Privacy International's submission in advance of the consideration of the periodic report of Macedonia (former Yugoslav Republic of), Human Rights Committee, 114th Session, 29 June – 24 July 2015

5 June 2015

Privacy International is concerned at recent reports that Macedonian security service have intercepted phone communications of around 20,000 individuals, including members of non-governmental organisations, journalists and opposition politicians. If these reports are correct, the relevant surveillance measures were likely conducted outside applicable domestic law. Macedonian law requires telecommunication service providers to build in "backdoors" to allow interception of communications by the intelligence services, which is conducted without effective safeguards or oversight.

Privacy International is concerned that the current laws in Macedonia facilitate mass surveillance, and the absence of any effective oversight and accountability of the intelligence services means that the State is not adequately protecting from unlawful interference with the right to privacy, in violation of Article 17 of the International Covenant on Civil and Political Rights.

Current law on interception of communications

Privacy of communications is expressly guaranteed in article 17 of the Macedonian Constitution, which states that "the freedom and confidentiality of correspondence and other forms of communication is guaranteed. Only a court decision may authorize non-application of the principle of the inviolability of the confidentiality of correspondence and other forms of communication, in cases where it is indispensable to a criminal investigation or required in the interests of the defence of the Republic."

Under the law, interception is authorised by a judge, on request by the public prosecutor, who can act on their own initiative or on requests from other officials, such as police or other persons authorised by law. The monitoring period is up to four months, but it may be extended for up to two years for persons suspected of grave crimes.

In 2014, the UN Special Rapporteur on the right to freedom of opinion and expression noted that "despite these clear protections of the right to privacy, additional norms and

legal reforms have recently expanded the scope of surveillance of communications without establishing adequate protections and oversight."[1]

The Law on electronic communications of 2014 regulates the conditions and manner of provision of public electronic communications networks and public electronic communication services.

Under the law operators of telecommunications networks and the providers of public telecommunications services need to ensure confidentiality in communications to the best of their technical abilities. Article 175 introduces a series of requirements to telecommunications providers. In particular, under this article telecom operators are obliged to allow appropriate interface and establish lines for the transfer of electronic communication to those institutions that are authorized for communications surveillance. The operators are obliged to enable competent authority to monitor the communications in real time and ensure that persons under surveillance do not notice changes in the quality of the communication services caused by the interception.[2]

Reports of wiretapping of journalists, opposition politicians and others

In February 2015, the Macedonian opposition party (Social Democratic Union of Macedonia, SDSM) alleged that over 20,000 persons, including political figures, members of non-governmental organisations and journalists, were subjected to communication surveillance by the Macedonian security agency. The government did not deny the existence of the wire-tapping, but initially attributed it to the work of a "foreign intelligence service".[3]

This brought into sharp light the long-standing concerns on the lack of effective supervision and control of the activities of the Macedonian Security and Counter Intelligence Service (UBK) to limit unlawful interference with the privacy of personal communications.

The only body authorised to supervise the work of the UBK is a Parliamentary Commission. According to media reports, the UBK's written reports to the Commission contained no data on the agency's use of what are called "specific investigative measures", such as eavesdropping. Members of the Commission in the past have voiced their frustration over this lack of accountability.[4]

1See report of the UN Special Rapporteur on freedom of expression visit to the Former Yugoslav Republic of Macedonia, UN doc. A/HRC/26/30/Add.2.

2 Relevant laws (in Macedonian) available here: http://www.pravo.org.mk/documentlaws.php?name=електронски+комуникации

3 See http://www.dw.de/macedonia-reels-over-evidence-of-orwellian-surveillance/a-18285626

4 The former head of the Parliamentary Commission has reportedly stated in 2011: "we have been asking the UBK to submit quarterly reports on eavesdropping but did not receive a single such report, which indicates that the use of 'special investigative measures' is being misused". See http://www.balkaninsight.com/en/article/veil-of-secrecy-shrouds-macedonia-s-fifth-sector

If the recent reports are confirmed, the scale of the mass surveillance in Macedonia would represent a serious violation of the right to privacy and it is already having a chilling effect on freedom of expression.

Recommendations

Based on these observations, Privacy International suggests that the following recommendations are addressed to the Macedonian government:

- Take all necessary measures to ensure that its surveillance activities conform to its obligations under the Covenant, including article 17; in particular, measures should be taken to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity, regardless of the nationality or location of the individuals whose communications are under surveillance.
- Ensure that public and private telecommunications and internet service providers can review warrants before any interception of personal data from their network takes place or whenever data related to their subscribers is requested, and that they can challenge such warrants to an independent monitoring authority or before the courts.
- Reform the current oversight system of surveillance activities to ensure its effectiveness, including by establishing an effective and independent oversight body with a view to preventing abuses.