



Erosion of the Privacy in the Republic of Macedonia

On the Amendments to the Law on Electronic Communications

The right to privacy in the Republic of Macedonia in the last few days has been threatened again. This is not the first time for the Government to seriously limit the right to privacy, one of the fundamental civil rights, without opening a broader public debate for such an important question. With allegedly a “technical” law on the electronic communications, essentially, the most protected spheres of privacy guaranteed with the international human rights agreements and the Constitution of the Republic of Macedonia have been violated. Namely, with the proposed amendments this law interferes with the penal law, since it envisages new authorities for the police and the secret services that are far beyond those envisaged in the Law on Criminal Procedure and the Law on Communications Surveillance. With the proposed amendments the controversial methods of personal data processing are introduced, which one could say are improper and too broad in regard to the purpose for which are collected and processed in the sense of the provisions from Article 5 Paragraph 1 Indents 1 and 3 from the Law on Personal Data Protection.

Namely, instead of simple “harmonization of the Law on the Electronic Communications in the area that regulates the obligations of the public communication services operators and providers with the provisions in the Law on Communication Surveillance” (as stated in the Government’s proposal), this Law establishes new possibilities for easy and direct interfering of the police and the secret services in the privacy, without any previous connection to the conditions and the practices for applying special measures from the Law on Criminal Procedure. Additionally, the police and the secret services have the freedom of making their own assessment without any previous permission or control. It is not very clear what the proposer means when he says that “the customers are in the focus, especially in the area of strengthening of their rights”, pointing it as the justification for the amendments?!

The **body authorized** for communication surveillance according to the proposed amendments is the **Ministry of Interior**, which **has a permanent and direct access** to the electronic communication networks and the buildings of the public communication networks operators and public communication services providers (a new subparagraph 47 in Article 4)! They, on the other hand are

obligated upon a request by the “competent state bodies” (no other body except the Interior Ministry is mentioned, not even the Ministry of Defence!?) to provide information about the traffic when necessary (and this something that is based on their own assessment!) for the purpose of preventing or disclosing crimes, to support the criminal proceedings or when it is in the interest of the security and the defence of the Republic of Macedonia. Hence, the grounds for applying the measures are much broader than those that have been envisaged so far with the Law on Criminal Procedure and the Law Communications Surveillance (disclosing and prosecuting crimes).

The public communications networks operators and the public communications services providers are obligated to provide the body authorized to perform surveillance (MOI) with permanent and direct access to their electronic communication networks as well as **“conditions for independent collecting of data about the traffic”**.

The courts or the Public Prosecutor's Office are nowhere mentioned as bodies competent for establishing and applying measures in compliance with the laws that the MOI only implements upon their request, i.e. orders. This approach is contrary to the Constitution of the Republic of Macedonia which in a number of provisions clearly and unambiguously states an enormous reserve, i.e. distrust in regard to the police and the other bodies with special authorities and for that reason the court is pointed out as the only body that could decide when the fundamental rights and freedoms are concerned.

According to the proposed amendments to the Law and the already weak controlling role of the court and the Public Prosecutor's Office, it becomes even less real when there will be no obligation for a court order to be presented to the operators and the public communications services providers! ¹

Among the measures envisaged within the Law on Electronic Communications as a matter of fact there are also two “new” so-called special investigative measures that our LCP or the Law on Communication Surveillance have not envisaged, explicitly not up till now.² Namely, the measure that consists

¹ Even before this the controlling role of the courts was minimized with the latest amendments to the Law on Criminal Procedure and the Law on Communications Surveillance, and since the special investigative measures are introduced in a very early stage of the procedure without demanding any specific evidences about the crime and the perpetrator the court is unable to assess whether the measures are really justified and even less whether all the other ways of disclosing and proving have been used. In the area of the state security the judge of the Supreme Court is not really capable to assess whether the measures are really necessary and justified. On the other hand the way the things are for the time being there are no real possibilities for anybody, not even the court, the prosecutor's office or the parliamentary committees to carry out any real, regular and efficient control over the real range of wiretapping.

² See: The Law Amending the LCS (Official Gazette of the Republic of Macedonia No. 110 from 2 September 2009); The Law Amending the LCP (Official Gazette of the Republic of Macedonia No. 83 from 10 July 2008).

of “providing data about the traffic” i.e. “a listing” about the contacts made on the fixed or mobile phone line, internet messages, etc. has been used by the police and the secret services for a long time, and the data collected in this way about the suspect, his habits, contacts, movements and other things after they are processed at the Analytical Sector they become an utterly useful tool for disclosing and preventing crimes, as well as for security and political goals (frequently even abuses). A somewhat newer method is the one that enables locating and following the movement and the contacts using the mobile phones or monitoring the internet connecting via a computer, a state of the art phone, etc. which is very similar to the measure of secret surveillance, as now envisaged with the LCP, but it is more efficient because practically it enables surveillance of the movement and the contacts of the suspects for a longer period of time in the past (practically, since the introduction of mobile telephony and Internet). For the state bodies these measures save a lot of time and staff engagement compared to the classical methods of operative surveillance performed by people.

The main problem is, certainly, the great intrusiveness of these measures, especially having in mind their duration (more specifically the long period during which they could be extended).

The easiness with which the government is trying to present these measures as some kind of superficial technical issue is astonishing. On the contrary these are measures that the European Court of Human Rights has characterized as **serious interference with the right to privacy**, and for that reason they require the same or similar regime as the wiretapping or other special investigative measures that are encompassed in the LCP and the Law on Communications Surveillance. The first most famous case that treated the so-called “metering” (listing) is the case of *Malone v. the United Kingdom* from 1984 when the European Court of Human Rights established that getting the details about the numbers that were dialled, the time of the calls and their duration were not regulated with clear legal rules that should have referred to the range and the manner of practicing discretion by the authorities.

The secret surveillance practice on the other hand was characterized by the European Court of Human Rights also as interfering in the privacy that is guaranteed with the European Convention on Human Rights in the famous case of *Klass v. Germany*. Ever since, the Court in Strasbourg has constantly emphasized the need of national laws to ensure proper protection from the arbitrary and uncontrolled interference of the state in the privacy of the individuals. It is not enough for the state to adopt some kind of legislation and to be considered that the human rights requirements have been fulfilled. In most of its verdicts the European Court of Human Rights looks into the quality of the national laws that primarily have to be sufficiently clear so that the citizens get enough indications about the conditions and the circumstances in which the authorities are authorized to reach for the secret and potential meddling with the right to respecting the private life and correspondence (*Malone v. the United Kingdom, Khan v. the United Kingdom, Contreras v. Spain, etc.*).

Even when the domestic system has certain incorporated protection mechanisms on different levels, including involvement of an independent judge, the system can still be open for abuse. In order to avoid possible abuses and arbitrary behaviour, the European Court of Human Rights states that the national legislation needs to define at least the following protection mechanisms: the nature of the punishable acts for which surveillance could be ordered; definition of the categories of persons whose communications could be under surveillance; the maximum duration of the surveillance; the procedure that needs to be followed for analysis, use and retention of the collected data; measures of caution that need to be undertaken if the information is passed to other persons and the circumstances in which the collected information could be or have to be deleted, and the recordings destroyed (*Weber and Saravia v. Germany* from 2006)

The law needs to be enough clear and precise so that the circumstances under which it would be applied should be sufficiently predictable in the sense that the citizens should know when the police or other security bodies could monitor the telephone and other private electronic communications.

Having in mind the fact that the risks from arbitrariness are always big when the competences of the public institutions are performed in secrecy and since the use of measures for communications secret surveillance in practice is not open for control by the concerned individuals or the broader public, it would be contrary to the rule of law if the legal discretion, which is in the hands of the executive power is a kind of a non-controllable authority.

Collecting and archiving the data about citizens in connection to the national security, should also be within the legally established limitations. In that sense the law needs to envisage the type of information that could be recorded; the category of individuals against which surveillance measures and data processing could be undertaken, for how long the data could be kept as well as the circumstances under which such measures could be undertaken and last but not the least the procedure that needs to be followed (*Rotaru v. Romania*). This means prescribing real procedures for supervising the implementation, either at the time when the prescribed measures were effective or later.

We could conclude that the measures that they are trying to legalize do not follow consistently the principles of legality, proportionality and subsidiarity as elemental protection from arbitrariness and abuse. In compliance with the requirement for necessity and proportionality emphasized by the European Court of Human Rights, the measures can be applied only in the most serious crimes and cases of organized crime. Apart from that a sufficient, proper and independent system of implementation control needs to be ensured for all the measures that interfere with the privacy of the citizens.

The requirements that refer to the interests of the national security should be seen with an especially healthy sense of scepticism. Namely, with the proposed changes, the security services will not be required to prove before

anybody that there is a direct, imminent, concrete and serious threat for the state and the constitutional order, and not only some undefined or speculative threat.

A law should allow the citizens to have access to an independent institution (a court) before which they will be able to legally contest every application of these measures against a person as well as the way in which it is done.

The deadline for retention of non-processed data is the maximum deadline that has been envisaged as a standard of 24 months (Article 112, Paragraph 1), even though in most of the countries of the European Union the maximum period of 6 months for retention data has been accepted, in order to respect the safety and secrecy of personal data. Apart from that there should also be new provisions in Article 112 from the Law that will operationalise the content from the 2006/24/EC Directive of the European Parliament and of the Council of the European Union on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks.

The Law should incorporate also provisions that will provide harmonization with the provisions from the Directive 2009/136/EC of the European Parliament and of the Council of the European Union amending the Directive 2002/58/EC in regard to the processing of personal data and protection of privacy in the area of the electronic communications.

Transparency Macedonia

“Ferid Bajram” 39, 1000 Skopje, Republic of Macedonia

Tel./fax: 02/ 31 21 100

www.transparentnost-mk.org.mk