Lawful Interception of Telecommunications in Kosovo: Security Implications

Shpend Kursani[1]
Kosovar Centre for Security Studies

Abstract
Building upon the current multitude security actor environment and legislative set-up, this paper assesses the interception of telecommunications in Kosovo as a sensitive, yet very effective measure of investigation. It elaborates in detail the current problems pertaining to interception of telecommunications which include the legislative gaps, the overlap created by poorly defined authority over the execution of orders of interception of telecommunications and the lack of cooperation not only between the domestic and international security institutions present in Kosovo but within the domestic security institutions as well. The analysis is not limited to the security institutions per se; the paper further extends on to the procedures and cooperation that exist between the security institutions and the telecommunications operators as well as their capabilities and infrastructural set-up which are important in preventing misuse of private data throughout the process of lawful interception of telecommunications. Based on the policy objectives that this paper draws, policy recommendations are provided which in general and among other things include the enhancement of the current legislation, the establishment of a central system that would boost cooperation between all the security actors, the introduction of new and advancement of current inspection and monitoring mechanisms. The implementation of the recommendations would ensure an effective lawful interception of telecommunications on the one hand and protection of privacy as a fundamental human right on the other hand.

Keywords: lawful interception of telecommunications, special investigation measures, security actors

[1] Shpend Kursani has an MPhil degree in International Relations from the University of Cambridge (2011) and a BSc degree in Public Policy and Management from the American University in Kosovo (2007). Kursani has been involved in various sectors and institutions in Kosovo. He has been involved in the establishment of the American Chambers of Commerce in Kosovo (2004) and has continued to work as a consultant at the Management and Development Associated in strategic planning and in research intensive projects (2004-2006). Kursani has also been involved in the telecommunications industry while working at Ipko Telecommunications as a product development department manager (2007-2010). Currently he is a research associate at the Kosovo Centre for Security Studies, a contributing analyst at Wikistrat Global Strategies, and an adjunct lecturer at the Universum University.

Methodology

This paper is a result of a qualitative research which has covered various primary and secondary sources. The primary sources include interviews that have been conducted with current and former high officials at the Kosovo Police, the officials dealing with the interception of telecommunications at EULEX, and the current and former employees working in the administrative and technical divisions in telecommunications companies. Laws pertaining to criminal procedures, special investigation measures, intelligence agencies, telecommunications as well as relevant regulations and official decisions taken by relevant authorities in this sector have been also consulted and thoroughly researched. Various secondary sources from electronic and printed media as well as policy briefs and research reports published by various local and international institutions have been considered where examples have been drawn to support various claims and arguments in this paper.

KCSS would like to acknowledge the support of Open Society Foundation – Think Tank Fund, for making the research and release of this publication possible. Apart from that, it is worthwhile mentioning the overall institutional support of the Think Tank Fund in strengthening the capacities and skills of KCSS researchers

List of Abbreviations

CEO	Chief Executive Officer
DAJP	Duly Authorised Judicial Police
EULEX	European Union Rule of Law Mission in Kosovo
IHSOP	Institute for Strategic Research of the Public Opinion (Instituti për Hulumtime Strategjike të Opinionit Publik)
ISP	Internet Service Provider
JSI	Justice and Security Institutions
KIA	Kosovo Intelligence Agency
MVNO	Mobile Virtual Network Operators
PCPC	Provisional Criminal Procedure Code
PTK	Post and Telecommunications of Kosovo
SHIK	Kosovo Information Service (Shërbimi Informativ i Kosovës)
TRA	Telecommunications Regulatory Authority
UNMIK	United Nations Mission in Kosovo
VAS	Value Added Services

Contents

1. BACKGROUND

The nature and mandate of the security institutions in Kosovo have altered several times during the past decade. Although the mandate to provide intelligence services and to take special investigation measures has over time gradually shifted from international security actors to the local ones, especially after the declaration of independence of Kosovo, interception of telecommunications continues to be gloomy. There are several instances where the issues of interception of telecommunications, and the cracks in the system thereof, have made it to the public. Not very long ago, a deficiency in the system has been hinted by the Chief Executive Officer (CEO) of the Post and Telecommunications of Kosovo (PTK) when he complained about having only PTK's customers exposed to lawful interceptions, due to the alleged refusal of the other operator to allow the Justice and Security Institutions (JSIs) to intercept their customers.[2] In addition to this, the previously raised debates and news reports over the existence of party affiliated intelligence organisations (especially from the post-war period) and the presence of foreign intelligence services in Kosovo[3] have raised eyebrows among the public.

The general public is not the only confused party in this muddle. The expression of suspicion by the Minister of Interior, whose mission is to built, preserve and increase the security for all citizens in Kosovo, for being intercepted by the international organs in Kosovo, more specifically by the EULEX, adds to this gloomy environment and extends the confusion of this issue over to the institutional level as well. Some of the civil society actors might have considered the minister's declarations insincere; however, it has certainly questioned the actual ownership of surveillance and special investigation measures in the country. Another highly relevant yet tacit security concern for Kosovo and its institutions is the current fixed line international interconnection set-up with Serbia. The current set-up, which allows Serbia to have full control of the international incoming calls diverted to Kosovo, raises security concerns even more when considering the fact that relations between Kosovo and Serbia are pending and rather undefined.

Interception of telecommunications may be considered an insidious tool, yet it is a powerful measure of investigation which helps in identifying and prosecuting the suspects who are engaged in serious criminal offenses and those who otherwise threaten national security in general. Although this provides a clear and straightforward purpose of interception of telecommunications, this measure of investigation in Kosovo inherits various deficiencies in many different levels. First, there is no clear distinction in the legislation between interception of telecommunications and other special investigation measures which make the legislation unable to restrict their use depending on the degree of a specific criminal offense and their effects on privacy. Second, there is a lack of clear ownership over ordering lawful interception of telecommunications and there are no proper mechanisms to regulate the cooperation between multiple security actors present in Kosovo. This in turn allows for overlaps to occur when issuing and executing orders of interception of telecommunications, which in turn make this measure of investigation rather inefficient. Moreover, there are no existing inspection and monitoring mechanisms that would prevent abuse of the measure by either side: the JSIs or the telecommunications operators. These gaps, together with the non-functional vetting procedures provided by law lead to the inability of the security institutions to effectively tackle and prevent

[2] Haxha, 2010
[3] One of the cases is reported by: Spiegel Online, 2008

crimes while preserving and protecting the right to privacy[4] as a fundamental human right[5] guaranteed by the Constitution of the Republic of Kosovo.

2. PROBLEMS, STARTING WITH THE DEFINITION

A primary factor that leads to the overall perplexity over the issue of lawful *interception of telecommunications* in Kosovo is the lack of a standard definition in the legislation governing this matter. The Provisional Criminal Procedure Code (PCPC) does not define what the *lawful interception of telecommunications* means or what it refers to; therefore, it is left to be implied. What can be gathered from the PCPC is that the investigations involving telecommunications services are divided into: (1) *metering of the phone calls*, (2) *interception of telecommunications*, and (3) *interception of communications by a computer network*. While it defines *metering of the phone calls* as "obtaining a record of telephone calls made from a given telephone number"[6], it does not define the other two. The other laws governing the activity provide just a general reference on the activity. The law on interception of telecommunications that is currently being drafted provides a definition for *interception* which too fails to provide definitions for and address distinctions between other special investigation measures. Nevertheless, this paper does not analyse the draft law since it is not approved by the Assembly of Republic of Kosovo yet, and substantial changes in it may still be made.

The problem with the lack of having a proper definition of *lawful interception of telecommunications* in Kosovo is that it creates difficulties for the Justice and Security Institutions in taking the necessary measures in crime investigation and intelligence collection, because not all the surveillance measures involving the telecommunications services qualify for interception of telecommunications, nor all such measures have a legal base on current legislation in Kosovo. For example, the police have used *location data*[7] as a telecommunications surveillance measure to locate the suspects who had been charged for kidnapping a 5 year old in March 2011.[8] According to a former high official of a telecommunications operator[9] in Kosovo, the police have acquired *location data* from one of the telecommunications operators. However, the problem with this is that *location data* of the telecommunications subscribers are less than very thinly regulated by relevant laws in Kosovo, therefore, acquisition of *location data* had not be based on any legislation. The authorities issuing the order to acquire *location data* may have interpreted this as *lawful interception of telecommunications*, but using such data goes beyond lawful interception of telecommunications. While interception of telecommunications refers to the interception of content (communications), live or recorded, transmitted through two or more individuals while using telecommunications services (telephone calls, e-mails, messages, etc),[10] the location data refers to the static data (information) such as (location data, traffic data, or personal data).

The lack of proper definition of lawful interception of telecommunications in the relevant legislation affects the quality of investigations and the ability to protect privacy rights.

[4] Const. of the Rep. of Kosovo, Article 36
[5] Const. of the Rep. of Kosovo, Article 53
[6] UNMIK, PCPC, Article 256, Paragraph (10)
[7] Location data is the information provided by the telecommunications operators which can be used to identify an individual's physical location that can also be used to track his/her location changes.
[8] Elezi, 2011.
[9] Interview A, 2011, Prishtina.
[10] Thorogood, 2007.

It is important to differentiate between these measures, because of the level of sensitivity that each of them bears and the consequences that each of them has on the individual's privacy. Acquiring content (communications) between individuals by intercepting their telecommunications, for instance, is much more sensitive than acquiring static data (information) about individuals' location by obtaining *location data.* This in turn has consequences on restrictions applied by law on special investigation measures. For example, the law applies more restrictions on JSIs' orders for *interception of telecommunications* than for *metering the phone calls*, because of the level of sensitivity each of these measures has on individual privacy.

3. RESTRICTIONS ON LAWFUL INTERCEPTION OF TELECOMMUNICATIONS

Not all criminal offences may be investigated by lawfully intercepting telecommunications. The Provisional Criminal Procedure Code outlines different conditions under which various measures of covert surveillance or investigation may be undertaken. The interception of telecommunications may be ordered only if a suspected person has committed "a criminal offence punishable by imprisonment of at least four years"[11] and has committed one or more of 17 other criminal offenses[12] in the furtherance of terrorism or organized crimes. In cases where the suspected person "has committed a criminal offence which is prosecuted *ex officio* or, in cases in which attempt is punishable, has attempted to commit a criminal offence which is prosecuted *ex officio*", the relevant JSIs may order other telecommunications surveillance measures such as metering of the phone calls,[13] but they are not able to order the interception of telecommunications.

Some restrictions applied on lawful interception of telecommunications ensure the protection of privacy rights

This division, according to a high level official at the Kosovo Police[14], is positive, not so much for the quality of investigations, but for the suspected person. Restricting the practice of lawful interception to specific criminal offenses[15] provides guarantees for privacy as an important element of human rights and fundamental freedoms of the suspected person. It prohibits the Kosovo Police and the prosecutors, who would otherwise want to get as much information as they possibly can, from interfering with the privacy of individuals anytime they wish to collect information.[16] While these restrictions are desirable in ensuring that human rights are protected, their rigidity, at least as provided by law, may have various side effects on national security:

- ***Anticipating unintended criminal consequences***: These restrictions do not account for criminal offences which, although they may not qualify to be investigated by lawful interception of telecommunications, they may still have unintended consequences on causing un-anticipated damages or crimes that may qualify for such measure to be used otherwise. There have been cases where these restrictions have greatly endangered national security in the past.[17] For instance, some of the employees at 'Ferronikeli' plant had threatened the high level management that unless they paid the racketeering fee put forth to them they would

[11] UNMIK, PCPC, Article 257, Paragraph (3); Subparagraph 1); (i)
[12] UNMIK,PCPC, Article 257, Paragraph (3); Subparagraph 1); (ii)
[13] UNMIK,PCPC, Article 257, Paragraph (1); Subparagraph 1)
[14] Interview B , 2011, Prishtina
[15] UNMIK,PCPC, Article 257, Paragraph (3); Subparagraph 1); (ii)
[16] Interview B, 2011, Prishtina
[17] Marmullaku, 2011, Prishtina

destruct the main electricity transmission line at the plant. Since the prosecutor and the police had qualified this blackmailing activity as 'a threat', which is an offense not punishable by imprisonment of more than four years, the pre-trial judge had not approved the order for intercepting the telecommunications of the suspects. The problem with this, according to the former high official at the Kosovo Police[18] was that, had this threat been allowed to be executed based on how the suspects had planned it, the damages caused would have been difficult to repair because severe damages would have been caused to the overall electricity transmission line. This has led the police to change the approach to the offense by qualifying it as punishable by imprisonment of more than four years, so that they could obtain the approval by the pre-trial judge to intercept the telecommunications of the suspects. This in the end has led to the identification of the right persons among the employees involved in this blackmailing activity.

- ***Judicial control****:* The Provisional Criminal Procedure Code states that when making an application for interception, one of the things that should be mentioned in the application, among other things, is "a complete statement of the facts, relied on by the applicant to justify his or her belief that the relevant criteria in Article 257 [in the PCPC][19] are satisfied"[20] so that the relevant judicial authority (a judge or a court), can assess whether or not interception of telecommunications is a necessary measure for investigating a particular criminal offense. This seems to provide a balance between judicial control (concerned with protecting human rights) and executive control (concerned with collecting information and initiating criminal proceedings) during investigations. However, while this balance is necessary to be maintained, the inefficient judicial sector in Kosovo may be unable to identify the extent to which an actual criminal offense may be considered a threat to national security.
- ***Efficiency*****:** Providing a rigid restriction will also make the JSIs unable to take preventive measures. There may be criminal offences that do not qualify for being investigated by lawful interception of telecommunications, but which could expand into more major offenses. Thus, in some cases information that may be acquired by lawful interception of telecommunications may be vital to preventing some criminal offenses from expanding.

The Law on the Kosovo Intelligence Agency (KIA) on the other hand does not provide any restrictions on lawful interception of telecommunications based on criminal offenses. This is partly because according to the aforementioned law, the KIA does not have the power of either arresting or initiating criminal proceedings against someone;[21] its scope primarily concerns information and intelligence gathering in regards to the threats to "the territorial integrity, integrity of the institutions, the constitutional order, the economic stability and development, as well as threats against global security."[22] So, the KIA, upon the approval of relevant authority, may initiate lawful interception of telecommunications in order to fulfil its duties and responsibilities as stipulated by the law on the KIA.[23] The legislative analysis thus far, however, could not identify whether or not the information gathered by the KIA can be used as evidence in the court against a suspect.

[18] Marmullaku, 2011, Prishtina
[19] Information in squared brackets hereinafter is in-text intervention by the author of this paper.
[20] UNMIK,PCPC, Article 258, Paragraph (3); Subparagraph 2)
[21] Rep. of Kosovo, Law on KIA, No. 03/L-063, Article 3, Paragraph 3.1
[22] Rep. of Kosovo, Law on KIA, No. 03/L-063, Article 2, Paragraph 2.1
[23] Rep. of Kosovo, Law on KIA, No. 03/L-063

4. MIXED AUTHORITY AND THE NEED TO DEFINE OWNERSHIP (EXPLICITLY)

The authority over who may order lawful interception of telecommunications is somewhat stretched over different judicial bodies within domestic and international structures in Kosovo. Under the Provisional Criminal Procedure Code, the interception of telecommunications may be issued by a pre-trial judge on the basis of an application by a public prosecutor.[24] Moreover, in cases where more than one telephone or nodes need to be intercepted, the order may be issued by a three-judge panel of a District Court.[25] Additionally, the Law on the KIA gives the right to the Supreme Court Judge, on the "written application made under oath and approved by the KIA Director or the Deputy KIA Director", to authorize the KIA employees to carry out the surveillance of telecommunications as referred to by the Law on the KIA.[26]

In addition to the authorities under the domestic structure of the security sector, EULEX is the authority under the international structure of the security sector in Kosovo that has to ensure that criminal offenses such as, but not limited to, organized crime, corruption, and war crimes are "properly investigated according to the law […] by international investigators"[27]. Although this implies that they can order the interception of telecommunications the research for this study has not led to any explicit references pertaining to this issue.

The stretched authority over different bodies in issuing orders for this measure of investigation may be necessary; however the lack of proper cooperation and information sharing mechanisms between and over these different authorities may inhibit the quality and swiftness of investigations. There appears to be no clear rules which establish grounds for cooperation between the JSIs within the domestic security structures (i.e. within the Kosovo Police or between Kosovo Police and KIA), as well as between the domestic JSIs and international JSIs (i.e. between the KIA and EULEX). Only few provisions in the current legislation provide some clues in this regard. Article 266 of the PCPC provides that "the judicial police [which does not exist] may, where appropriate, seek the assistance of other authorities responsible for maintaining law and order and a secure environment in Kosovo in connection with the implementation of [lawful interception of telecommunications]."[28] Moreover, Article 8, paragraph 8.3 on the Law on the KIA stipulates that "the KIA and other bodies and institutions in Kosovo shall be obliged to mutually cooperate and assist one another in performing their duties and shall coordinate activities within their competence, consistent with the applicable laws and regulations regarding the protection of sources, methods and other classified information."[29] These are the provisions that get closest to providing legislative base in establishing cooperation mechanisms between various JSIs, which, as it is evident, remain very vague.

These provisions, moreover, do not prevent the overlap of responsibilities and duties from happening among different security actors. For instance, the former high official in the investigation unit at the Kosovo Police[30] describes how the lack of cooperation between the investigation units in different

[24] UNMIK, PCPC, Article 258, Paragraph (2); Subparagraphs 4) and 5)
[25] UNMIK, PCPC, Article 259, Paragraph (6)
[26] Rep. of Kosovo, Law on KIA, No. 03/L-063, Article 28, Paragraph 28.1
[27] Compr. Prop. for the Kosovo Stat. Settl., Annex IX, Article 2, Paragraph 2.3, Subparagraph (a)
[28] UNMIK, PCPC, Article 266
[29] Rep. of Kosovo, Law on KIA. No. 03/L-063, Article 8, Paragraph 8.3
[30] Marmullaku, 201, Prishtina.

regions within the Kosovo Police (i.e. between Peja and Prishtina) has led the investigators in both regions to request the interception of telecommunications of the same person at the same time for the same case to be carried out. Had there been some sort of 'central information system' or a 'centralized flagging system' whereby the police can share any necessary information regarding their investigations and their suspects, this overlap of responsibilities would not have occurred.

In terms of potential overlaps between the activities of local and international JSIs, there are some attempts that have been made in an effort to minimize the overlaps between these JSIs. According to an EULEX official,[31] there is a 'joint investigation team' which is supposed to coordinate the activities between the Kosovo Police and EULEX. While the joint investigation teams may be effective in preventing potential overlaps, it appears that these joint teams are not active in all cases. Some of the investigations are still conducted separately and independently by local (the Kosovo Police) and international (EULEX) authorities, which in some cases proved to be ineffective. For instance, when independent investigations have been conducted separately by local and international authorities, it has led the investigation units of both authorities to interfere in each other's attempts to investigate the same case. This in practice has led for a suspect to be arrested while the other unit had been in the process of intercepting telecommunications of the same suspect in their effort to gather yet more information.[32]

The lack of clear ownership over lawful interception of telecommunications in Kosovo significantly hinders the quality of investigations

One of the causes of having an independent hand and no permanent cooperation between the different Justice and Security Institutions in Kosovo is the fact that the local and international JSIs have independently signed the agreements with the telecommunications operators for this matter.[33] This has allowed for some complaints to be addressed towards the EULEX for intercepting telecommunications without any coordination with local security authorities. In a recent attempt to seize control of the two border crossings in northern part of Kosovo, the Minister of Interior, Bajram Rexhepi, has been criticized by the relevant parliamentary committee for ordering the operation only two hours before it had occurred. The Minister reiterated that he had to keep the operation secret because his conversations with the Prime Minister have been continuously intercepted, so disclosing the information about the operation earlier, would have compromised the operation, because allegedly the international community would have reacted against the operation. He finger pointed first at the United Nations Mission in Kosovo (UNMIK) and then at EULEX, as those responsible for intercepting his telecommunications for many years now.[34] While the rules on cooperation between the domestic and international security actors are not explicitly known, the EULEX has claimed that they follow the same procedures provided by the PCPC and the procedures that the local actors follow.[35] When asked about this case, the Chief Prosecutor of the Republic of Kosovo, said that "the Minister could press charges, in which case the Prosecutor's Office will act according to the law; however, he claimed that the international community has immunity [over these issues]."[36]

[31] Interview D, 2011, Prishtina
[32] Marmullaku, 201, Prishtina.
[33] Haxhiu and Kostanica, Klan Kosova, 2010 (At the time, Ipko was still in the process of negotiating these agreements (still separately) with local and international JSIs.
[34] Kajtazi, 2011.
[35] Interview D, 2011, Prishtina. See also: Kajtazi, 2011.
[36] Kabashi 2011.

Therefore the security environment in Kosovo which is characterised by the presence of multiple security actors with mixed and overlapping mandates as well as poor mechanisms of cooperation when carrying out interception of telecommunications greatly hinders the quality of investigations and protection of privacy rights.

5. PROCEDURES

5.1. The process

The procedure for lawful interception of telecommunications in Kosovo seems to depend on the legislation regulating the measure. There is no standard procedure for interception. Under the Provisional Criminal Procedure Code, after having made an application with the relevant authorities, the public prosecutor or the duly authorised judicial police (DAJP) officers receive an order with the relevant information which includes[37]:

1. The name and address of the subject or subjects of the order;
2. The nature of the measure;
3. The grounds for the order;
4. The period within which the order shall have effect, which shall not exceed 60 days from the date of the issuance of the order; and
5. The agency of the judicial police authorized to implement the measure and the officer responsible for supervising such implementation.

Then, this order shall include as an annex a separate written instruction addressed to persons other than the DAJP officers whose assistance may be necessary for the implementation of the order, in this case "the director or the official in charge of the telecommunications system, computer network, […] and shall specify only the information, which is required for assistance in the implementation of the order."[38]

It is difficult to know the role of the assisting personnel of the telecommunications operator on this matter; however, according to the former high official[39] at Ipko Telecommunications, the person involved in this activity has a separate office at the premises of the operator and her/his identity or her/his job description is not revealed among other staff within the telecommunications operator. This seems to be the case with the PTK as well, whose managing director, Shyqri Haxha, has stated that none of the employees of the operator have access [to the secure location] where only a confidential team who professionally execute the orders without interference from PTK management are involved."[40] However, little is known about whether or not the personnel employed at the telecommunications company who is involved in assisting the justice and security authorities have gone through vetting procedures.

5.2. Emergency cases

The ordering of lawful interception of telecommunications in case of emergency differs depending on the law. According to the Provisional Criminal Procedure Code "in emergency cases, if the delay that

[37] UNMIK, PCPC, Article 259, Paragraph (1)
[38] UNMIK, PCPC, Article 259, Paragraph (8)
[39] Interview A, 2011, Prishtina.
[40] Haxha, 2010.

would result from a pre-trial judge issuing an order […] would jeopardize the security of investigations or the life and safety of an injured party, witness, informant or their family members, a public prosecutor may issue a provisional order for one of the measures provided for in paragraph 2 of the [Article 258]. Such provisional order ceases to have effect if it is not confirmed in writing by a pre-trial judge within twenty-four [24] hours of issuance."[41] According to the Law on the Kosovo Intelligence Agency, however, in an emergency situation, "when time does not permit the preparation of a written application by the KIA Director or the Deputy KIA Director or the granting of a written order by a Supreme Court Judge, the application may be made and the order for covert surveillance granted orally, to be confirmed in writing within forty-eight (48) hours."[42] Although a collision between the PCPC and the law on the KIA exists in regulating the operating period of provisional orders; a huge concern remains with monitoring the emergency cases especially in making sure that provisional orders cease to have effect as provided by law.

5.3. Safeguard mechanisms

The PCPC outlines some mechanisms for safeguarding the information and privacy of individuals. One such provision is that the interception of telecommunications is allowed to be carried out only if "the information that could be obtained by the measure to be ordered would be likely to assist in the investigation of the criminal offence and would be unlikely to be obtained by any other investigative action without unreasonable difficulty or potential danger to others."[43] Another safeguard provided by the PCPC is the provision stating that the "evidence obtained by [interception of telecommunications] shall be inadmissible, if the order for the measure and its implementation are unlawful."[44] Moreover, "the period within which the order shall have effect, which shall not exceed 60 days from the date of the issuance of the order"[45] is another provision under the PCPC that serves as a safeguard. If the above provisions are breached, or if the subject's telecommunications have been intercepted unlawfully, a 'Review Panel' shall compensate the subject, terminate the order, and order the destruction of the materials.[46]

There are some safeguard mechanisms in place provided by the current legislation that protect the information and privacy of individuals

The restrictions provided by the law on the KIA to the KIA employees, also serve as a safeguard mechanism. The KIA does not enjoy executive functions and shall not: "(1) have the right to use direct or indirect force; (2) have any power of arrest; (3) be able to initiate criminal proceedings; and (4) have power to compel persons or companies to cooperate with their activities, though persons or companies may cooperate with the KIA on a voluntary basis."[47]

5.4. Control and monitoring mechanisms

Kosovo has established relevant parliamentary committees to oversee the security sector in order to guarantee civilian and democratic control over security institutions, as stipulated in the Constitution of the Republic of Kosovo.[48] There are two functional parliamentary committees that oversee the security sector in Kosovo: the Committee on Internal Affairs, Security and Supervision of the Kosovo

[41] UNMIK, PCPC, Article 258, Paragraph (4)
[42] Rep. of Kosovo, Law on KIA, No. 03/L-063, Article 29
[43] UNMIK, PCPC, Article 257, Paragraph (1) and (3), subparagraphs 2)
[44] UNMIK, PCPC, Article 264, Paragraph (1)
[45] UNMIK, PCPC, Article 259, Paragraph (1), Subparagraph 4)
[46] UNMIK, PCPC, Article 265
[47] Rep. of Kosovo, Law on KIA, No. 03/L-063, Article 3, Paragraph 3.1
[48] Const. of the Rep. of Kosovo, Article 125

Security Force; and the Oversight Committee for Kosovo Intelligence Agency. There are no strict obligations provided under these two committees to control and monitor lawful interception of telecommunications. Nonetheless, the Law on Parliamentary Investigation provides the legislative base for Investigation Committee to be created which can "investigate problems, issues that involve directly the responsibilities of the Government or State."[49] This Committee may also summon "the holders of public functions to be heard before the Committee"[50] within its mandate. However, while this law gives the Committee the mandate to investigate various cases, which may include cases pertaining to interception of telecommunications, it does not give the Committee explicitly the mandate to control and monitor such activities.

While the PCPC does not provide any details on the democratic, or any other, oversight and monitoring mechanisms, the law on the KIA provides several provisions in this regard. The activities of the KIA are supervised by the Oversight Committee for the KIA of the Assembly of the Republic of Kosovo, which among other things is responsible for "overseeing the legality of the work of the KIA; reviewing reports from the KIA Director regarding the operations and expenditures of the KIA; reviewing reports from the Inspector General; conducting inquiries regarding the work of the KIA, and alike"[51]

As far as the independent bodies are concerned, the complaints concerning the domestic institutions may be addressed to the Ombudsperson, as provided by the law on the KIA,[52] however the Ombudsperson, as an independent institution, does not have the mandate to oversee and control the measures of investigations, lawful interception in particular, that the Kosovo Police, the KIA, and EULEX carry out. While the Ombudsperson has the mandate to deal with the domestic institutions, the EU, for instance, has established an independent monitoring body, the Human Rights Review Panel, in order to oversee the overall EULEX accountability. This body overseas the EULEX Internal Investigation Unit and the EULEX Third Party Liability Insurance Scheme while reviewing complaints submitted over potential EULEX violations of human rights.[53]

The Ombudsperson, as an independent institution, does not enjoy the mandate to oversee and control lawful interception of telecommunications that the Kosovo

There seems to be no indication of the existence of a formal internal inspection and monitoring mechanisms within the Justice and Security Institutions in carrying out lawful interception. The PCPC obliges the Duly Authorised Judicial Police officers to "make a record of the time and date of the beginning and end of each action undertaken in implementing the order. [Moreover it states that] the record shall state the names of the [DAJP officers that have] carried out each operation and the functions they performed."[54] However, there seem to be no mechanisms, either provided by law or implemented in practice, whereby the judiciary (judges and courts) take the responsibility on overseeing the overall implementation of the order on the one hand, and some sort of internal inspection within the JSIs which would oversee the activities of all parties involved in the whole process of interception of telecommunications on both sides the JSIs and the telecommunications operators on the other hand.

[49] Rep. of Kosovo, Law on Parliamentary Investigation, No. 03/L-176, Article 2, Paragraph 2
[50] Rep. of Kosovo, Law on Parliamentary Investigation, No. 03/L-176, Article 13, Paragraph 1.1
[51] Rep. of Kosovo, Law on KIA, No. 03/L-063, Article 36. See also Articles 37 and 38 under the same law
[52] Rep. of Kosovo, Law on KIA, No. 03/L-063, Article 39, Paragraph 39.2
[53] Human Rights Review Panel, 2011.
[54] UNMIK, PCPC, Article 260, Paragraph (4)

6. HUMAN RIGHTS ISSUES

Lawful interception is often believed to be a mistrusted measure of investigation, at least among the public, because they believe it violates one of their essential human rights, which is the right of privacy. The Provisional Criminal Procedure Code attempts, with its relevant provisions describing the scope, the procedure, and the rights of various parties involved in interception of telecommunications, to protect the fundamental human rights and freedoms. For example, there are two essential elements that the subjects being intercepted enjoy under the PCPC:

6. The right to access the collected materials as a result of an order to investigate the subject;[55] and
7. The right to be promptly informed by the public prosecutor (when there is no grounded suspicion) about the order to investigate him or her.[56]

However, there are still some gaps that remain in protecting human rights. For example, in stating that the "implementation of an order shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception"[57], the PCPC gives the JSIs the flexibility to intercept individuals other than the suspects. This is because instead of completely restricting the interception of communications not otherwise subject to interception, the PCPC just asks to "minimize" such practice.

Additionally, there is another element of potential breach of rights of privacy with the order (annex) that is sent to the telecommunications operators by the JSIs. Although this annex, which is handed over to the telecommunications operators to execute the order does not include the identification of the person under investigation, as mentioned earlier, the new Telecommunications Regulatory Authority (TRA) regulation for registration of the mobile phone numbers[58] make the order (annex) more susceptible to breaching privacy rights. This new regulation obliges all physical and legal persons to register their full names and other personal details including their address with their SIM Cards (phone numbers). In other words there shall be no SIM Cards (phone numbers) without designated ownership. In this respect, when the Justice and Security Institutions hand over the annex to the telecommunications operators in which the phone number of the suspected person is included as an essential information to execute the order for interception, the phone number can easily be traced to the identification of the person and his/her address, due to the implementation of the new TRA regulation. So, the PCPC's provision for not disclosing the identity of the suspected person when issuing the annex in this case is void.

The new TRA regulation for registration of the mobile phone numbers makes the overall process of lawful interception of telecommunication susceptible to breaching privacy rights.

[55] UNMIK, PCPC, Article 263, Paragraph (1), Subparagraphs 1)
[56] UNMIK, PCPC, Article 263, Paragraph (1), Subparagraphs 2)
[57] UNMIK, PCPC, Article 260, Paragraphs (2)
[58] Rep. of. Kosovo, TRA Regulation, No. 3. See also: TRA Decision, No. Prot. 015/B/11

Another important problem in regards to privacy remains with the translation of the intercepted records. According to an employee at the procurement,[59] during the UNMIK administration, the local translators have been involved in translating the intercepted materials to and from Albanian, Serbian, and few other languages. There is little information in regards to whether or not the translators have had clearance from the police; nevertheless, this practice raises concerns about the ability of the international JSIs to protect the privacy of, not only the suspects, but of the individuals that were communicating with the suspects as well. Although there have been (in that case) some safeguard mechanisms whereby the authorities have divided the materials to be translated, so that the translators would not understand the whole story, the translators are still exposed to substantial amount of information. Similar to UNMIK, when EULEX intercepts telecommunications nowadays, it has to engage local translators in translating the intercepted materials. In this respect, although the law on Classification of Information and Security Clearances has been approved, the special vetting department which should have been established by the KIA, as stipulated in the respective law,[60] is not operational yet.[61] This makes it impossible for international security actors, in this case EULEX, to conduct security clearance procedures for the individuals involved in translating the intercepted materials.

Local translators who are engaged in translating the intercepted materials for the international security actors may not go through the security clearance as provided by law.

While the PCPC does not provide anything explicitly related to the protection of human rights and fundamental freedoms, the law on the KIA does provide such provisions. The law states that "the KIA shall respect the principles and carry out its activities in accordance with the Universal Declaration on Human Rights, the International Covenant on Civil and Political Rights, the European Convention for the Protection of Human Rights and Fundamental Freedoms, and other relevant principles reflected in internationally recognized legal instruments,[62] which are not provided therefore by the PCPC.

7. TELECOMMUNICATIONS OPERATORS

The continuous advancements in the telecommunications industry are enabling people in Kosovo to use a wide range of telecommunications services. There is a steady growth among users of mobile services, internet, and other telecommunications services. According to the Telecommunications Regulatory Authority, there are 48 telecommunications operators that have at least one telecommunications services license issued by the TRA,[63] which are subject to orders for interception of telecommunications. Among these there are only three fixed line operators, two mobile operators, and two Mobile Virtual Network Operators (MVNOs). Most of the other licensees are internet service providers (ISP) and valued added services (VAS) providers.[64] These advancements in both the usage and the number of services in the telecommunications industry unavoidably increase the many ways the JSIs may have to intercept telecommunications.

The telecommunications operators play a vital role in protecting and guaranteeing individual privacy, not least, because they provide the human and technical resources for successful lawful interception of

[59] Interview C, 2011, Prishtina.
[60] Rep. of Kosovo, Law on KIA, No. 03/L-178, Article 24, Paragraph 2
[61] KCSS, et. al., Progress Report Made in Kosova, 2011.
[62] Rep. of Kosovo, Law on KIA, No. 03/L-063, Article 2, Paragraph 2.4
[63] Rep. of Kosovo, TRA, 2011.
[64] Rep. of Kosovo, TRA, 2011.

telecommunications, as well as they are the warehouse of sensitive and personal data of their customers. However, with this in mind, when looking at current legislation pertaining to lawful interception of telecommunications as well as regulations on telecommunications in general, there seems to be very little provided in standardizing and managing the interaction between the JSIs and the telecommunications operators.

First of all, the JSIs orders have not been handled consistently; the telecommunications operators have not always responded to the orders brought in by the JSIs. For instance, it was not until very recently (est. 2010) that the JSIs could practically intercept telecommunications of Vala[65] subscribers only, when Ipko began to follow suit.[66] This has made some Vala customers to switch operators out of fear of being intercepted. Accordingly, some have interpreted Ipko's unwillingness to allow the JSIs to intercept its customers as providing safe havens for potential suspects. In PTK director's words "we have many cases where our customers, afraid of being intercepted, ran away from us and the other operator has enjoyed benefits out of this."[67] The competent official at Ipko on the other hand, claimed that they have strictly acted in accordance with the Criminal Procedure Code.[68]

The telecommunications operators have not always responded to the orders brought in by the security institutions.

Second, the capacities and capabilities of the telecommunications operators to execute the Justice and Security Institutions' orders vary. In executing its orders with PTK, for instance, the JSIs have been provided access to full customer database (enabling the JSIs to intercept other numbers as well); thus, expositing a wide range of unnecessary customer data to the JSIs, which in turn has provided space for abuse by the parties involved. It is difficult to confirm whether or not the PTK's case is true, but according to a former high official at the police,[69] there used to exist a possibility with PTK to have access to their entire customer database. This, according to some telecommunications experts, is due to the lack of technical capability to provide access restrictions to JSIs. There appears to be some changes in place at the PTK, and there are indications that such practices do not take place anymore. Ipko, on the other hand, seems to have been more capable in protecting individual privacy, because according to the competent representative at Ipko, the technical specificities provided by them prevent any abuse to occur on this matter.[70]

There appears to be a lack or no mechanisms of inspection of telecommunications operators. The safeguards mechanisms and even the narrow control and monitoring mechanisms that exist on the JSIs side, are not present on the side of telecommunications operators at all. There seems to be no inspection that the telecommunications operators, and the relevant employees thereof, undergo in making sure that the lawful interception interface and the overall system is not misused for personal or other reasons. There seems to be examples in the past where the system has been misused on the side of the telecommunications operators. Some of the Vala employees assert that today no one at PTK carries out unlawful interception, although, cases of misuse have been reported in the media where

Some of the telecommunications operators' infrastructure has shown to be incompatible with the legislative requirements to protect customer data and privacy rights.

[65] Vala is the mobile operator subsidy under PTK
[66] Kosova Sot, 2010.
[67] Haxha, 2010.
[68] Kostanica, Klan Kosova, 2010
[69] Marmullaku, 2011, Prishtina.
[70] Kostanica, Klan Kosova, 2010

employees of PTK have claimed that there were cases in the past where un-authorized interception of telecommunications has been ordered by the previous managing team. [71]

8. A TALE OF SHADOWY ACTORS

The presence of a large number of actors involved in the interception of telecommunications from domestic and international Justice and Security Institutions to the telecommunications operators and the lack of cooperation between them is not the only concern. So far, there has been a considerable presence of various information and intelligence actors in Kosovo. According to a report,[72] the Kosovo Information Service (SHIK)[73] and the Institute for Strategic Research of the Public Opinion (IHSOP)[74] have been operating for a while, at least for the larger part of the period after the war; however, little is known about whether or not they have possessed and continue to possess capabilities for intercepting telecommunications. Nevertheless, their recent dismantling[75] leaves less room to be concerned about their still alleged existence, but more room to be concerned about the aftermath of their capabilities and capacities.

There is another (active) shadowy side of the current telecommunications infrastructure set-up in Kosovo. Kosovo continues to use Serbia's country code (+381) for its fixed line services, which opens some doors to numerous concerns about national security. All the incoming fixed line calls to Kosovo go through the central telecommunications switches in Belgrade and are then diverted to Prishtina. According to an expert on the field and a former employee at one of the telecommunications operators, Serbian authorities may, as they wish, monitor, register, and intercept any calls made to any of the subscribers in Kosovo.[76] Additionally, a current high official at the Kosovo Police who seemed to understand the technical side of the interception has affirmed the possibility for Serbia to be able to intercept international incoming calls to Kosovo. "Technically you can do that, and it is not difficult; we may never know it, but the possibility exists."[77] So, this seems to be more a matter of will rather than a matter of capability from the Serbian side. If this is a matter of will for Serbia, than the status quo on this issue is a matter of trust for Kosovo; do the governing institutions in Kosovo believe that the current international telecommunications interconnection set-up is free from abuse by Serbia? Considering the fact that there are more than 80,000 fixed line users in Kosovo[78] as well as the fact that the vast majority of local and international governing institutions use fixed lines to receive calls from abroad, it provides enough room for security concerns. Little is known about the usage pattern of the fixed lines by high officials in Kosovo, be that in their office or at home, but this issue deserves a detailed research and study.

Do the governing institutions in Kosovo believe that the current fixed-line international telecommunications interconnection set-up is free from abuse by Serbia?

In addition to security concerns provided by the current international interconnection set-up on the fixed line, the wide presence of Serbian mobile infrastructure in Kosovo can be considered a threat to

[71] Ekonomisti, 2011.
[72] Peci and Dugolli, 2006.
[73] Acronym in Albanian: Shërbimi Informativ i Kosovës
[74] Acronym in Albanian: Instituti për Hulumtime Strategjike të Opinionit Publik
[75] Ekonomia, n.d.
[76] Interview A, 2011, Prishtina.
[77] Interview B, 2011, Prishtina.
[78] Rep. of Kosovo, TRA, 2011, p.6

national and public security in many different levels. Most of the Serbian majority areas in Kosovo are covered with mobile telephony infrastructure of the Serbian operators, allowing a considerable number of people to use illegal mobile services in Kosovo. This makes both the domestic and the international Justice and Security Institutions in Kosovo unable to intercept telecommunications of around 120,000 people using illegal mobile services.[79] Moreover, the presence of illegal Serbian infrastructure in Kosovo may also provide safe havens not only for the Serbian population, but for the other part of population either passing by or living close by the areas where the Serbian operators have coverage. Therefore, interception of telecommunications, as an effective special investigation measure, may not be carried out for a considerable number of populations in various parts of the territory of Kosovo.

9. POLICY OBJECTIVES

The following are the main policy objectives that aim at addressing the concerns raised throughout this paper:

- Find the desired balance between ensuring state and public security on the one hand, and protecting and guaranteeing fundamental human rights and freedoms on the other;
    - Guarantee the right to privacy;
    - Boost state and public security in a multitude security actor environment;
- Enhance the cooperation between different Justice and Security Institutions within the domestic security sector and between the domestic and international security actors;
- Enhance, democratic, independent, and internal control and oversight mechanisms;
- Advance the regulation of the activities of the telecommunications operators in the area of cooperation with the JSIs and that of data retention and protection.

10. POLICY RECOMMENDATION

The following are the policy recommendations for the relevant institutions of the Republic of Kosovo on several policy levels:

Legislation

1. Upgrade the Provisional Criminal Procedure Code, the law on the Kosovo Intelligence Agency, the law on telecommunications, and any forthcoming law that pertains to matters of interception of telecommunications, to provide a clear definition of and a distinction between:
    - Interception of telecommunications, which it shall refer to the *content* of communications, either real-time or recorded
    - Traffic data, location data, and personal data, which it shall refer to events and static data obtained by the telecommunications operators on their customer's telecommunications services usage patterns.
    - Data retention, which it shall refer to the terms on data protection and storage

    These distinctions are paramount in managing the restrictions set for interception of telecommunications in order to protect privacy rights. I.e. it shall be more flexible and easier

[79] PC-World, 2010

for the JSIs to access static data (traffic, location, and personal data), and more restrictions shall apply to accessing content (real-time or recorded communications);

2. The relevant law, which could be the current draft law, shall be upgraded to include detailed provisions on standardizing the procedures of cooperation between all the JSIs Justice and Security Institutions (authorized to intercept telecommunications) and all the telecommunications operators licensed by the Telecommunications Regulatory Authority.

3. Provide deadlines by when the telecommunications operators shall respond to orders issued by relevant JSIs;

4. Fines and other measures should be introduced in cases where the telecommunications operators do not follow orders issued by the authorized body. There should be three stage working mechanism, whereby the first two warnings for non-cooperation shall be associated with fines in progressive terms from first to second one; the second fine being more expensive than the first. The third warning for non-cooperation shall be associated with punishable measure as outlined in the PCPC.

5. The relevant legislation should provide provisions that would allow for more resilient utilization of interception of telecommunications in cases where this measure is prohibited as provided in Article 257 of the PCPC, while making sure that the human rights and freedoms are guaranteed and protected.

Overall procedure

6. Two mechanisms of cooperation between the Justice and Security Institutions should be introduced and enhanced. First, there should be an online 'central information system' accessible by all the JSIs which will serve as a central point for the JSIs and will flag any attempts to overlap the interception of the same person. This will help in clarifying ownership of the case and the measures used to investigate the case. Second, the 'joint investigation team' should be enhanced in including all the JSIs.

7. Enhance the democratic oversight of the interception of telecommunications by explicitly extending the responsibilities of an existing parliamentary committee to inspect the activities of the JSIs in intercepting telecommunications. This should oversee all the JSIs (currently: Kosovo Police, KIA, and EULEX), as well as all the telecommunications operators in Kosovo. This inspection body should have full immunity in accessing all premises and instruments of the parties involved in interception of telecommunications and it should possess the expertise to inspect such activities;

8. The mandate of Ombudsperson shall be extended to cover (control and monitor) all the JSIs and all their measures of surveillance and investigations, including interception of telecommunications.

Justice and Security Institutions

9. Expand the interception of telecommunications beyond the two telecommunications operators and mobile services to include other dozens of telecommunications operators;

10. Create a committee of experts to discuss and propose the course of actions to be taken for switching the country code from +381 to codes of other partner countries.

BIBLIOGRAPHY:

Interviews

Interview A. Former high official at the telecommunications company. 20 October 2011. Prishtina

Interview B: High official at the Kosovo Police. 22 October 2011. Prishtina

Interview C: Employee at UNMIK procurement. 22 October 2011. Prishtina

Interview D: Official at EULEX. 26 October 2011. Prishtina

Marmullaku, Rifat. Former high official at the Kosovo Police. 22 October 2011. Prishtina

Legal Documents

Constitution of the Republic of Kosovo. 2008.

Republic of Kosovo, Law on the Kosovo Intelligence Agency, No. 03/L-063. 2008.

Republic of Kosovo. Law on Parliamentary Investigation, No. 03/L-176. 2010

Republic of Kosovo. TRA Decision, Nr. Prot. 015/B/11

Republic of Kosovo. TRA Regulation, Class 01/1, Reg.No. 3. 2010

UNMIK. Provisional Criminal Procedure Code. 2003.

UNSC. Comprehensive Proposal for the Kosovo Status Settlement. 2007.

Other sources

Ekonomia. "E vërteta mbi SHIK-un kërkohet nga AKI-ja." n.d. http://www.ekonomia-ks.com/?page=1,5,5628

Ekonomisti. "Sa përgjohemi?." August 22, 2011. http://www.ekonomisti.net/artikulli/4/0/20670/sa-pergjohemi/

Elezi, Valmir. "Prishtinë, gjendet fëmija i rrëmbyer." TV News Report. *Top-Channel*. March 3, 2011. http://www.balkanweb.com/notizia.php?IDNotizia=57231

Haxha, Shyqri. "?Ipko?, bisedime me policinë për përgjimet." *Kosova Sot*, September 6, 2010. http://www.kosova-sot.info/ekonomi/ipko-bisedime-me-policine-per-pergjimet

Haxhiu, Baton. "Me Merita Kostanica." Zona B. Klan Kosova. September 26, 2010. http://klankosova.tv/index.php/zona-b/5624-me-merita-kostanica.html

Human Rights Review Panel. Accessed on 7 October 2011. http://www.hrrp.eu/

Kabashi, Ismet. "*Kabashi - Rexhepit, bëjë kallëzim penal, por ndërkombëtarët kanë imunitet*." *Bota Sot*. 2011. http://www.botasot.info/def.php?category=3&id=137001

Kajtazi, Vehbi. “Minisrti Rexhepi thot se se është nën përgjim nga viti 2002.” *Koha Ditore*. September 14, 2011.

KCSS, et. al. “Raporti i Progresit: Made in Kosova.” October 10, 2011. http://qkss.org/new/images/content/PDF/raporti-shablon-design-english.pdf

Kosova Sot. “?Ipko?, bisedime me policinë për përgjimet.” September 6, 2010. http://www.kosova-sot.info/ekonomi/ipko-bisedime-me-policine-per-pergjimet

Kostanica, Merita. “Me Merita Kostanica.” Zona B. Klan Kosova. September 26, 2010. http://klankosova.tv/index.php/zona-b/5624-me-merita-kostanica.html

Mellon, Jerome. “Understanding Intelligence in a Kosovo Context.” Safe World, May (2007). http://cv.jmellon.com/swgi.pdf

PC-World. “Operatorët e palicencuar dëmtojnë shitjen e Telekomit të Kosovës.” March 30, 2010. http://www.pcworld.al/lajmet/1992-Operatort-palicencuar-dmtojn-shitjen-Telekomit-Kosovs.html

Peci, Lulzim and Dugolli, Ilir. “Intelligence Agencies of Kosovo: Dismantling, Osmosis, or Integration.” Policy Brief Series: paper #2. *KIPRED*: Pishtinë, 2006.

Republic of Kosovo, TRA, Pasqyrë e Tregut të Telekomunikacionit, K4-2010, Prishtinë, April 2011. http://www.art-ks.org/repository/docs/Pasqyre%20e%20tregut%20te%20telekomunikacionit%20K4%20-%202010.pdf

Spiegel Online International. “Spy Scandal:German Intelligence Officers Detained in Kosovo.” November 24, 2008. http://www.spiegel.de/international/europe/0,1518,592298,00.html

Thorogood, Rupert and Brookson, Charles. “Lawful Interception” 2007. *Telektronikk*, Febryary (2007) http://www.telektronikk.com/volumes/pdf/2.2007/Page_033-036.pdf

Kosovar Centre for Security Studies (KCSS)
Rr. Qamil Hoxha, 2-2
Prishtina 10000
Kosovo

Email: **info@qkss.org**
Web: **www.qkss.org**
Tel.Fax: **+381 38 221 420**