany*, no 5029/71, § 50.
[37] See, inter alia, *Prado Bugallo v. Spain*, no. 58496/00, § 30, 18 February 2003; *Liberty and others v. United Kingdom*, no. 58243/00, § 62, 1 July 2008.
[38] §232.

B. Circumstances in which public authorities are empowered to resort to secret surveillance and metadata collection

38. The first question is whether the *material scope* of Articles 19 and 20c is defined clearly and whether it is foreseeable in which circumstances the police may put in place secret surveillance measures or obtain metadata.[39]

1. Substantive grounds for ordering surveillance under Article 19

a. Which crimes may justify secret surveillance? The proportionality principle in the context of secret surveillance

39. Article 19 of the Act establishes a *closed* list of offences which may be investigated by means of secret surveillance, which adds clarity to the material scope of application of this article. The catalogue of crimes, contained in Article 19 para. 1 is, however, quite broad. The Venice Commission recalls that the proportionality analysis under Article 8 of the Convention involves a substantive aspect; in other words, given its very intrusive character, secret surveillance of the *content* of private communications may be justified only in order to investigate *serious* crimes. Turning back to the Act, the Venice Commission doubts whether, for instance, telephone interception would be necessary to investigate some cases of illegal possession of psychotropic substances (see Article 19 para. 1 (5)), where it is evident from the outset that the case concerns very a small amount of such substances destined for personal use.[40]

40. Moreover, the Venice Commission reiterates that some of the surveillance measures provided by Article 19 para. 6 not only involve an interference with the secrecy of private communications but also an interference with the home (to the extent that the Act permits "bugging" of offices[41] or living premises). Such types of surveillance need particularly good justification and should be permissible only to investigate the *most dangerous* crimes. The Venice Commission recalls that in the case of *Iordachi and Others v. Moldova*, the ECtHR criticised the national law for allowing telephone interception in relation to more than a half of all the offences provided for in the Criminal Code.[42]

41. That being said the Venice Commission acknowledges that the Polish authorities have a large margin of appreciation in defining what crimes should be on that list, since this question relates to a large extent to setting priorities of the national penal policy.

42. What is more important, the law should explicitly incorporate the principle of *proportionality*. Indeed, some elements of the proportionality test are already contained in the Act – for

[39] The "foreseeability" requirement covers not only the material scope of application of the law, but also procedural guarantees. Thus, in *Weber and Savaria v. Germany*, no. 54934/00, 29 June 2006, § 95, the ECtHR formulated minimum safeguards "that should be set out in statute law to avoid abuses of power: the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed." At the universal level similar principles apply; thus, the UN report on the oversight of intelligence services (entitled "Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight", by Special Rapporteur Martin Scheinin, prepared at the request of the Human Rights Council), in para. 21 recommends that "national law outlines the types of collection measures available to intelligence services; the permissible objectives of intelligence collection; the categories of persons and activities which may be subject to intelligence collection; the threshold of suspicion required to justify the use of collection measures; the limitations on the duration for which collection measures may be used; and the procedures for authorizing, overseeing and reviewing the use of intelligence collection measures."

[40] At least, the Act does not contain any qualifier related to the purpose and scale of possession.

[41] See *Niemietz v. Germany*, 16 December 1992, §§27-33, Series A no. 251-B

[42] *Iordachi and Others v. Moldova*, no. 25198/02, §44, 10 February 2009

example, Article 19 defines surveillance measures as a subsidiary tool of investigation (see paragraph 46 below), and sets a closed catalogue of crimes where surveillance may be ordered. However, the proportionality cannot be reduced to that. In addition, all the actors involved – the police as well as the courts – should be required to assess, in each particular case, whether the seriousness of the crime (even from the catalogue contained in Article 19 para. 1) and the difficulty of the investigation necessitate any of the surveillance measures. While for some most serious crimes the answer may be self-evident, not all crimes from the catalogue would automatically require surveillance measures (especially those involving interference with the home), and that should clearly follow from the text of the Act.

b. The need for factual substantiation

43. The list contained in Article 19 para. 1 of the Act explains what types of crimes the police may investigate by means of secret surveillance. This is, however, a purely *formal* criterion which relates to the qualification given by the police to a factual situation which gives rise to an investigation. However, the police may assess the facts wrongly, or deliberately give to the facts of the case a legal characterisation which would bring it within the scope of Article 19 para. 1 – see, as an example, the situation described in the ECtHR case of *Lind v. Russia*.[43] Hence, in addition to verifying whether the crime referred to by the police is on the list set by Article 19 para. 1, the courts, while examining requests under Article 19 para. 2, should also assess the *factual evidence* which is already available, and decide on this basis whether secret surveillance would be justified.[44]

44. The ECtHR stressed in *Roman Zahkarov*, cited above, that the national court "must be capable of verifying the existence of a reasonable suspicion against the person concerned, in particular, whether there are factual indications for suspecting that person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures, such as, for example, acts endangering national security. It must also ascertain whether the requested interception meets the requirement of "necessity in a democratic society", as provided by Article 8 § 2 of the Convention, including whether it is proportionate to the legitimate aims pursued" (§ 206). Of course, the very purpose of secret surveillance is to obtain more evidence, when the existing evidence is not sufficient to open a criminal case. However, the law should be clear that in order to conduct surveillance the police and the prosecutor must have at least some *prima facie* evidence of a criminal activity, and that the court must examine such evidence before authorising surveillance.[45]

c. Probability that important information may be obtained through surveillance

45. Furthermore, the police should have sufficient reasons to believe that the surveillance of the targeted person or group could produce information which is important for further investigation. The "usefulness" of the information sought by the police is yet another manifestation of the more general principle of proportionality mentioned above. Again, it is not required that the police are certain about it; it suffices to demonstrate some *probability* that the surveillance is likely to lead to the disclosure of such information. However, any such assertion should be supported by reference to some factual circumstances and evidence.

[43] *Lind v. Russia*, no. 25664/05, 6 December 2007, §§ 77 and 78; it must be noted, however, that the case of Lind concerned authorisation of pre-trial detention and not surveillance.
[44] The requirement to examine factual evidence, to a certain extent, follows from Article 19 para. 1a, which stipulates that the police have to provide the court with "materials that justify the need for operational control".
[45] When speaking of "evidence" the Venice Commission does not mean that this should be the evidence obtained, recorded and tested according to the formal rules of criminal procedure.

d. Subsidiarity

46. The last criterion set by the Act is the *subsidiarity* requirement (see the last sentence of Article 19 para. 1): secret surveillance may be ordered only where "other means appeared ineffective or there is significant probability of the means being ineffective or useless". Again, this requirement is essential to make such measures proportionate: secret surveillance should be a measure of last resort.[46]

e. Evidentiary value of information

47. Finally, the Police Act is silent as to the evidentiary value of information, obtained by means of secret surveillance which turned out to have been ordered without sufficient justification. It is unclear whether materials obtained as a result of such surveillance (recordings, images etc.) may be used in criminal proceedings.[47] The ECHR does not, generally speaking, regulate admissibility of evidence. There is no requirement made in the ECHR of *unconditional* exclusion of all unlawfully obtained evidence.[48] Where there are adequate controls in law and practice against abuse of investigative powers by the police or security agencies, then a rigid rule on exclusion of unlawfully obtained evidence is less necessary. In the context of the Polish law it is clear that materials obtained without the prior authorisation by the court (or, in the case of an "urgent" procedure – without *ex post* authorization required under Article 19 para. 3) should not be introduced in criminal proceedings.

48. However, it is open to doubt to what extent such materials may be used where such authorisation has been obtained, but on insufficient grounds. The Venice Commission recalls that the authorisation procedure, in most cases, will take place behind the closed doors and neither the public nor the person concerned will know whether the court in that procedure had seriously considered the privacy interest involved. In such condition, the court examining the merits of the case where the materials obtained through secret surveillance are presented by the prosecution in evidence should have discretion to exclude them, if they have been obtained with gross and flagrant disregard of the law, in order to combat abusive surveillance.

2. Substantive grounds for metadata collection under Article 20c of the Police Act

a. Which crimes may justify metadata collection?

49. The police enjoy a much wider discretion when collecting metadata; it is permitted "in order to prevent or detect crimes or in order to save human life and health, or in order to support rescue and find missions" (Article 20c para. 1 Police Act). The question is whether this formula satisfies the requirement of "foreseeability" of the law enshrined in Article 8 of the ECHR.[49]

50. The first point to make here is that "prevention" involves making a different, forward-looking, type of assessment as compared to past, or on-going offences. Admittedly, the dividing

[46] The Venice Commission observes that a similar three-steps test is set in e.g. the Danish legislation; surveillance measures in Denmark may be ordered where (1) there are specific grounds for suspicion that information is being transferred from/to the subject of the surveillance; (2) the coercive measure is strictly required for the investigation; (3) the investigation is conducted in relation to a crime punishable with a minimum of six years of imprisonment, or for the prevention and investigation of certain specifically enumerated crimes, e.g. terrorism (see the 2015 guidebook prepared by the European Union Agency for Fundamental Rights (FRA) on "Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU Mapping Member States' legal frameworks", para. 20).

[47] As direct evidence, or whether it is possible to introduce other evidence obtained *as a result* of such irregular surveillance.

[48] With few exceptions which concern evidence obtained under torture, etc. – see, for example, *Harutyunyan v. Armenia*, no. 36549/03, §§59 et seq., ECHR 2007-III

[49] The Venice Commission considers that the reference to the "rescue and find missions" is sufficiently precise to outline situations where the police may collect metadata.

line is not hard and fast, especially in relation to inchoate offences generally, and terrorism and organised crime specifically. Nonetheless, the greater uncertainty involved in making an assessment of future events increases the scope for abuse, or overuse, of this investigative method.

51. The Venice Commission recalls that in *Szabó and Vissy v. Hungary*,[50] the ECtHR stressed that "the requirement of 'foreseeability' of the law does not go so far as to compel States to enact legal provisions listing in detail all situations that may prompt a decision to launch secret surveillance operations. The reference to terrorist threats or rescue operations can be seen in principle as giving citizens the requisite indication […]". The Court further contrasted the situation in Hungary with the situation in Moldova, examined earlier in the case of *Iordachi and Others*, cited above. In the latter case the national law had been criticised by the Court because it allowed wiretapping in a very large spectrum of criminal investigations. The question is whether the same logic applies in respect of the metadata collection.

52. In *Uzun*, cited above, which concerned GPS-tracking of a car used by a supposed terrorist, the ECtHR defined, first of all, whether the law allowing for such measures was "foreseeable". While the Court, in its own words, is not barred from *gaining inspiration* from the principles developed in the sphere of "classical" surveillance of telecommunications, these principles are not applicable directly to cases concerning surveillance by GPS-tracking, because such measure must be considered to interfere less with the private life of the person concerned than the interception of his or her telephone conversation (§ 66).

53. That being said, in the *Uzun* case the ECtHR didn't find a violation of Article 8 of the ECHR in particular because the GPS-tracking could have been ordered in respect of "a person suspected of a criminal offence of considerable gravity" (§ 70). In other words, the German law narrowed down the possibility of using such technique to the most serious cases. This element is absent from Article 20c of the Police Act: it allows metadata collection in all, even the most trivial, investigations. Furthermore, it is reasonable to assume that the metadata collection under Article 20c of the Act may, on occasions, lead to a more serious interference with the privacy, compared to a relatively short-term GPS-tracking of movements of a car – for example, where content-related metadata is analysed (such as the web-logs, for example).[51]

54. In its 2015 report on the Democratic Oversight of Signals Intelligence Agencies (hereinafter "the 2015 Report")[52] the Venice Commission formulated its approach as follows: "how broadly or narrowly drafted the agency's mandate is, is a crucial part of limiting the scope for abuse". It is doubtful that the broad formula used in Article 20c (namely that metadata collection may be used by the police "in order to prevent or detect crimes") satisfies the "foreseeability" requirement of Article 8 of the ECHR. One means of limiting the scope of abuse of this investigative method is to provide that metadata collection may only be used to investigate offences punishable by a certain minimum penalty. This can be supplemented by a shorter list of offences which may not attract this minimum penalty, but where metadata collection is, or is part of, the primary evidence for prosecution, e.g. certain cyber-crimes. So, better methods exist to avoid the risks caused by the broad formula used by the Act. The Venice Commission invites the Polish legislator to reflect on how to narrow down the rule currently contained in Article 20c of the Act.[53]

[50] No. 37138/14, §64, 12 January 2016 (not yet final)
[51] GPS surveillance lasted for some three months, whereas the Act does not contain any limitation in time on the collection of metadata under Article 20c.
[52] CDL-AD(2015)011, § 70
[53] The Venice Commission understands that the powers of other State agencies to collect metadata under the Act are linked to their respective remit.

b. Probability that important information may be obtained through metadata collection

55. The next question is the *level of probability* which needs to be demonstrated, with reference to the relevant facts, in order to start metadata collection. This is a difficult question, partly because metadata collection, contrary to classical surveillance, often is not "targeted" (see below the discussion about the "untargeted" information gathering). Hence, it is not always possible to link metadata collection to a specific person who is suspected of a particular crime, or a group of such persons.

56. That being said, Article 20c contains no probability test the police have to meet in order to start collecting metadata. In the opinion of the Venice Commission it is crucial that the police should have *specific reasons to believe* that:

- a crime has been committed or a criminal activity is going on or being prepared, and that
- monitoring is likely to contribute to finding more about it.

In other words, the police should be able to explain, with reference to the facts, in which way collection of metadata would promote investigation into a particular criminal activity.[54]

c. Subsidiarity

57. The Venice Commission observes that, unlike the secret surveillance under Article 19 of the Act, metadata collection, according to the Polish law, is not supposed to be a subsidiary means of obtaining information.

58. Metadata collection is, indeed, very useful for "contact-chaining", i.e. identifying a suspect's network of contacts, and as such often comes into play at a relatively early stage of investigations. However, the general principle of proportionality applies to metadata collection as well, as with all other coercive measures, and a balance must always be drawn between effectiveness and intrusion into privacy. The fact that the legislation does not require that other methods have first been tried and failed, or would be fruitless, is a factor which operates to strengthen the need for other safeguards to avoid overuse by law enforcement and security agencies. The procedural safeguards which may prevent abusive metadata collection will be discussed in paragraphs 109 et seq. below.

59. In addition, the law should contain a substantive rule which gives to the police an indication as to when to make recourse to this method. As has already been mentioned in paragraph 58 above, even when collecting the least "sensitive" kind of metadata, the police should do it only if it is justified in the circumstances. The essential question is what standard of review the courts should apply when defining whether the police acted lawfully and remained within its discretion. This standard should be stricter when it comes to the content-related secret surveillance: the police will have to demonstrate convincingly the "impossibility" of obtaining information by other means, and prove the essential value of the information it seeks to obtain. By contrast, when it comes to the metadata collection, the court may be satisfied by the fact that this method of obtaining information is the easiest one in the circumstances, and that it is *reasonably related* to the goals of a specific investigative activity. It belongs to the Polish legislator to formulate the rule which would show the distinction between the proportionality tests applied in the context of the secret surveillance and the metadata collection.

[54] To a certain extent the question of the "level of probability" refers to the same criteria, which has been earlier used for analysing the "classical" surveillance: need for some factual substantiation, a minimal probability that important information may be so obtained, etc.

d. The notion of "metadata" under Article 20c

60. The remaining question is what sort of information may be collected under Article 20c. The Act itself does not describe precisely what "metadata" is. Instead, it refers to several other acts which regulate telecommunications, internet and postal services (see CDL-REF(2016)036). It is up to the specialists in the relevant fields to assess whether the technical terms used in those other acts describe "metadata" with sufficient precision. However, certain elements attract attention even of non-specialists.

61. At the outset, the Venice Commission observes that under the Act metadata "does not constitute a telecommunications message" (Article 20c para. 1 of the Police Act). The Venice Commission understands that the metadata, in the logic of the Police Act, may not reveal the content of the communication *stricto sensu*. However, at the meetings in Warsaw the rapporteurs received conflicting answers as to whether metadata, under the Polish law, also includes "content-related" information: web-logs, Internet cookies, content of research requests, headings of e-mails, etc. In the opinion of the Venice Commission, either the Act should associate that kind of metadata with the "content" of communications, access to which is regulated by Article 19, or exclude it from the notion of metadata in explicit terms.[55] It is important to make this distinction in order to decide whether more or less stringent procedural guarantees and substantive rules apply to the content-related metadata.

62. Second, pursuant to Article 180c para. 2 of the Telecommunications Act, it belongs to the competent ministers, including the Minister of Interior, to specify, by means of an ordinance, a detailed list of data which is mentioned in Article 180c para. 1 and which may be collected by the police pursuant to Article 20c. It is very important to make sure that the power to issue ordinances in this sphere does not result in an uncontrolled expansion of the notion of "metadata". The Venice Commission recalls its position expressed in the 2015 Report that "case-law, even where it lays down detailed standards and comes from the Supreme, or Constitutional Court, is in itself not sufficient to regulate the area [of secret surveillance] and nor is subordinate legislation".[56]

63. Third, Article 20c also refers to Article 180d of the Telecommunications Act, which, in turn, refers to Article 161.1 thereof. The latter stipulates that "the provider of publicly available ICT[57] services may, with the consent of a user who is a natural person, process *other data* [emphasis added] of such user in connection with the service rendered". This formula seems to imply that the metadata may include any information which a user of a popular ICT service agrees to share with the provider. However, it is well-known that few users really read the "small print privacy agreements" which define the information they "voluntarily" share with the ICT providers in order to get access to their services. Thus, this provision, when read in conjunction with Article 20c of the Act, may lead to a virtually uncontrolled expansion of the notion of "metadata" which may be collected by the ICT providers and ultimately by the government. Nor is this approach compatible with the idea behind "informational self-determination" which forms a part of the concept of privacy, i.e. that the individual himself or herself determines to what extent he or she shares personal information with different actors.

---

[55] According to a briefing paper of 29 April 2016 given to the rapporteurs at the meeting in the Chancellery of the Committee of Ministers, para. 5, metadata does not include "logins and passwords, as well as addresses of the web-sites visited". However, other interlocutors the rapporteurs met in Warsaw had different views on this point. Furthermore, the information received from the Ministry of Interior of Poland suggested that the police may collect such information as a part of the "metadata monitoring"; thus, statistical information on metadata collection included such positions as, for example, "www addresses" and "chats", which are clearly content-related.

[56] See CDL-AD(2015)011, § 93. That being said, it is not excluded that subordinate legislation may regulate some highly technical or very secret elements of the metadata collection.

[57] ICT refers to "information and communications technologies"; it is an umbrella term that includes any communication device or application, encompassing: radio, television, cellular phones, computer and network hardware and software, satellite systems and so on, as well as the various services and applications associated with them, such as videoconferencing and distance learning.

64. The Venice Commission recognises that the quick development of modern technologies calls for some flexibility in regulating metadata collection. However, State agencies should not be allowed to expand the notion of "metadata" beyond its original meaning and include there completely new types of information. If there is a need to regulate access to new types of information and introduce new forms of surveillance, only the legislator should have the power to define which data may be collected, on which grounds and in which procedure.

65. In sum, the Venice Commission recommends that the Polish legislator reviews, if necessary with the help of ICT professionals and the lawyers working in the relevant field, whether the description of metadata in the relevant legislation sufficiently defines categories of information which may be collected pursuant to Article 20c. Special attention should be paid to the definition of "content-related" data. In doing so the Venice Commission recommends avoiding open-ended formulas, which refer to the regulations adopted by the executive or to the data policies of the ICT companies.

C. Who may be subjected to surveillance and metadata collection?

1. Large groups of people

66. "Classical" covert surveillance allows for obtaining information about a specific person, group or organisation. However, modern surveillance measures, and especially metadata collection sometimes start without a specific target. The targeted person is only defined *after* the collection and filtration of data so obtained.

67. Thus, for example, by "emptying" a mobile relay station one can discover the mobile phones in the area during a particular time period, helping the police identify whether e.g. mobiles belonging to known members of organized crime were present in the area when a bank robbery occurred. At the same time this technique may help identifying who was in the area when a large demonstration was going on against the government. It is easy to see how this can "chill" freedom of association or assembly protected by Article 11 of the Convention. "Herein lay both the value [such monitoring] can have for security operations, and the risk it can pose for individual rights".[58] And even where such non-individualised monitoring is used for legitimate purposes (for example, to prevent a terrorist attack, or for a search and rescue mission), and is cheaper than other methods, the main problem with this type of surveillance is that it inevitably affects a large number of innocent/unconcerned people.

68. The first question is whether the Act permits broadly targeted surveillance. Article 19 para. 7 of the Act requires that the police should indicate "data of a person or other data facilitating unambiguous determination of the entity or object" of surveillance. It is unclear to what extent the reference to the "object" of surveillance may relate to a large group of people (for example, residents of a neighbourhood, or a group of protesters or worshippers at church). However, the reference to "unambiguous determination", if narrowly interpreted, ensures that surveillance under Article 19 cannot be ordered without at least some individualisation,[59] even if it targets a group of people. So, "classical" surveillance by the police in Poland should always be targeted.

69. By contrast, as to the collection of metadata under Article 20c, nothing in the Act seems to prevent the police from collecting such information without having a specific target. The Venice Commission recalls in this respect that the Parliamentary Assembly of the Council of Europe

[58] 2015 Report, CDL-AD(2015)011, §3

[59] When speaking of "individualisation", the Venice Commission does not imply that the police must always know exactly the identity of the person under surveillance; sometimes a surveillance order may concern an anonymous user of a certain suspicious telephone number or a certain computer etc.

(PACE) in its Resolution 2045 (2015)[60] urged the Council of Europe member States, *inter alia*, to ensure that their national laws only allow for the collection and analysis of personal data (including metadata) "following a court order granted on the basis of reasonable suspicion of the target being involved in criminal activity".

70. The Venice Commission is reluctant to be so categorical. The Assembly seems to question the very idea of strategic surveillance, because it is not based on a "targeted" court order. The ECtHR in its case-law, by contrast, seems to accept broadly targeted collection of information.[61] In the opinion of the Venice Commission, broadly targeted surveillance without a court order may be accepted if the law contains sufficient safeguards against indiscriminate capturing of vast amounts of communications. To reduce that risk the law should describe situations where broadly targeted monitoring is permitted, and define categories of persons liable to have their communications monitored. The threshold requirement for permitting such monitoring should be set high – for example, it may be linked to investigation of specific serious crimes *which have occurred in the past*. Exceptionally, it might be possible to allow this to concrete future dangers, such as terrorist threats.[62]

71. Where it is allowed, oversight must be particularly strong. There should be an efficient system of oversight of such measures, implemented by an independent body (or bodies) external to the police.[63] That body should have access to the materials justifying such monitoring, and to the results of such monitoring. Its task should be to ensure, in particular, that such broadly targeted monitoring is reasonably connected to the needs of the specific investigations, that it is not based on discriminatory grounds (i.e. that it does not target categories of population which are "usual suspects" for certain categories of crimes), that it is never used for purposes not related to the mandate of the police or another respective law-enforcement body, and that strict destruction requirements are applied to all material not necessary for the specific investigation involved.

2. Non-suspected "bystanders"

72. The Act is not entirely clear as to who may be subjected to "classical" secret surveillance or to metadata collection. It appears that those measures may target any person or any group (including friends, family members etc. of the primary targeted person), provided that these measures are likely to disclose information which may eventually contribute to achieving the goals of the surveillance or of metadata collection set in Articles 19 para. 1 and in Article 20c para. 1 respectively.

73. In the opinion of the Venice Commission, the principle of foreseeability requires that the Act should define *the extent of connection* of people/groups in question to the criminal activity under investigation. Obviously this includes people suspected of the specified offences. In addition, the Act may also specify that other persons in contact with such people may, under certain circumstances, be subjected to surveillance.[64] With regards to the standards set in Article 8 § 2 of the ECHR, it is very important to describe in the Act the circumstances in which persons not involved directly in the criminal activity (at least on an arguable basis) may be targeted. For

[60] "Mass surveillance"; adopted on 21 April 2015, para. 19.1

[61] See, for example, the case of *Weber and Saravia v. Germany*, cited above, where the ECtHR analysed "strategic intelligence" system employed in Germany (i.e. non-targeted interception of communications and their analysis with the use of the system of "key words") and found it compatible with Article 8 of the ECHR.

[62] In *Weber and Saravia*, §§ 96 and 97, cited above, the ECtHR stressed that in the German system the law "enumerated […] the exact offences for the prevention of which the strategic interception of telecommunications could be ordered. The amended [Act] therefore defined in a clear and precise manner the offences which could give rise to an interception order." Furthermore, the law "indicated which categories of persons were liable to have their telephone tapped" and "the persons concerned either had to have used catchwords capable of triggering an investigation into the dangers" listed in the law or "had be foreign nationals or companies".

[63] See *Roman Zakharov*, cited above, §275

[64] See the 2015 Report, § 98

example, the Act might allow such measures only in respect of certain particularly grave crimes (such as terrorism, large-scale drug-trafficking, proliferation of weapons of mass destruction, etc.), and put in place strengthened justification requirements (a higher threshold of probability that such surveillance may help obtaining crucial information) and procedural safeguards (such as the involvement of a privacy advocate).[65]

74. During the visit to Warsaw the rapporteurs have been informed that in April 2016 the Criminal Procedure Code has been amended, and paras. 15a-15e of Article 19 of the Police Act have been repealed. Those amendments seem to give to the prosecutor a discretion to decide whether the information about non-targeted third persons obtained "by accident" in the course of the surveillance should be introduced in the criminal proceedings against them as evidence. The Venice Commission considers that the use of incriminating information about non-targeted third persons so obtained may only be permissible in exceptional circumstances, and should be decided by a court. It is doubtful whether such materials should be allowed as evidence in prosecutions concerning relatively insignificant crimes. The Venice Commission also considers that the law must specify clearly when such materials cannot be used in evidence - for example, when conversations accidentally captured on tapes concern privileged communications.

3. Lawyers, priests, and other persons covered by professional privilege

75. Article 19 of the Police Act defines what to do with the information covered by the professional privilege. The competent officials of the police are required to:

- destroy this information if it is protected by the *absolute* privilege enjoyed by defence lawyers and priests (see Article 19 para. 15f (1) of the Act, read in conjunction with Article 178 of the Polish Code of Criminal Procedure),[66] or
- pass this information to the prosecutor and ultimately to the court, which should decide what to do with it, if this information is covered by a *weaker* professional privilege which covers notaries, advocates and legal advisors (who do not act as defence lawyers), tax advisors, doctors, mediators or journalists (see Article 19 paras. 15f (2) and 15g-j of the Act, read in conjunction with Article 178a and Articles 180(2) and 180(3) of the Polish Code of Criminal Procedure).

76. At the outset, the Venice Commission notes that the lawyer-client confidentiality is protected not only by virtue of Article 8 of the Convention (as any other private communication), but also, implicitly, under Article 6 § 3 (c) thereof. The seal of confession, is, in turn, protected by Article 9 of the Convention. It is possible to say that those two types of communications have a particular status even within Article 8 of the Convention; at least, in respect of the secrecy of the lawyer-client communications the ECtHR expressed a view that they require special measures of protection, since "where a lawyer is involved, an encroachment on professional secrecy may have repercussions on the proper administration of justice and hence on the rights guaranteed by Article 6 of the Convention".[67]

77. The Venice Commission detects two major flaws in the provisions regulating surveillance of privileged communications. The first relates to the *lawyer-client privilege*. While the Act defines what to do with the information *already obtained* through the secret surveillance and covered by

[65] The above said is not relevant for broadly targeted monitoring, which necessarily concerns a large majority of purely innocent people which have nothing to do with the subject-matter of the investigation. As it was stressed above (see paragraphs 66 et seq.), broadly targeted monitoring may be allowed provided that an efficient oversight mechanism is in place.

[66] Article 178 provides that it is not permitted to examine as witnesses (1) a defence counsel or advocate acting pursuant to Article 245 § 1 with regard to facts learned while giving legal advice or conducting a case; (2) a clergyman with regard to facts learned during confession.

[67] *Smirnov v. Russia*, no. 71362/01, § 48, 7 June 2007, with further references.

such privilege, it does not appear to prohibit the surveillance of lawyers' communications as such. Nothing prevents the police from secretly listening to the conversations between a defence lawyer and his or her client. In the opinion of the Venice Commission, this is inadmissible, for the reasons set out below.

78. The fact that the information obtained in breach of a professional privilege may not be used as *evidence* in criminal proceedings against the suspect and should be destroyed pursuant to Article 15f is not sufficient. By listening to the conversations between the lawyer and his/her client the police may obtain important information which may lead to the discovery of other inculpatory evidence, which may, in turn, be introduced in criminal proceedings. And even if in the Polish criminal procedure evidence which is the "fruit of the poisonous tree"[68] is inadmissible, listening to the conversations between the lawyer and the client gives the police a tactical advantage and undermines the trust which must exist between the defence lawyer and the accused.

79. In the opinion of the Venice Commission, the Act should distinguish between *deliberate* and *accidental* interference with the lawyer-client privilege. The first should be, as a general rule, prohibited. There are certain evident situations where the police should *presume* that a conversation is covered by the privilege – for example, it concerns conversations of a lawyer with his/her client in the prison or in the courtroom, consultations by telephone, etc. Such communications should be, as a rule, exempt from any eavesdropping.[69] In the Netherlands, for example, law firms can provide the Ministry of Interior with their "privileged phone numbers", and these numbers will then automatically be filtered out from any kind of surveillance operations.

80. This presumption is not absolute. The ECtHR case-law indicates that the Convention does not require member-States to abstain totally from engaging in surveillance of "privileged communications".[70] However, the presumption may only be departed from in exceptional cases – for example, where there is *strong evidence* of the personal and conscious involvement of the lawyer in a *particularly grave crime*, which cannot be investigated further by *any other means* than by listening to his/her conversations with a client. Any such derogation should be, in addition, accompanied by strengthened procedural safeguards (like entrusting the power to monitor communications to an independent judge unconnected with the investigation, who is under a duty to keep the information thus obtained confidential if it is irrelevant).[71]

81. The second issue relates to the interception of communications of *other professionals* who also have the duty of confidentiality vis-à-vis their clients (such as doctors and mediators). The Venice Commission observes that, as in the case with lawyers and priests, nothing in the Polish law prevents the police from listening to such conversations, even if later the recordings cannot be introduced in evidence. Furthermore, under Article 19 para. 15h the court must allow recordings of such conversations as evidence "if it is necessary from the viewpoint of the justice system" and if no other means of establishing the facts of the case were available.

82. The second part of this test (subsidiarity) is sound; however, the first part – the "necessity" for the justice – is problematic. Any useful information shedding light on the circumstances of a case may be seen as "necessary from the viewpoint of the justice system". However, if the

[68] The theory of the "fruit of the poisonous tree" proclaims that evidence, obtained as a result of information which had been obtained in breach of law, should also be declared inadmissible. For a detailed analysis of this theory see the ECtHR case *Gäfgen v. Germany* [GC], no. 22978/05, ECHR 2010.

[69] The Venice Commission observes in this respect that Article 15 para. 1 (4a) of the Act allows the police to record conversations in "the rooms for arrested persons"; such interception is seemingly exempted from the general regime provided by Article 19 para.1. Moreover, Article 19 para. 6 (2) permits the police to "obtain and record image or sound of persons from rooms" which may be interpreted as permitting eavesdropping in the meeting rooms.

[70] *Erdem v. Germany*, no. 38321/97, § 65

[71] *Erdem*, cited above, § 67

usefulness of a wiretapped conversation is the only criteria for introducing it as evidence, "professional privilege" becomes an empty word.

83. This is particularly important where the surveillance targets a journalist, since it may easily reveal his or her sources. The Venice Commission recalls that protection of journalistic sources is one of the basic conditions for press freedom. As transpires from the case of *Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands*,[72] the ECtHR is ready to subject disclosure orders which may lead to the identification of the journalistic sources to the strictest scrutiny. Thus, there should be some form of heightened internal decision-making standard in such cases, where the journalistic freedom may be at issue. The Venice Commission, in its 2015 Report, cited above, stressed that "methods must be devised to provide lawyers and other privileged communicants and journalists with some form of protection, such as requiring a high, or very high, threshold before approving signals intelligence operations against them, combined with procedural safeguards and strict external oversight" (§18).

84. The Venice Commission considers that, in addition to preventing targeted interception of protected communications, the law should contain safeguards which give extra protection to such communications even when they have been *accidentally* intercepted. In *Weber and Saravia*, cited above, the journalist complained that her communications with the sources of information could be revealed as a result of the "strategic monitoring" conducted by the Federal Intelligence Service. In that case the ECtHR decided that the safeguards in place in Germany were adequate and effective for keeping the disclosure of journalistic sources to an unavoidable minimum, and thus satisfied the requirements of Article 8 of the ECHR (§151).

85. In sum, the Venice Commission recommends that the Polish legislator reflects on a more stringent rule which would, while respecting international human rights standards, describe the circumstances in which privileged professional communications could be secretly recorded and then introduced as evidence.

86. Any substantive rule concerning accessing professional communications of lawyers would remain dead letter if not supported by a proper system of oversight. In Chapter D (see, in particular, paragraphs 98 et seq. and 11 et seq. below) the Venice Commission will discuss various procedural mechanisms of oversight of the police and other services and verification of the lawfulness of the specific surveillance operations. In particular, the national legislator may put in place a mechanism which would allow preserving materials protected by the professional secrecy from the police' knowledge - see, as a possible solution, the Dutch system described in *Mulders v. the Netherlands*, or the rules regulating seizures of the lawyers' documents analysed in *Tamosius v. the United Kingdom* (dec.); cf. to *Wieser and Bicos Beteiligungen GmbH v. Austria*.

D. Procedural safeguards

1. Duration of the surveillance measures and metadata collection

87. According to the Act, secret surveillance shall be ordered for a period not exceeding 3 months (Article 19 para. 8); a prolongation is permitted by a court's decision for further 3 months; finally, in justified cases surveillance may be prolonged by a higher court for several consecutive 3-months' periods, not exceeding *in toto* 12 months (Article 19 para. 9). It appears that the overall duration of surveillance measures may not exceed 18 months.[73]

[72] No. 39315/06, § 127, 22 November 2012

[73] This reading of Article 19 paras. 8 and 9 is confirmed by an outline of the Act prepared on 29 April 2016 by the Chancellery of the Committee of Ministers of Poland, page 4.

88. The Venice Commission observes that the maximum length of the surveillance set by the Act is quite long by itself. However, the most important issue relates to the possibility of an indeterminate duration of metadata collection (see Article 20ca). The Act does not explain how much historic data the police may retrieve from the ITC service providers, although the 12 month retention period will usually set a limit in practice on this. Nor does the Act specify for how long the police may monitor live metadata flows. In the light of the proportionality principle, this should be specified in the law. That being said, the Venice Commission understands that periods of retention of historic data and periods of continuous retrieval of on-going (live) exchange of metadata (in particular in the form of strategic surveillance) may be relatively long.

2. Judicial control *ex ante* and *ex post*, complaints mechanisms and oversight by an independent body

89. The Venice Commission acknowledges that the Act cannot avoid some catch-all formulations when outlining situations where surveillance is necessary. A law which is somewhat imprecise may nonetheless be corrected by a procedural safeguard (which compensates for the risk of abuse caused by the imprecision). For this reason it is important to ensure that the body which would apply the rule is professional, independent and has all necessary legal tools to fulfil its controlling functions.

90. As the Venice Commission noted in the 2015 Report (§ 105), "it is apparent that the two most significant safeguards are the authorisation process (of collection and of access to the collected data) and the follow-up (oversight) process. That the latter must be performed by an independent, external body is apparent from the [ECtHR] case-law. The question which arises here is whether even the authorisation process should be independent."

a. Authorisation and oversight of the surveillance operations under Article 19

I. Authorisation

91. Under Article 19, secret surveillance is to be performed with the prior consent of a district court. As an exception, in cases of utmost urgency, police may perform surveillance without such prior consent; however, if consent is not granted within 5 days, surveillance must be suspended and the material gained from it must be destroyed (see para. 3).

92. Even though for the ECtHR the judicial authorisation for surveillance is not *conditio sine qua non*,[74] the Court sees it as an important procedural guarantee.[75] Thus, Article 19 para. 1 of the Act which establishes such mechanism is welcomed. In addition, it would be desirable to extend judicial pre-authorisation to the collection of content-derived metadata which is, as noted above (see paragraph 26 above), by its nature, very close to the interception of communications regulated by Article 19.

93. The "urgency" exception, contained in para. 3 of Article 19, is known to other jurisdictions as well. In Latvia, for instance, when there is a need to act without delay to prevent a threat to vital public interests, such as an act of terrorism or subversive activity, a murder or other serious crime, or if there is an actual threat to the life, health, or property of a person, surveillance can be initiated without the judge's approval. In its stead, a prosecutor must be

[74] *Kennedy v. the United Kingdom*, no. 26839/05, 18 May 2010

[75] See the case of *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, no. 62540/00, §§81 and 84, 28 June 2007, where the Court approved the system of judicial authorisation of the secret surveillance measures. See also the judgment in the case of *Klass v. Germany*, 6 September 1978, § 55, Series A no. 28, where the ECtHR stated that "the rule of law implies, *inter alia* that an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary, at least in the last resort, judicial control offering the best guarantees of independence, impartiality and a proper procedure".

notified within 24 hours and the judge's approval must be received within 72 hours.[76] That being said, the Venice Commission notes that in Poland the "urgency exception" is not conditioned upon the *gravity* or *type* of the crime under investigation, but only by the risk of the loss of evidence. Furthermore, it is unclear what happens if the "urgent" interception is discontinued by the police before the 5-days' period; this provision, if broadly interpreted, may allow the police to make relatively short interceptions free from any judicial control. That should be reconsidered.[77]

94. Judicial authorisation of surveillance constitutes an important safeguard against abuses; however, there are two factors which may undermine the efficiency of this legal mechanism. The first consists of the risk of overburdening of judges with such requests. Judicial control over surveillance operations should be seen as a part of the essential work of a judge, and should be counted in the judicial statistics. Furthermore, the judge should have adequate assistance by staff members who have adequate insight into the technology and practice of surveillance operations. Otherwise the judge would tend to minimise the effort and limit him/herself to a purely formal review.[78]

95. The second factor is the lack of adversarial proceedings. As follows from the Act, the courts examine the requests of the police *ex parte*, without the participation of the person targeted by the surveillance. As such this is understandable: "the very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be effected without the individual's knowledge".[79] However, in the absence of a real adversarial debate, judges tend to be less critical to the position of the police. Moreover, if the judge turns down the request, there is a risk of appeal, which is absent when the judge accepts a request by the police and orders the surveillance. In such circumstances the prior judicial authorisation of the surveillance measures may become a simple formality.

96. The participation of a prosecutor in the process of authorisation of surveillance, provided by the Act, is welcome, but in view of the close relations between the prosecution service and the police in the Polish system, involvement of the prosecutor cannot be considered as a sufficient procedural safeguard.[80]

97. To increase the effectiveness of the preliminary judicial control, the *ex parte* judicial review could be supplemented by introducing in the authorisation proceedings a figure of a "privacy advocate" – an independent legal professional, having necessary technical skills and the security clearance, who is not institutionally related to the police and the prosecutor's office.[81]

---

[76] See the FRA guidebook, para. 54

[77] See *Roman Zakharov*, cited above, "The domestic law does not limit the use of the urgency procedure to cases involving an immediate serious danger to national, military, economic or ecological security. It leaves the authorities an unlimited degree of discretion in determining in which situations it is justified to use the non-judicial urgent procedure, thereby creating possibilities for abusive recourse to it (see, by contrast, *Association for European Integration and Human Rights and Ekimdzhiev* […] § 16)".

[78] At the meeting with NGOs the rapporteurs were informed that the adoption of the amendments was not accompanied by the change in the courts' duties or allocation of additional resources enabling the judges to supervise properly. District courts have already a heavy workload, and may be tempted to do only the most superficial review of the requests for the surveillance measures.

[79] *Roman Zakharov v. Russia*, no. 47143/06, § 233. See also *Klass and Others v. Germany*, cited above, §§ 55 and 56

[80] Thus, in *Dumitru Popescu v. Romania (no. 2)*, no. 71525/01, 26 April 2007, § 78, the Court considered that the Romanian authority which ordered the surveillance – namely the prosecutor – was not independent from the executive. The rapporteurs were informed that a special prosecutor's office has been recently created to follow more closely the investigative activities of the security and intelligence services. This is also to be welcomed, but for the same reasons cannot be seen as a sufficient procedural safeguard.

[81] See a description of the position of such advocate in the UK, in the CDL-AD(2007)016, Report on the Democratic oversight of the Security Services, §§215-216

The function of such "advocate" would be to defend the interests of the person under surveillance in his/her stead.[82]

II. *Ex post* oversight

98. There are several other ways of remedying the limitations of the authorisation procedure. Occasionally, material obtained as a result of surveillance would be used as evidence in the criminal proceedings. In this case the accused may, at least in theory, contest the lawfulness of the surveillance in the proceedings on the merits of his/her case.[83] Several questions remain, however.

99. First, if such review is possible, the only consequence for the accused would be the disqualification of the evidence obtained as a result of the surveillance. In other words, such review would not be appropriate if the accused, for example, seeks compensation for the allegedly unlawful interference with his or her privacy. In addition, such remedy would be accessible only to the accused, but not to a third person whose privacy has been violated by the unlawful interception – simply because such person would not have the standing necessary to claim the exclusion of the evidence.

100. Second, it is unclear whether the court reviewing a surveillance warrant in the proceedings on the merits would have full jurisdiction in this matter and whether the accused would have full access to the materials which justified the warrant. As the rapporteurs understood, materials of the "operational control" are, as a general rule, treated as secret in Poland.[84] Hence, there is a risk that the court reviewing the surveillance warrant in the proceedings on the merits would refuse to disclose to the defence the materials relevant to the authorisation of the wiretapping. Exclusion of such materials from the adversarial examination may put the defence into a significant disadvantage vis-à-vis the prosecution and be contrary to the principle of fair trial.[85]

101. Finally, and most importantly, this remedy would be available only in a fraction of all cases, only where the fact of the surveillance has become known in the criminal proceedings. In the vast majority of situations, the surveillance would remain "secret".

102. For such cases the Act might provide for a system of *posterior complaints* by the persons targeted by the surveillance measure. To realise this right the person has to be aware of the

[82] Participation of such "privacy advocate" may take different forms. In Austria, for example, a Legal Protection Commissioner (Rechtsschutzbeauftragter, RSB) was established to afford citizens another level of protection in the context of secret investigations carried out without their knowledge. The RSB needs to approve covert investigations (verdeckte Ermittlung), or covert audio and video recording, in the context of the observation of groups thought to present a serious danger to public security through acts of religiously or ideologically motivated violence. The Federal Minister of the Interior seeks the RSB's pinion
during operative and strategic analyses of personal data. This type of analysis is performed in the defence against criminal organisations or to prevent dangers emanating from the preparation or commission of criminal offences. The RSB has to provide an opinion on each surveillance measure. Once the opinion has been provided, the analysis can be conducted (see FRA guidebook, para. 53).

[83] It is unclear whether the court examining the case on the merits will be able to review and annul a decision of another court which authorised a surveillance measure. The rapporteurs were informed that the recent changes to the Criminal Procedure Code, which are not the subject-matter of the present opinion, seriously curtailed the power of the court to disqualify unlawfully obtained evidence.

[84] To a certain extent it is confirmed by Article 19 para. 16 which stipulates that "the person subject to operational control shall not be provided with materials collected during the control". Furthermore, Article 20b of the Act stipulates that "disclosure of information about detailed form, principles and organisation of preliminary investigation, activities being carried out, as well as applied measures and methods of their implementation shall be allowed only in the case of justified suspicion that a crime prosecuted on indictment has been committed in relation to performance of these activities". In other words, in trivial cases of unjustified requests for surveillance, which do not amount to a criminal behaviour, materials justifying the surveillance may be seen as confidential, since they may arguably contain elements related to the "organisation of preliminary investigation" etc.

[85] See *Mirilashvili v. Russia*, no. 6293/04, § 200 et seq., 11 December 2008; *Roman Zakharov*, § 261

surveillance. In the context of "classical" surveillance, a standard requirement in many countries is that the target is *notified* – of course, when the surveillance has ceased – about the fact of the surveillance and the reasons thereof (if this can be done without imperilling investigation methods or sources).[86] In this respect the Venice Commission notes that, as it seems, the Act does not contain any requirement to notify the target, even after a lapse of time.

103. The Venice Commission acknowledges that the notification may jeopardise confidential methods or on-going operations. Therefore, notification of the target is not an absolute rule and in certain cases the authorities may legitimately deviate from it. Nevertheless, it is important to set in the Act a general obligation of the relevant authorities to notify the target *ex post*, and formulate exceptions from this rule. When the person learns about the surveillance, *ex parte* proceedings before the court issuing the surveillance warrant may be supplemented by fully adversarial proceedings in which the court would examine the lawfulness of the surveillance *de novo*.[87] An alternative is to create a standing non-judicial mechanism to which persons concerned about possible surveillance can apply.

104. In addition to that, it would be desirable explicitly to allow the judge who issued the surveillance warrant to regularly review materials obtained by the police as a result of the surveillance. It will, first, permit the judge to assess whether the police remained within the original mandate, issued under Article 19 para. 1, and, second, it will allow him or her to understand better the usefulness and the intrusive effect of such measures. It would appear, from the Act, that the judge may request materials obtained as a result of surveillance only in the cases of prolongation of the wiretapping warrant, or in the cases of retroactive authorisation of the "urgent" surveillance which has been ordered without pre-authorisation (see Article 19 paras. 3, 9 and 10).

105. Another option would be to put in place a system of *ex post* oversight of the surveillance operations by some independent body acting on its own initiative.[88] The Venice Commission observes that under Article 19 of the Act, the Minister of Interior has to present before the Parliament, every year, a report on the surveillance activities conducted by the police. Yet, the Minister's role under Article 19 is to give a general overview of the surveillance activities, not to justify the necessity of specific operations. This mechanism, therefore, cannot replace the oversight of the *specific* surveillance operations by an independent body, which has an insight into the practice of surveillance and interception, but which is not institutionally linked with the police and which is not too close to the executive, to the law-enforcement or intelligence services.[89]

106. The Venice Commission stresses that this independent body should be able to review all aspects of the operations (with due deference to the reasonable operational discretion of the

[86] See the 2015 Report, §§ 39 and 126

[87] The courts are not the only institution which may be entrusted with the examination of such complaints; in addition, the States are free to establish other complaints and oversight mechanisms as long as these are effective: the ombudsman, the national human rights commission, the national audit office, the parliamentary oversight body, the inspector general, the specialized intelligence oversight body and the complaints commission for intelligence services (see the national examples of such complaints mechanisms in the UN Report of the oversight of intelligence services, para. 11). That being said, the Venice Commission considers that the judicial or quasi-judicial examination of complaints provides for stronger guarantees.

[88] In contrast to a complaints mechanism, such body would review surveillance operations *ex officio*, on the regular basis and not necessarily at the initiative of the targeted individuals.

[89] The UN report on the oversight of intelligence services (entitled "Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight", by Special Rapporteur Martin Scheinin, prepared at the request of the Human Rights Council) indicates as follows: "An effective system of intelligence oversight includes at least one civilian institution that is independent of both the intelligence services and the executive" (para. 8).

relevant agencies), to have access to all materials (even classified),[90] and be able to apply legal remedies appropriate in the situation.[91]

107. The Venice Commission is aware that the creation of a totally new body in Poland, and the delimitation of its competence *vis-à-vis* the police/prosecutors on the one hand and the courts on the other, can take time. Bearing in mind the limited amount of time the Polish legislature had, it is not surprising that no such body was created in December 2015. However, at least in the light of how the present system of metadata access under Article 20c is constructed (see paragraphs 109 et seq. below), and taking into account the weaknesses in the *general oversight* of more intrusive secret surveillance (provided by Article 19) such a body does seem to be necessary.

108. In sum, prior judicial authorisation, provided by Article 19, is a very important procedural safeguard; however, by itself it is not sufficient to ensure the accountability of the police (and other law-enforcement agencies which may be involved) in relation to the secret surveillance operations. The Polish authorities are free to design a model which would ensure effective control of the surveillance operations, provided that it involves an *independent body* which conducts effective review of specific operations and has the necessary legal tools to detect and combat abuses (or several such bodies).[92] Individuals concerned by the surveillance should be notified *ex post* about the measures in order to be involved in the process of review, or, when it is impossible, other mechanisms should be put in place which would permit looking at the case from the point of view of the privacy interest of those concerned by the surveillance, or enable an effective oversight of the reasonableness and lawfulness of such measures.

b. Authorisation and oversight of metadata collection under Article 20ca

I. Authorisation

109. The Act does not provide for a judicial authorisation of metadata monitoring operations under Article 20c: in the logic of the Polish law, metadata collection is regarded as a less intrusive method of information gathering, which does not necessitate the same level of procedural guarantees as "classical" surveillance under Article 19. The Venice Commission admits that even though judicial pre-authorisation of each operation of metadata collection would be desirable, in some cases such procedure may be too cumbersome for the police. The police (and rescue services) need this type of data very often, and providing for a system of prior independent authorization for access to this is not practicable, nor is it necessary – at

[90] The Commissioner for Human Rights of the Council of Europe, in the 2015 issue paper entitled "Democratic and effective oversight of national security services" (para. 13) noted as follows: "[A]ll bodies responsible for overseeing security services [should] have access to all information, regardless of its level of classification, which they deem to be relevant to the fulfilment of their mandates. Access to information by oversight bodies should be enshrined in law and supported by recourse to investigative powers and tools which ensure such access. Any attempts to restrict oversight bodies' access to classified information should be prohibited and subject to sanction where appropriate."

[91] The Venice Commission only describes the powers of the independent oversight body which relate to the verification of the lawfulness and necessity of the particular surveillance operations. However, the mandate of such body may be much broader, and include powers related to the more strategic control of the activities of the relevant State agencies. Thus, for example, an idea to explore would be to get such body involved in the allocation of budgets by the Parliament related to the surveillance operations; by giving such powers to this body the law might give it an additional and very powerful tool of responding to the abusive surveillance requests.

[92] In *Weber and Saravia* the ECtHR was satisfied with the German system of supervision of strategic (i.e. non-targeted) surveillance which included a Parliamentary Supervisory Board, which consisted of 9 MPs, including members of the opposition, the Federal Minister, and an independent Commission, which had to authorise surveillance measures and had substantial power in relation to all stages of interception. In *Kennedy v. UK*, cited above, the ECtHR approved the system by which the Investigatory Powers Tribunal ("IPT"), an independent body composed of persons who held or had held high judicial office and experienced lawyers which had the power, among other things, to quash interception orders, interacted with the Interception of Communications Commissioner, likewise a functionary who held or had held high judicial office and who had access to all interception warrants and applications for interception warrants (see also *Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands*, No. 39315/06, 22 November 2012, § 98).

least, as regards the less sensitive kind of metadata (such as subscriber information). In these cases *ex post* notification to a court (or another independent oversight body – see paragraph 113 below) would suffice.

110. The main exception from this rule may be the "content-related" metadata: the Venice Commission recommends the Polish authorities to consider including it (if it is not already the case) into the scope of Article 19, with all procedural guarantees which may accompany access to it (i.e. essentially judicial pre-authorisation). *Ex ante* authorisation could also be considered for measures of broadly targeted metadata collection (where a geographical area at a given time is the target). However, for the collection of most types of metadata *ex post* oversight of specific operations should be an adequate safeguard against abuses.

II. *Ex post* oversight

111. Article 20ca requires the police to submit, to a competent regional court, a semi-annual report containing bulk statistical information about the metadata monitoring during the past period.[93]

112. The Venice Commission considers that this reporting obligation is insufficient to ensure the accountability of the police in respect of the operations related to metadata collection. First, such reports contain only summarised information, which does not give insight into the particulars of each specific case. It is unclear what sort of conclusions a judge may draw from reading such report. Indeed, under Article 20ca para. 3 a judge may take an initiative and request "the materials that justify disclosure" of metadata to the police; however, it is unclear what would incite him or her to entertain such individualised analysis. Finally, in the unlikely event that a judge is pro-active, examines the materials of a specific case and detects any irregularity in them, it is unclear what sort of measures s/he might take in such a case.

113. The question is whether the *ex post* oversight should be entrusted to a court or to another independent body. In some countries, the solution is to give this function to the prosecutor, who is "one step further away" from the investigation from the police. In theory, the culture of the prosecutor should be more dominated by the law than the police culture, but the degree of formal/institutional independence of the prosecution service from the executive varies depending on the country.[94] And, as already noted above, the ECtHR has been reluctant to accept a prosecutor as an "independent" official who can be entrusted with the supervision of the police operations.[95]

114. A possible solution would be to involve the *courts* more deeply into the oversight of the specific metadata monitoring operations. This is possible if the courts are given sufficient resources (time, access to technical expertise, specialist competence etc.). However, the problem is that metadata interception is difficult to separate from other aspects of police investigative work. It may be difficult for the ordinary courts to exert a sort of standing control function over the police.[96]

---

[93] Namely "(1) the number of cases of obtaining telecommunications, postal, or on-line data in the reporting period, quoting the type of the data; 2) legal qualifications, with connection with which the requests for the telecommunications, postal, or on-line data were filed, or the information on obtaining the data in order to save human health or life, or to support rescue and find missions."

[94] See CDL-AD(2010)040, Report on European Standards as regards the Independence of the Judicial System: Part II - the Prosecution Service, §§23 et seq.

[95] See *Dumitru Popescu v. Romania (no. 2)*, cited above, *Iordachi and Others*, cited above, § 47, *Roman Zakharov*, §§277 et seq.

[96] See the 2007 Report on the Democratic oversight of the Security Services (see §§ 201 et seq., hereinafter "the 2007 Report"), where the Venice Commission concluded (see §§212 and 213) that "control by the ordinary courts does not appear as the best instrument of accountability for or redress against security and intelligence agencies".

115. A better alternative is expert bodies which can serve as either a supplement or a replacement for judicial accountability. The Venice Commission refers to its 2007 report (see §§ 218 et seq.) which describes composition and mandate of such bodies, where it stressed, in particular, that "where an expert body […] operates only as a substitute for judicial authorisation and not simply as a complement to it, it is especially important that the body in question is sufficiently capable and independent to exercise a real control" (§ 240).

116. Be it as it may, any system of *ex post* oversight should involve a genuinely independent body having the necessary expertise and powers to adequately review specific operations of metadata monitoring. As in the case of secret surveillance under Article 19, the Polish authorities have considerable freedom to design a system involving an independent body, which would ensure that the police have to "go outside of the house" and convince an independent observer of the need for the measure.[97] The law should require that the oversight body conducts proactive and continuous control of all operations and has necessary powers *vis-à-vis* the police/prosecutors. The Act may also provide for a qualified notification obligation and a complaints mechanism (before a court or before an independent oversight body).[98]

117. The Venice Commission reiterates that the existence of an *ex post* control does not exclude the possibility of a judicial pre-authorisation of certain most intrusive surveillance measures, including those in the field of metadata collection. In some countries (for example, in Sweden) judicial control *ex ante* is supplemented by the *post hoc* control by an independent organ. The experience of other states shows that this does not involve an interference with judicial independence. An important advantage of such a body is that it could be given a special mandate to monitor (and so deter abuse of) metadata collection in more controversial situations: i.e. interception of privileged communications, interception of geographical targets, content-related metadata, preventive (of crime or security dangers) access to metadata, etc.

118. To simplify the task of the police and reduce the burden of the courts, it should be possible for the Polish legislator to remove even from the scope of *ex post* control operations related to the police accessing the *subscriber data*. If the Polish legislator decides to do so, such operations will not be scrutinised by the courts (or other independent body) on a regular basis; however, in this scenario a system of logging should be in place, combined with some sort of posterior, sampling testing of the appropriateness of such selected operations. That being said, beyond that "least intrusive" kind of metadata, all other operations of the police should be susceptible to a comprehensive and effective *ex post* control.

c. Direct access to metadata

119. Article 20c para. 3 provides for direct access of the police to metadata "without participation of the employees" of the ICT service provider, "if it is provided for in the agreement concluded by and between the Police Commander in Chief and that entity". Thus, the police may have permanent and direct access to the metadata.

120. In *Roman Zakharov*, cited above, the ECtHR held as follows: "[A] system, such as the Russian one, which enables the […] police to intercept directly the communications of each and every citizen without requiring them to show an interception authorisation to the communications service provider, or to anyone else, is particularly prone to abuse. The need

[97] In *Klass and Others*, cited above, §56, the ECtHR held that although it is in principle desirable to entrust supervisory control to a judge, supervision by non-judicial bodies may be considered compatible with the Convention, provided that the supervisory body is independent of the authorities carrying out the surveillance, and is vested with sufficient powers and competence to exercise an effective and continuous control.

[98] According to the FRA guidebook of 2015, parliamentary oversight bodies of several EU Member States, namely Croatia, Hungary, Lithuania and Romania, also function as complaints-handling bodies. Oversight bodies other than parliamentary committees, such as those entailing executive and expert oversight, may also provide remedies, as is the case in Belgium, Croatia, Germany, Denmark, Hungary, Malta, the Netherlands, Portugal and Sweden (para. 70).

for safeguards against arbitrariness and abuse appears therefore to be particularly great" (§ 270). So, such direct access is not per se forbidden by the ECtHR, but because it is particularly prone to abuse, any State having such a system must provide for particularly strong safeguards.

121. Indeed, direct access to metadata has its practical advantages. Furthermore, at the meetings in Warsaw the authorities assured the rapporteurs that only certain designated officers of the police have direct access to metadata of the ICT providers,[99] and that the police keep record of all log-ins by those officers. These are minimal safeguards, which should be preserved. However, the fact that law-enforcement agencies can access data without the telecommunications companies knowing they have done so, in unlimited quantities, without significant costs (which has been a major factor limiting overuse of this method in other countries, but which does not appear to be an important consideration in Poland) obviously involves a much greater scope for abuse. Furthermore, these specially designated officers, while being specialists, do not appear to function as "gatekeepers", filtering away unjustified applications (which is the case in some other states, like UK or Sweden), but rather only as facilitators (i.e. communication channels).

122. The Venice Commission stresses that, under the current Act, there is no effective oversight of the metadata collection by an independent body, which might verify whether the police uses its powers in a reasonable manner, in accordance with good investigative practices (see above, the discussion about authorisation and oversight of metadata collection in paragraphs 91 et seq.).

123. Furthermore, as understood by the rapporteurs, in the case of the real-time direct access there may be difficulties in separating, technically, content from metadata. If this is the case, then it is necessary to build in blocks into the system, which would ensure that the content is clearly distinct from metadata, and that the police have no access to the former.

124. In any event, and in sum, direct access strengthens even more the argument for putting in place an efficient mechanism of supervision.

d. Recording obligation

125. The ECtHR has found that an obligation on the intercepting agencies to keep records of interceptions is particularly important to ensure that the supervisory body had effective access to details of surveillance activities undertaken.[100] This is *a fortiori* true for metadata collection, since the Act, in its current form, does not provide for prior control of such operations by the courts. Such records should explain, at least briefly, the reasons for such monitoring, and refer to specific facts. The reasons given should be detailed enough to enable the oversight body to assess the reasonableness of the actions of the police.

126. Furthermore, those recordings should always be available for independent examination. Technical protocol of access to metadata (in case of direct access) should guarantee that the competent officer would not be able to get access to it without leaving traces. Oversight bodies should be able to conduct surprise controls *in situ*, obtain all necessary documents, obtain testimony of the agents under oath, etc. Finally, the absence of the records or their inaccuracy should be defined in the law as serious professional faults, if not crimes.

[99] Thus, as the rapporteurs learned, there are about 102,000 police officers, but only a "few hundred" are authorized to access metadata. At regional, city and national levels the police appoint single points of contact between the police and telecommunications/internet companies.

[100] *Kennedy*, cited above, § 165; *Roman Zakharov*, cited above, § 272.

E. Liability of State officials

127. Principles 15, 16 and 17 of the UN report on the oversight of intelligence services,[101] stress the importance of regulating criminal, civil and other liability of the officials involved in the surveillance operations for violations of domestic law and breaches of the international human rights obligations. The Venice Commission fully subscribes to these principles. The rapporteurs understood that criminal liability for abusive surveillance may be covered by other statutes (such as the Criminal Code). However, it is important to ensure – if necessary by referring in the Act to relevant provisions in other legislation – that deliberate and gross breach of privacy or misuse of official powers in collecting metadata or conducting secret surveillance is clearly defined as a criminal offence.

128. The Venice Commission also recommends attaching liability not only to material violations of somebody's privacy, but also to more "formal" breaches of the procedure (such as the failure to record properly the results of the surveillance operation, failure to destroy the materials in time, or their transmission to unauthorised persons), even if it may be sometime difficult to link such infringements to a violation of somebody's privacy.

VII. Conclusions

129. The Venice Commission welcomes the effort made by the Polish legislator to implement the judgement of the Constitutional Tribunal of Poland of 30 July 2014. The amendments to the Act introduced in 2016 followed some of the recommendations contained in that judgement.

130. The Venice Commission notes that many states now face very real threats from terrorism and organized crime. Under the ECHR, states have a margin of appreciation in deciding how to draw the balance between security and liberty. The Polish legislator is by no means alone in having attracted considerable criticism as to how this balance has been drawn. Nor is the Polish government alone in reacting slowly to changed public conceptions, and to the judgments of the CJEU and the ECtHR, which indicate that metadata monitoring involves a larger interference with privacy.

131. Having said this, procedural safeguards and material conditions set in the Police Act for implementing secret surveillance are still insufficient to prevent its excessive use and unjustified interference with the privacy of individuals.

132. In order to improve the Act, the Venice Commission makes the following most important recommendations (in addition to other recommendations contained in the text of the opinion):

- to incorporate into the Act the principle of proportionality, guaranteeing that secret surveillance/metadata collection is to be ordered only in the most serious cases, especially under the "urgent procedure" (Article 19 para. 3); to describe in the Act a probability test for ordering the surveillance/metadata collection;
- to review the definition of various types of metadata and, in particular, to extend the procedures provided by Article 19 to the "content-related" metadata;
- to prohibit in the Act surveillance of communications which are *on the face* covered by a lawyer-client privilege; to define precisely when this presumption can be overturned, and to do so also in respect of other privileged communications;
- to limit the duration of the metadata monitoring; to require the police to keep proper records which should enable effective *ex post* control of the monitoring operations, especially implemented through "direct access",

[101] "Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight", by Special Rapporteur Martin Scheinin, prepared at the request of the Human Rights Council

- to complement the system of judicial pre-authorisation of the “classical” surveillance under Article 19 with additional procedural safeguards (a “privacy advocate”, a complaints mechanism, a system of ex-post automatic oversight of such operations by an independent body, etc.);
- to provide, in respect of metadata collection under Article 20c, an effective mechanism of oversight of specific operations by an independent body; such body should have necessary investigative powers and expertise and be able to use appropriate legal remedies.

133. The Venice Commission remains at the disposal of the Polish authorities for any further assistance they may need in case of the revision of the legislation analysed in the present opinion.