Analysis

The use and misuse of telephone taps and communications data by Bulgarian intelligence

Alexander Kashumov (Access to Information Program, AIP)

Tzvetan Tzvetanov, Minister of Interior in the Citizens for European Development of Bulgaria (GERB) government from 2009-2013, was criticised for widespread unauthorised wiretapping after information was published in the media in 2013. Concerns surfaced following an anonymous complaint registered with the Public Prosecutor's Office and a former minister's outspoken allegation, in a television interview, that all GERB cabinet ministers were subject to permenant phone-tapping throughout their time in office. On 15 April 2013, the Prosecutor General told a press conference that his investigation had revealed a lack of oversight within the Internal Ministry Directorate responsible for the technical performance of phone tapping. The investigation's report was only partly classified as secret, but neither the open nor the secret part of the report was made available to the public.

The scandal widely influenced public opinion before the May 2013 parliamentary elections.

The context

During Bulgaria's communist past, the secret surveillance of people by the former state security services was common practice. This included the opening of correspondence and the interception of other communications. The purpose and result of this surveillance remains "unclear." The 1991 Constitution prohibited tracking, taking pictures and the filming or recording of individuals without their knowledge or consent, except in cases prescribed by law (Article 32, para. 2). In addition, Article 34, para. 2 of the Constitution allows interference with correspondence and other communications only when it is necessary for the detection or prevention of serious crime (punishable by imprisonment of more than five years) and when prior permission has been granted by judicial authority.

The constitution necessitated the adoption of a special law to cover wiretapping which was passed in 1999 and has been amended several times since. It provided two grounds for permissible wiretapping: the investigation of serious crime and the protection of national security. It also established a list of bodies entitled to request the use of intercepts. Each request must be approved in a court of law before an application can be made. An exception from this rule is allowed in cases of pressing need, when approval by a judge must be given within 24 hours.

In 2007 the European Court of Human Rights (ECtHR) found the law to be in violation of Article 8 of the European Convention of Human Rights (Convention, ECHR) since it failed to guarantee a system of secret surveillance consistent with the right to private life. [1]

Brief summary of the ECtHR case on secret surveillance

The ECtHR generally examines issues under Article 8 of the Convention by following the three-part test under para. 2. It found that the existence of secret surveillance itself represents interference with the right to private life and therefore issues under the three-part test should be examined. The assessment of whether the interference is "in accordance with law", in the meaning of Article 8, para. 2 of the ECHR, includes an assessment of the quality of the law.

In view of the risk of abuse intrinsic to any system of secret surveillance, the law governing the system must be sufficiently clear and particularly precise. The ECtHR has developed a set of minimum safeguards for such laws to be evaluated. They cover the following six issues:

- the nature of the offences which may give rise to an interception order;
- a definition of the categories of people liable to have their communications monitored;
- a limit on the duration of such monitoring;
- 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 data obtained may or must be erased or the records destroyed.

In its judgment, the ECtHR found that the Bulgarian law:

> "does not provide for any review of the implementation of secret surveillance measures by a body or official that is either external to the services deploying the means of surveillance or at least required to have certain qualifications ensuring his independence and adherence to the rule of law. Under the SSMA [the Bulgarian law], no one outside the services actually deploying special means of surveillance verifies such matters as whether these services in fact comply with the warrants authorising the use of such means, or whether they faithfully reproduce the original data in the written record. Similarly, there exists no independent review of whether the original data is in fact destroyed within the legal ten-day time-limit if the surveillance has proved fruitless (see, as examples to the contrary, Klass and Others, p. 11, § 20; and Weber and Saravia, § 100; and Aalmoes and Others, all cited above). On the contrary, it seems that all these activities are carried out solely by officers of the Ministry of Internal Affairs." [2]

In addition, the Strasbourg court found there was no provision in the law for acquainting the judge with the results of the surveillance and for instructing him or her to review whether the requirements of the law had been complied with. Nor do regulations exist that specify with an appropriate degree of precision, the way in which intelligence obtained through surveillance should be screened, the procedures for preserving its integrity and confidentiality and the procedures for its destruction. [3]

Further, the court found that no statute lays down a procedure governing the Minister of Interior's actions in exercising control. The Minister has not issued any publicly available regulations or instructions on the subject. As to oversight by an external body, the ECtHR outlined that neither the Minister, nor any other official, is required to report regularly to an independent body or to the general public on the overall operation of the system or the measures applied in individual cases. [4]

Finally, the Court noted that under Bulgarian law persons subjected to secret surveillance are never notified of this fact. Although the right to access such information is not unlimited and exercisable at any time by preference of the individual concerned, the Court adheres to established case-law, accepting that:

> "as soon as notification can be made without jeopardising the purpose of the surveillance after its termination, information should be provided to the persons concerned." [5]

The ECtHR has also assessed the situation in the UK, Germany, Sweden, Norway and Switzerland over different periods. It is unclear, however, what is going on among the other Council of Europe members on this matter, nor within the narrower circle of EU Member States. It seems that the latter were pushed to implement EU legal instruments, such as Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks (Data Retention Directive), without a preliminary assessment of the national systems of secret surveillance and guarantees against its possible abuse.

Retention of electronic communications (traffic) data

The establishment of mobile phone service providers in Bulgaria in the 1990s created a new source of communications data and made it necessary for these companies to formulate agreements with the police and intelligence services regarding the circumstances and conditions of access to their customers' traffic data.

Following Bulgaria's accession to the EU in 2007, in January 2008 the Ministry of Interior (MI) and a state agency responsible for information technology and communications issued a regulation on data retention (Regulation No. 40). It stated that all companies providing mobile phone or internet services are obliged to store traffic data for 12 months (the Data Retention Directive mandates for retention between 6 and 24 months, leaving Member States the discretion to choose). Access to data was provided to: to the Ministry of Interior special directorate through an interface (which means the existence of permanent electronic connection for **unlimited access**); to the police and public prosecutor in cases of a simple written request; to the security services on simple written request. The regulation was justified as the transposition of the Data Retention Directive. Protests by bloggers and civil society groups in early 2008 were not taken into account and did not even elicit a response by state authorities.

In spring 2008, the Access to Information Program (AIP), an NGO that has operated in Bulgaria since 1996, filed a complaint claiming that Regulation No 40 as a whole should be declared null and void and that its provision regarding access to stored data (Article 5) is contrary to the constitutional right of respect for private life and communications and to Article 8 of the ECHR.

The first instance level of the Supreme Administrative Court (SAC) accepted that AIP had the standing to challenge the Ministry of Interior regulation on points of law, but rejected the complaint on its merits. AIP appealed and in December 2008 a five-member SAC panel repealed all three paragraphs of the Regulation's provision on the basis that unauthorised access to traffic data contravenes the constitutional right to privacy and correspondence and the Convention. The court action in Bulgaria was not isolated. In the period between 2008-2009 there were also decisions taken by the Romanian Constitutional Court and the German Federal Constitutional Court on the matter of the compatability of data retention regimes with the fundamental right to private life and correspondence. In all of these cases the domestic implementation of the data retention regime was found to be problematic.

The Bulgarian government reacted to SAC's ruling by immediately proposing changes to the Electronic Communications Act, with the aim of re-establishing automated access to data stored by electronic services providers. The parliament rejected the proposal and in March 2009 adopted a regime under which every request for access requires approval by a court to be processed.

Nevertheless, in 2010 after an acrimonious debate, the new parliament amended the Electronic Communications Act again to permit access to traffic data requests in criminal investigations to be processed without authorisation by a judge. In all other cases the requirement for court permission before access remained. The government abandoned its effort to re-establish an automated connection between the Ministry off Interior and service providers' databases.

Statistics about intercepts and access to traffic data

In 2009, the Bulgarian law on intercepts was changed following the Strasbourg court's judgment. A parliamentary sub-committee was established to monitor surveillance and the data retention system and practices. It did not do much in terms of exercising control but published statistics, which is an important contribution to the debate and a precondition to push for change.

According to a report by the Bulgarian Supreme Cassation Prosecution's Office in 2001, over the period 1999-2000 courts issued 10,000 authorisations for wiretapping for a population of less than 8 million people. This statistic was referred to in the Strasbourg court judgment with the comment that in the *Malone case* [6] it was found that in the UK there have been 400 telephone tapping warrants and less than 100 postal warrants issued annually during the period 1969-79, for more than 26,428,000 telephone lines nationwide. [7] The Bulgarian report points out that only in 267 or 269 of the cases was the information collected used in criminal proceedings, barely 2-3%. In its first report in 2009, the parliamentary subcommittee reported that 9,600 warrants had been issued in one year, [8] which means that their number has doubled compared with 10 years ago (the 1999-2000 report covered a two-year period). According to data published in the Bulgarian press, US state courts reported 2,376 telephone intercepts for the same period. In 2010, the number of warrants issued by Bulgarian courts reached a record 15,864. For 2011, the number was nearly 14,000, while in the parliamentary subcommittee's report it is made clear that this figure was artificially reduced by including more than one warrant in the same document. As before, information collected was rarely used in court; in 2011 in only 5-6 % of all cases.

As regards data retention, Bulgarian media has reported that in March 2009 the Ministry of Interior told the parliamentary committee on internal security and public order that in 2009 there were 330,000 cases of access to traffic data involving about 40,000 persons. This huge number likely results from direct automated access between the electronic communication services' providers and the Ministry of Interior, which began at the end of January 2008, when Regulation No 40 came into force, and stopped in mid-December 2008 when the Supreme Administrative Court's decision on its lawfulness was published in the *State Gazette*. By comparison, the overall number of cases of access to traffic data for 2010 was 21,714. For the period between 1 January and 10 May 2010 only 2,760 warrants were issued (at a time when all access cases were authorised by the courts). After the amendments to the law which allowed access to traffic data without a court warrant criminal investigations came into force on 10 May 2010, access to traffic data increased. In 2012, there have already been 58,702 cases of unwarranted access to traffic data under open criminal investigations and 15,350 warrants for other cases. The overall number of accessed traffic data for 2011 exceeded that of 2010 by nearly four times.

Some conclusions

The facts and statistics about Bulgaria show that efforts to adopt legal instruments and measures to guarantee the right to private life and communications in the period of the transition to democracy, were jeopardised by newly adopted EU policies and legislation. The Data Retention Directive in particular was adopted without taking into account the capacity, tradition and ability of different member states to exercise control over - and be accountable for - wiretapping and access to traffic data. Assessment is lacking on the existence of measures to ensure that secret surveillance is exceptional, controlled and is used only to detect and prevent really serious crime.

A monitored individual's access to information about his / her secret surveillance is still exceptional within EU countries, while data processing among law enforcement agencies and intelligence authorities and the technical possibilities to exchange data continue to expand.

Detailed published statistics on data retention and access to stored data, as well as intercepts, would help to identify problems, trends and differences between the states involved, and make it easier to find solutions

It cannot be concluded from the debate in Bulgaria that electronic communications providers are ready to contribute to the control of these activities. Rather, they are intimidated by penalties in cases of non-compliance and find it easier to collaborate fully with law enforcement and intelligence authorities. The EU's efforts to fight terrorism and organised crime could instead legitimise suspicious and undemocratic practices in which secret surveillance and e-communications data will be used for unacceptable purposes.

Endnotes

1 Case of *Association of European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, application No 62540/00, the decision became final on 30 January 2008.
2. Para. 85
3. Ibid. para. 86
4. Ibid. para. 88
5. Para. 90
6. Malone v. UK
7. Cited judgment, para.92
8. This number is not present in the official public report, but was communicated by the media after the presentation of the report and the parliamentary subcommittee did not object.