Interceptions of Communications in Albania: Legislation, Practice and Accountability System

Center for the Study of Democracy and Governance

Authors
Arjan Dyrmishi

September 2018

Disclaimer and Acknowledgement:
This policy paper is supported by the Friedrich-Ebert-Stiftung. The opinions expressed herein are solely those of the author and do not represent the official standpoint of the Friedrich-Ebert-Stiftung.

Executive Summary

Since 2005 Albanian authorities have been able to use digital technology to conduct lawful interception of multiple targets and multiple communication devices. This trend has been driven by the need to keep up with effective investigation of crime, as the technology in the field of telecommunications has constantly developed. However, the effectiveness of such policy remains questionable as pointed out on several reports of the Prosecutor General to the parliament.

While the law has been amended several times to allow for the increased effectiveness of the interceptions, the system for the control and oversight of the adequacy of the implementation of the legislation that regulates the electronic surveillance regime has remained underdeveloped. Over the last decade there have been a number of allegations on unlawful interceptions conducted by different institutions but no action has been taken to improve the existing accountability mechanisms.

The lack of effective control and oversight has seriously damaged the legitimacy of the use of such investigative procedure, as evidenced by the lack of trust displayed publically by the highest public and political figures of the country. The latest amendments of the law on interception and the Code of Penal Procedure in 2017 provide for an expansion of the interception competences and the increased use of such procedure through the development of multiple intercepting capabilities.

In the conditions of the lack of effective accountability system there is a risk abuse of competences and powers and of encroachment on the fundamental rights. This would have significant negative implications on the success of convictions, as the ruling could be overturned by higher level courts, including the European Court of Human Rights, but also on the integrity and political legitimacy of the security, law enforcement and judicial institutions. Such omissions may have negative implications for Albania's policy alignment with the European Union, as ensuring full compliance with fundamental rights and guaranteeing more transparency, accountability and democratic control, are among the key principles of the European Agenda on Security.

The Albanian executive and legislative branches should take steps to address these shortcomings by improving the legislation with the aim to strengthen the accountability framework and practices in order to align them with the European Court of Human Rights case law and the EU policies.

Introduction

Lawful interception (LI) is the legally sanctioned official access to private communications, such as telephone calls or online communications and e-mail messages. Through the LI, a network operator or service provider gives law enforcement officials access to the communications of private individuals or organizations.

As one of the most widely used special investigative techniques LI, plays a crucial role in helping law enforcement agencies to combat criminal activity among others. LI is particularly useful when dealing with sophisticated organised criminal and terrorist groups because it is dangerous and difficult to gain access to their operations, and gather evidence for use in prosecutions. LI is used also to investigate corruption and to allow the evidence collected to be admissible in courts.

LI is based on national legislation of each country. In conducting interception of telecommunications countries are required to maintain a balance between the needs of security agencies and the respect for fundamental rights to privacy, personal data protection, and private and family life.

LI does not automatically violate the rights to a fair trial and to property, but adequate and sufficient safeguards against abuse must be in place. There is a very fine line between Lawful and Un-Lawful Interception, which is dependent primarily on the legal and regulatory framework, followed by the policies and procedures involved in its utilization, monitoring and scrutiny, and on the technology used.

Due to LI's potential to be misused or abused and to the immense impact it can have when misused, it should be very well standardized and regulated in conformity with the best international norms and practices.

The European Convention on Human Rights and the case law of the European Court of Human Right (ECtHR) provide for a number of standards, which the national laws of the Member States of the Council of Europe must adhere. In order to prevent the misuse of interceptions there should be safeguards that include: comprehensive legislation, control mechanisms and effective oversight.

Through a number of Directives and Regulations, the European Union also sets out the framework for a balanced approach when using electronic surveillance. EU Members are required to maintain a balance between the needs of law enforcement authorities and respect for the fundamental rights to privacy, personal data protection, and private and family life. The European Agenda on Security (EAS),[1] adopted by the EU Commission in April 2015, defines as key principles the full compliance with fundamental rights and the guarantee for more

1 European Commission. (2015, April 28). Communication from the commission to the European parliament, the council, the European economic and social committee and the committee of the regions – the European agenda on security. Brussels: COM(2015) 185. https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf

transparency, accountability and democratic control.

In light of its obligations to adhere to the international conventions and the country's Constitution, Albania adopted a comprehensive law on interception of telecommunications (LIT) in 2003, although interception of telecommunications to collect evidence was used earlier also. The Criminal Procedure Code (CPC) adopted in 1995 provided for legal and procedural specifications on interceptions but did not elaborate on technical standards.

The LIT has been so far amended four times (2008, 2009, 2012, and 2017) with the aim to broaden the interception scope and improve the technical capabilities. The latest amendments of both the LIT and the Criminal Procedure Code were made in 2017, as part of the comprehensive justice reform that seeks to address the fight against corruption and organised crime.

In addition to the enhancement of the interceptions' framework and capabilities, to be used for investigation and prosecution organised crime and corruption, the use of interception has been expanded to become part of the integrity building process of the new institutions established to fight organised crime and corruption. According to the law on the Organization and Functioning of Institutions for Combating Corruption and Organized Crime (law on SPAK),[2] all the judges, prosecutors, employees of the new anticorruption institutions, as well as their family members will be subject to regular monitoring of their electronic communications.

While the frequent amendments of the legislation have targeted the enhancement of the interceptions' framework and capabilities, it has failed to proportionally provide for the establishment of an effective accountability system. The existence of an effective control and oversight of interceptions is required by the Council of Europe, the case law of the ECtHR, and the EU Directives and Regulations, which compliance although not being mandatory for Albania as an EU candidate country, would have contributed to the overall legislation approximation and policy convergence.

Moreover, the current legislation fails to satisfy criteria such as the quality of law standards, as set out by ECtHR case law. The lack of a solid legislation that is fully compliant with the best international practise and the ECtHR case law, and the lack of effective mechanisms of control and oversight risk to have negative implication for both the success of the efforts to combat crime and corruption as well as for the integrity and legitimacy of the law enforcement and judicial institutions.

It is important for Council of Europe member States to have legal framework in place that is fully compliant, because it can ultimately be subjected to the control of the ECtHR. Once domestic remedies have been exhausted, individuals can bring a case before the ECtHR, alleging that interception has violated their human rights. Therefore there is the risk that people accused of corruption or crime may be

2 Law on SPAK, http://www.reformanedrejtesi.al/sites/default/files/ligj-nr-95-dt-6-10-2016-1.pdf

cleared of their charges if the ECtHR finds that interceptions used to collect evidence have failed to meet the quality of law standards.

On the other hand such failure would contribute negatively to the efforts made to strengthen the capacities and enhance the legitimacy of the law enforcement and judicial institutions. Legality of interceptions is already a very hot political topic in Albania, as over the last decade frequent allegations have been made by the opposition parties of all sides accusing the government for misusing and abusing interception competences and capabilities for unlawful purposes. Ultimately the cost of such allegations has fallen upon the law enforcement and security institutions which political legitimacy, integrity and public trust have been constantly undermined.

The failure of the attempts to properly investigate and clear these allegations has revealed the lack of an effective and reliable control and oversight system, while the failure of the executive and the legislative to address the lack of such mechanisms, despite the opportunity given through the frequent amendments, shows that there is a lack of awareness on the implications of such omissions.

Against this context this policy paper analyses the Albanian legislation and practice for the conduct of lawful interceptions and examines the conformity of the country's legal provisions with the requirements of the case law of the ECtHR, and the EU's policy framework as provided in the European Agenda on Security.

The aim of this paper is twofold: (1) to analyse and examine the extent to which the Albanian legal and institutional frameworks on interceptions complies with the case law of the ECtHR, and the EU's policy framework; (2) to propose recommendations for improving the legislation on interceptions and the control and oversight mechanisms, as a means to strengthen both the effectiveness and the legitimacy and integrity of the law enforcement, security and judicial institutions.

The paper is structured as following: the next section provides an overview of LI as a technical and legal process. The following section provides an overview of the Albanian legal framework and the accountability system currently in place. The subsequent section provides an analysis of the Albanian legal framework and its conformity with the case law of the ECtHR, and compliance with the EU policy and European Agenda on Security. The last section provides some concluding remarks and recommendations.

1. Lawful interception

LI as a technical and legal process

This section provides a general overview on how LI is conducted, as an arrangement of legal and technical processes. At first, the difference is made between the lawful interception of communications, conducted through the use electronic means of communication, and the recording of conversation or/and images that is conducted by placing audio and/or video recording devices in private premises. Given the technological differences between the static and portable interception technologies, a description of the differences between the two is also made.

This is relevant because of both legal and policy implications. While interception of communications makes it easier to investigate only those people targeted, the use of listening devices implies the surreptitious entry into private premises and the danger of recording persons that may not be target to an investigation, and therefore violating their basic rights. On the other hand, while in Albania there is legislation in place for the LI of communications, no legislation is in place regarding the use of devices that are physically placed in private premises, so this special measure of investigation remains currently unregulated.

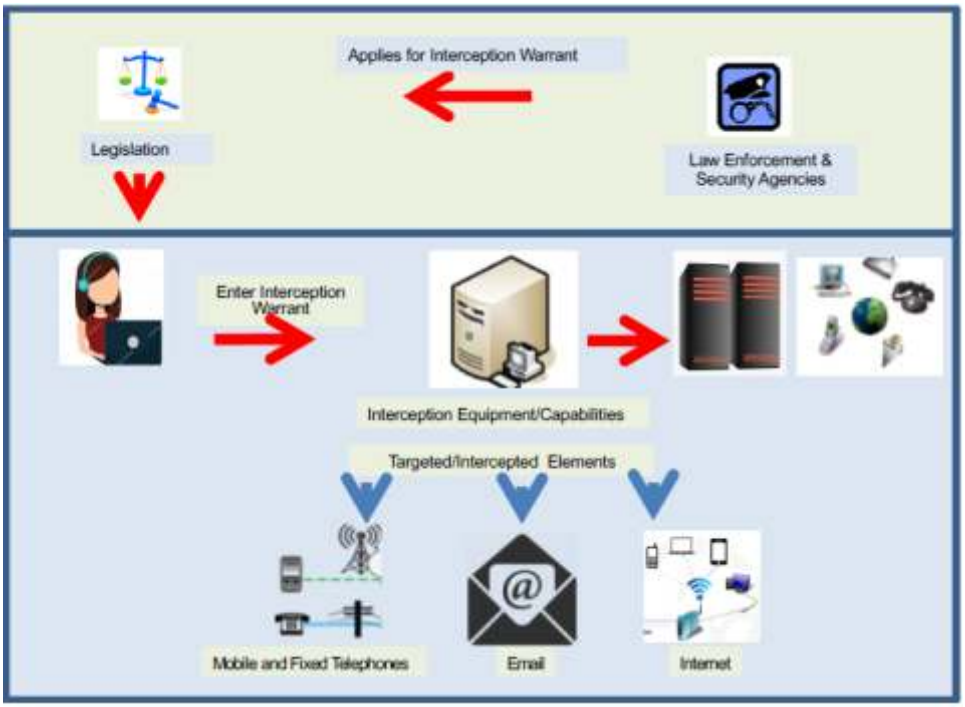


Figure 1. The request for an interception warrant

LI involves technology (hardware, software, networks), people (law enforcement agencies, government and legislation authorities, network and service provider employees), and official procedures that have to be followed in order for the interception to be legal, and in order for the evidence collected to be admissible for prosecution by the judicial authorities.

Generally, the LI is conducted through the following steps:

- The law enforcement or security agency applies for a warrant to an authority in charge of approving the interception of communications against a person.
- The warrant is approved by the responsible authority (judge, prosecutor, minister).
- The warrant is forwarded to the communications company or companies (either physically or electronically).
- The communications company(ies) initiates the interception based on the warrant.
- The law enforcement or security agency receives the intercepted material.

The figures below describe the two phases of the process, the application for a warrant and the delivery of the interceptions (Figures 1 and 2).

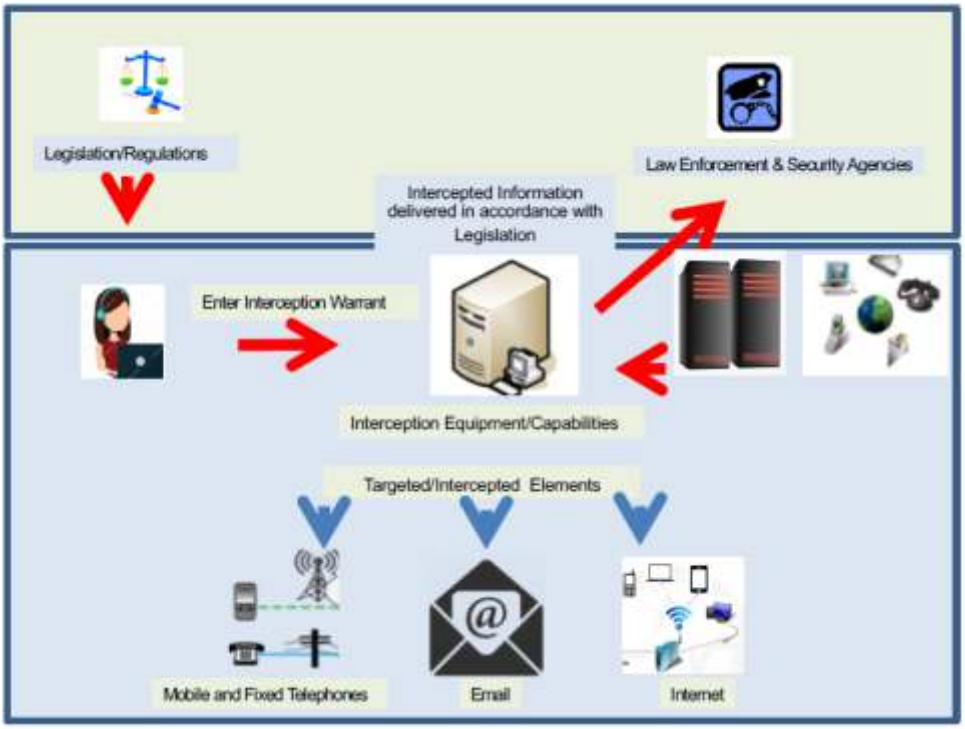


Figure 2. The delivery of interception materials

Generally the technological solutions allow for static or portable interception equipment. Most commonly interceptions are conducted by static interception facilities, as these allow for better processing of information as well as more effective controls and accountability. Portable interception equipment has been developed more recently and is used to complement the static interception capabilities. Portable interception equipment is used by law enforcement teams for specific operational purposes to complement interceptions conducted through the static interception equipment, for instance if there are areas where there is no proper GSM coverage, or to identify and track a phone or other compatible cellular data device even while the device is not engaged in a call or accessing data services. A well known portable technology, which is widely used for the interception of mobile communications, is the International Mobile Subscriber Identity catcher, or IMSI-catcher. The IMSI-catcher imitates a GSM tower in a way that is impossible for a mobile phone to distinguish it from an authentic GSM tower. This allows the IMSI-catcher to capture any data that a mobile phone would normally send or receive from a valid GSM tower (Figure 3).[3]

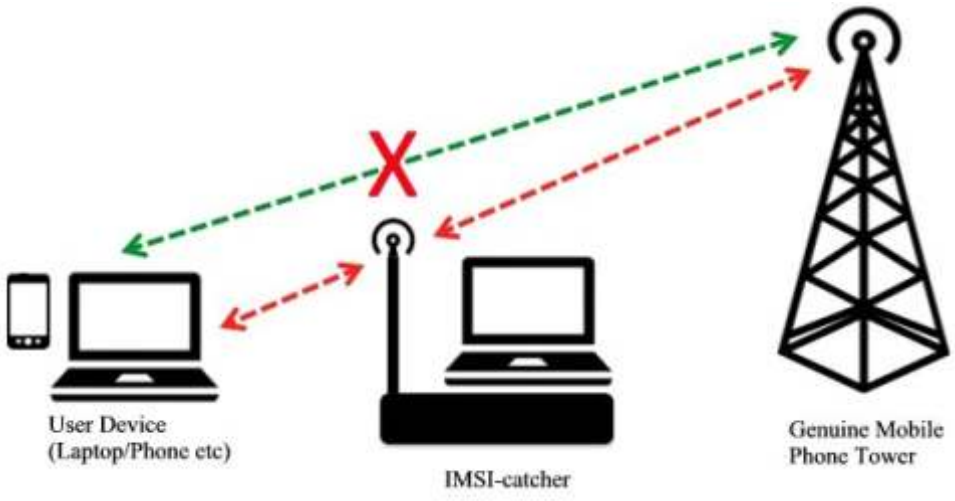


Figure 3. Interceptions conducted with an IMSI-catcher technology

Given its mobility, this technology can be used by the law enforcement or intelligence and security agencies without needing a warrant. Therefore concerns have been raised about its use while the existing legal framework doesn't provide for clear regulations.

In addition to the interception of communications, the law enforcement and security agencies use also audio and/or video recording devices that are placed in private premises (home, office, cars, etc.) of people that are target to an

3 Norman, Jason. "Taking the Sting Out of the Stingray: The Dangers of Cell-Site Simulator Use and the Role of the Federal Communications Commission in Protecting Privacy & Security." Fed. Comm. LJ 68 (2016): 139

investigation.
Legally, the interception of electronic communications and the interception of oral communications are distinct categories, since in order to record oral communications (via audio or/and video technical devices) the law enforcement and security officials may need to physically enter private residences to place these devices (Figure 4).

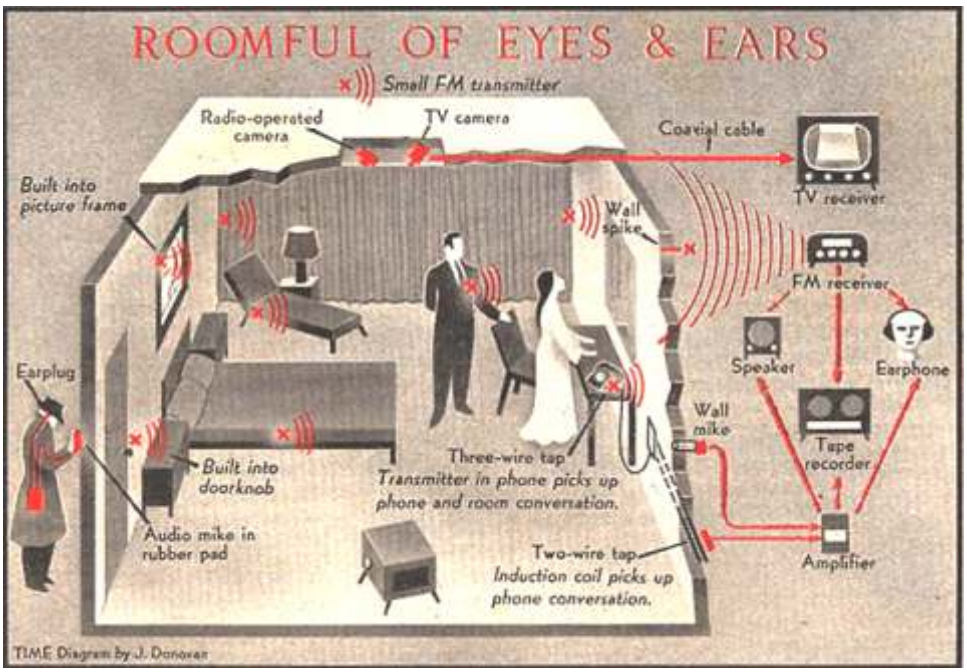


Figure 4. Various ways of placing audio/video recording devices in a private residence.[4]

The Albanian legislation on interception

The interception of telecommunications has been a known practice in Albania for decades but no specific legislation existed to regulate it until 1995, rather it was provided in the regulatory framework of the security institutions as an investigation and evidence collection method.
The Code of the Penal Procedure (CPP) approved in 1995 provided for the first time the procedure for carrying out judicial interceptions. The interceptions acquired through this procedure could be used as and evidence in courts. Meantime no legislation was adopted until 2003 for regulating the lawful interceptions for

4 Image used to illustrate the article "Bug Thy Neighbor", TIME Magazine March 6 1964. http://www.bugsweeps.com/info/time_article.html

collecting intelligence or security related information (security interceptions).
Drawing on the distinction between the judicial interceptions, conducted during a judicial investigation for the detection and the investigation of a crime, and the security interceptions authorised for collecting intelligence or security related information, this section provides an overview of both processes and procedures.

Security interceptions

The Albanian parliament adopted for the first time a law on lawful interceptions for conducting security interceptions in 2003. The law was adopted in response to the development of the telecommunication technologies and the increased usage of the mobile phones by the population, the need to tackle the increased activity of the organized crime, and the requirements for compliance with Convention for the Protection of Human Rights and Fundamental Freedoms which Albania has ratified a few years earlier.[5]
The law provides among others for the institutions eligible to use LI, the grounds upon which LI may be requested, the authority responsible for approving the interception warrants, the duration of the interceptions, the LI in emergency situations (Table 1).
The State Police, the State Intelligence Service and all the other intelligence and security agencies that operate under the ministries of Interior, Defence, Finances and Justice, are eligible to use interception of telecommunications under this law. The information obtained through this law cannot be used as evidence in the Court.[6]
Since its adoption in 2003, the law on interceptions has been amended four times. The first amendment made in 2008, provided for the Ministry of Interior to establish a section staffed with police officers in the premises of the State Intelligence Service where the interception facilities were based.[7] The amendment seemed to be a solution to give to the Ministry of Interior direct access to interception capabilities, as the relationship between the government and the head of the State Intelligence Service had worsened and the minister of interior was keen to have his own people being in charge conducting the interceptions.[8]
Nearly one and a half year later, the law was amended again to explicitly provide for more institutions to have access to interception. With these amendments the ministers of Finances and Justice were given the competence to apply for an interception warrant.[9] Originally the law (2003) specifically mentioned only the ministry of Interior and Defence, as well as any other intelligence/security or police agency established by law to apply for a warrant. The amendments revealed the trend of an increased use of interception by an increasing number of government agencies.

5 Arjan Dyrmishi. "Interception of Telecommunications in Albania: Legislation and Practice", Policy Series II, Institute for Democracy and Mediation 2010.http://idmalbania.org/wp-content/uploads/2014/10/interception-of-communications-in-Albania_June-2010.pdf
6 Law Nr. 9157, date 4.12.2003, On the interception of the Telecommunication
7 Law Nr.9885, date 3.3.2008, On some amendments to the law On the interception of the Telecommunication
8 US Embassy Tirana. Overview of the Albanian Intelligence Services. 2007 December 31. https://wikileaks.org/plusd/cables/07TIRANA1090_a.html
9 Law Nr.10 172, date 22.10.2009, On some amendments to the law On the interception of the Telecommunication

The law was amended for the third time in 2012 with the aim to reflect the development of broadband technologies and the increased use of internet for both voice and data communications.[10] This was reflected also in the title of the law which was modified to become the "Law on the interceptions of electronic communications".

The law provided also for the obligations of the communications providers to ensure the access to lawful interception with their own costs within 180 days from the receipt of the demand by the institutions that conduct interceptions. This clause sought to keep up with interceptions amid the expanding number of the communications providers, more specifically internet providers, and the risk that criminals tended to use services from the newly established providers that could not be intercepted.

In 2017 the law was amended again, this time with the aim to align it with the justice sector reform.[11] According to the new amendments, the authority for approving the interception warrants has been transferred from the Prosecutor General to the Chief of the Appellate Court on Anti-Corruption and Organized Crime (CHAC).[12] The law introduces a deadline of 48 hours within which the CHAC should approve or reject the application.

The law provides also for some modifications for the emergency situations. The interception can be initiated immediately upon verbal request by the agencies entitled to apply for a warrant but the applicant institution must submit a regular warrant application within 8 hours. The approving authority has the right to interrupt the interception after 24 hours from the initiation of the procedure.

The law specifies the deadline for the destruction of the intercepted materials after the termination of the interceptions within 10 days, unless there is a justified ground by the institution that retains the intercepted material to extend the destruction. The extension can be authorized by the CHAC.

A new clause in this amendment is the provision for the right to information by citizens being subject to interception. However, the provision of information is not mandatory as the intercepting institution may refuse to provide information on grounds of harming the activity of that institution, another person or the national security interests.

The law provides also for an increased number of the interception facilities. From 2003 until 2010, both security and judicial interceptions were conducted by the interception capability managed by the State Intelligence Agency (SHISH). In 2010 the judicial interceptions were conducted in the General Prosecution through a second facility that was established for this purpose. The 2017 law provides for the establishment of interception capabilities in the Special Prosecution on Anti-Corruption and Organized Crime (SPAK),[13] as well as the district prosecution offices. The National Bureau of Investigation (NBI) that will operate within SPAK is responsible for conducting the interceptions.

10 Law Nr. 116/2012, date 13.12.2012, On the interceptions of electronic communications
11 EURALIUS. Justice Reform.http://www.euralius.eu/index.php/en/library/justice-reform
12 Law Nr. 69/2017, date 27.04.2017, On the interceptions of electronic communications
13 Law 95/2016, date 6.10.2016. On the Organization and Functioning of Institutions for Combating Corruption and Organized Crime

Judicial interceptions

The lawful interceptions for judicial purposes are conducted in accordance with the Code of Penal Procedure. The CPP provides for the authorities responsible for applying for and issuing an interception warrant, the grounds on which the LI may be approved, and the duration and renewal of the warrants (Table 1).[14]

The authorities responsible for applying for a LI warrant are the prosecutors. The LI may be requested on grounds of crimes punishable with prison sentence up to seven years and any crime committed by means of telecommunications and information technology. Additionally, with the amendments made to the CPP in 2017, the prosecutors may apply for LI also for the investigation of corruption crimes committed by public officials and illegal benefits of interests.[15]

The authority responsible for issuing the warrants is the Court. The CPP provides also for use of LI without a Court warrant in an emergency situation. In such case, the prosecutor is obliged to inform to the Court within 24 hours, and in meantime, to apply for a warrant which the Court has to approve or reject within forty eight hours.

	Authorities eligible to apply for an interception warrant	Authorities eligible to approve an interception warrant	Grounds	Duration	Renewal	Emergency situations
Security Interceptions	Intelligence Service Ministry of Interior Ministry of Defence, Ministry of Justice, Ministry of Finance, the National Bureau of Investigation	Chief of the Appellate Court on Anti-Corruption and Organized Crime (Prosecutor General 2003-2017)	Increase the effectiveness of the work of investigative institutions to detecting unconstitutional, criminal and malicious activity, and to prevent the consequences that can come from such activity.	Three months	Unlimited extensions for three months period	Immediately, upon verbal request by the eligible institutions. Obligations to submit full application within 8 hours
Judicial Interceptions	The prosecutors (in accordance with their jurisdiction)	The Courts, (in accordance with their jurisdiction)	Crimes punishable with prison sentence up to seven years. Any crime committed by means of telecommunications and information technology. Active and passive corruption of public officials Illegal benefits of interests	15 days	Unlimited extensions for 15 days period	Immediately, upon motivated justification by the prosecutor. Obligations to inform the Court within 8 hours. Obligations to submit full application within 24 hours.

Table 1. Security and judicial interceptions: comparison of procedures

14 CPP, articles 221-226.

15 The crimes foreseen in the Penal Code in the articles: 244, 244/a, 245, 245/1, 257, 258, 259, 259/a, 260, 312, 319, 319/a, 319/b, 319/c, 319/ç, 319/d, 319/dh, 319/e.

The CPP provides also for the "interception via technical means of oral communications in private locations, the interception/recording via audio and video in private locations". However, although such kind of interception presupposes the entry and interference with private property, and therefore requires adequate specific legal requirements and safeguards, the legislation is not adequately developed.

Accountability

According to the Venice Commission accountability may be defined as "being liable to be required to give an account or explanation of actions and where appropriate, to suffer the consequences, take the blame or undertake to put matters right, if it should appear that errors have been made".[16]

As far as law enforcement and security agencies are concerned, there can be different types of accountability: to the executive, judiciary, parliament and independent bodies. There is also the accountability to international mechanisms, such as Council of Europe and the European Court of Human Rights. The monitoring role of civil society and the media are other forms of accountability.

As part of the democratic control of the security institutions the control and oversight of the interceptions is embedded in those processes.

There is no single model on how accountability is exercised as this depends on a number of factors, in particular the constitutional structure and history of the state, its legal and political culture and in the types of accountability exercised by the different branches of government. However an accountability system should include all or part of the following activities:

- Internal and government controls conducted in order to ensure that the employees and officials in charge implement the laws and regulations in an efficient, professional and legal manner.
- Authorisation of the interception warrants by an authority external to the law enforcement or security agency, as a rule by a judicial authority.
- The conduct of follow up controls by an independent expert body or a combination of parliamentary, judicial, and expert bodies.
- A complaint mechanism that allows individuals to complain on alleged violation of rights.
- An active monitoring role by civil society (NGOs, think tanks etc.) and the media (Figure 5).

16 European Commission for Democracy through Law (Venice Commission). Report On The Democratic Oversight of the Security Services. Strasbourg, 15 December 2015, CDL-AD(2015)010 http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)010-e

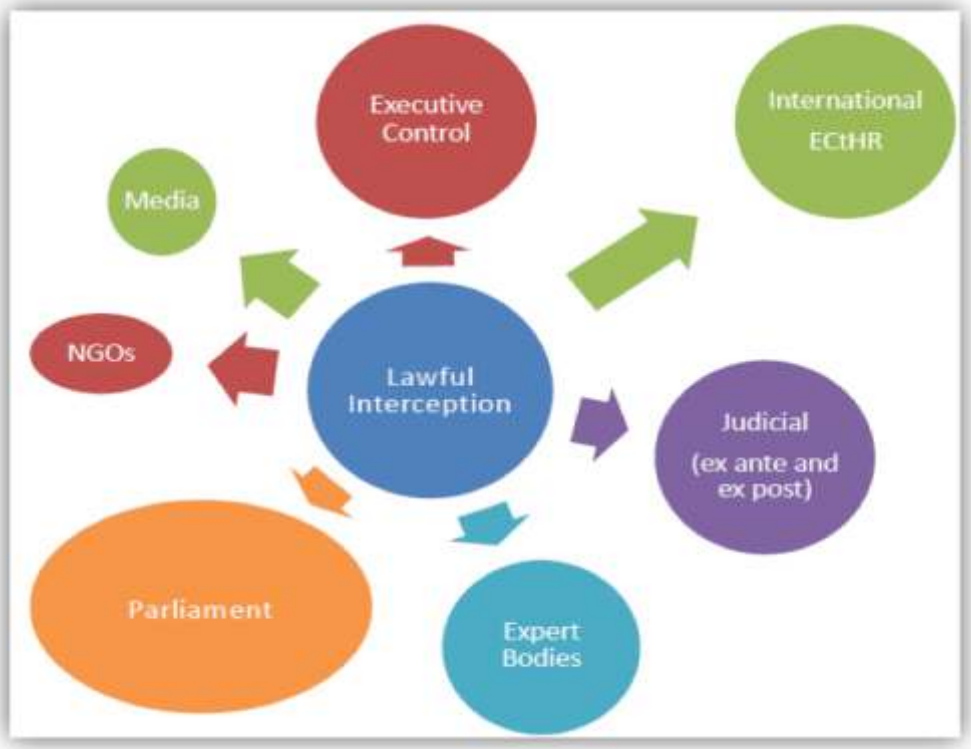


Figure 5. The accountability system of interceptions as promoted by the Council of Europe

Accountability mechanisms on interception have been generally improved in the European area, over the last decade.[17]

Accountability may exist ex ante, beforehand or/and during the interception, or/and ex post with the aim to review the activities conducted. It can concern general operations or specific acts. Hybrid forms of accountability may also exist. For example, an independent expert body can be given powers of authorization of warrants or/and scrutiny of implementation, while a parliamentary body can be given the power to conduct hearings and/or investigations.

The Albanian legal framework on LI, for both the security and judicial interception provides limited provisions on control and oversight. Some form of ex ante control is conducted through the division of competences between the law enforcement and security institutions that are entitled to use LI, and the authorities that issue the interception warrants. In order to control the execution of the warrants, the law empowers the General Prosecutor with the competence to have the control of the commanding equipment that enables the interception.[18]

However no procedures exist for controls to be conducted during the process of

17 European Union Agency for Fundamental Rights. "Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU - Volume II: field perspectives and legal update". Luxembourg 2017. http://fra.europa.eu/en/publication/2017/surveillance-intelligence-socio-lega

18 Law on interceptions, Article 13

the interception. The law provides for the PG to have access to the intercepted materials but only after the interception has been terminated.[19]

In the case of the judicial interceptions even the ex ante control is flawed, as the PG has both the control of the commanding equipment and of the listening equipment, where the intercepted material is routed to be processed by the intercept operators.

Regarding the oversight by the parliament of the security interceptions, no procedure exists and no procedure has been established by the parliament on the means or procedures to conducting parliamentary oversight, despite the frequent amendments of the law on interceptions. Over the last decade the parliament has made attempts to exert some form or scrutiny but the results have been negligible (Box 1).

Box 1. The case of interceptions conducted by the Defence Intelligence and Security Agency

In June 2012 the Socialist Party accused the Ministry of Defence (MoD) and the Defence Intelligence and Security Agency (DISA) for unlawful use of intercepting devices to eavesdrop the opposition and diplomats of friendly countries. The MoD and the government rejected the accusations and despite repeated requests did not authorise the Socialist Party members of the parliamentary National Security Commission to have access to the premises of the MoD and the DISA in order to oversee their activity. The head of the opposition pledged an investigation if the Socialist Party won the elections in 2013.

In March 2014 the new government and the MoD made public documents showing that in 2010 DISA had purchased electronic surveillance equipment worth about 1.6 million Euros. The intercepting device: Engage PI2 and Engage GI2 made by the Israeli company Verint Systems Ltd,[20] was shipped into Albania in the period around March 2011, and allegedly was used for interception purposes until July 2013.

The new Minister of Defence declared that the former MoD and DISA officials had used this surveillance equipment to unlawfully intercept the opposition.[21] The MoD filed a request to the Prosecution to investigate the former Minister of Defence, the former Director of DISA and five other MoD officials for violating the procurement legislation.[22] The Prosecution was asked also to establish whether the DISA, which maintained that the interception device was used only for providing support the Albanian troops in overseas missions, had conducted illegal intercepting operations against opposition politicians inside Albania. The MoD suspects that the former officials have replaced the hard discs with intercepted records with new ones

However the Prosecution has not formally charge any of the suspected officials. Due to lack of expertise and adequate technology the Prosecution has not been able to establish on whether the surveillance equipment has been used to intercept the alleged targets.[23] The Prosecution has not formally filed the case.

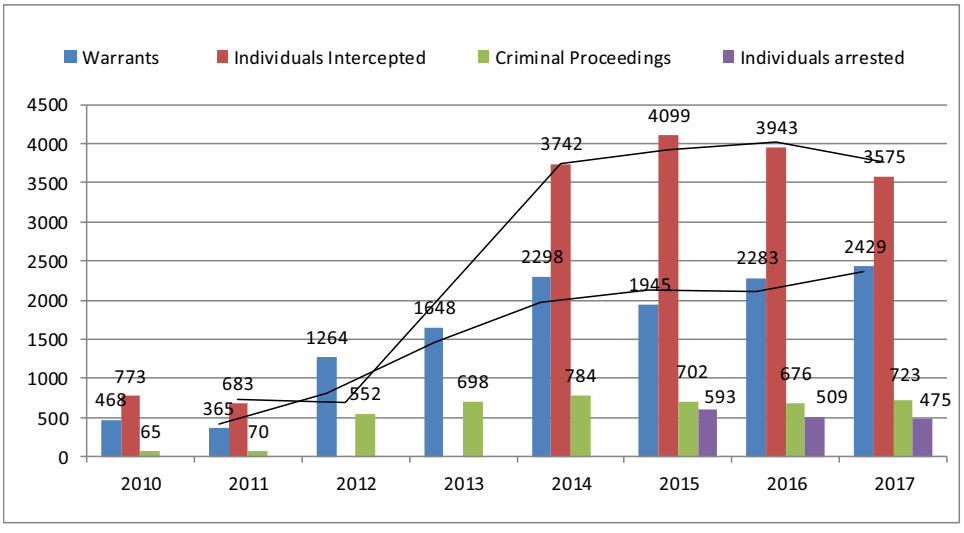
19 Law on interceptions, Article 15
20 https://www.verint.com/index.html
21 Ministria e Mbrojtjes. "Intervista e ministres së Mbrojtjes, znj. Mimi Kodheli në emisionin "Top Story" në Top Channel". 02 Maj 2014. http://www.mod.gov.al/index.php/newsroom-2/ministri-ne-media/401-intervista-e-ministres-se-mbrojtjes-znj-mimi-kodheli-ne-emisionin-top-story-ne-top-channel
22 Shqiptarja.com. Përgjimi i opozitës, PD e Ylli Zyla abuzime nën emrin e NATO-s. 25 Mars 2014. http://shqiptarja.com/lajm/pergjimi-i-opozites-pd-e-ylli-zyla-br-abuzime-nen-emrin-e-nato-s?r=pop5s
23 Respublica. Mungesa e teknologjisë bllokon hetimet për serverin e tatimeve dhe aparaturën e përgjimit në Ministrinë e Mbrojtjes. Prokuroria fajëson Policinë Shkencore. 3 Shkurt 2015. http://www.respublica.al/content/mungesa-e-teknologjis%C3%AB-bllokon-hetimet-p%C3%ABr-serverin-e-tatimeve-dhe-aparatur%C3%ABn-e-p%C3%ABrgjimit-n%C3%AB

In the case of the judicial interceptions there is some form of parliamentary oversight, as the PG reports to the parliament annually. Since 2010 there has been a chapter in the PG's annual report that is dedicated to statistics and issues pertaining to the judicial interceptions. However, no follow up action has been undertaken by the parliament to addressing the issues raised in the reports and to querying the trends with the interceptions use and effectiveness. The data from the PG's annual report shows that while the number of intercepted persons has increased considerably (up to 4-5 times) the number of criminal proceedings and the number of arrested persons has remained almost stagnant (Graph 1).

The increased gap between the number of people intercepted and the outcomes of the use of such investigative measure raises questions on whether the provision of increase the number of the interception facilities, as provided by the 2017 amendments of the law on interceptions. Since 2011 the PG has continually raised the concern in the annual reports that the 'results obtained by the use of interceptions are not satisfactory'.[24]

Moreover the PG has considered as problematic the relatively high number of people with access to interception, suggesting that this has been a weak point because leakages have made interception less effective.[25]

The increased number of the interception facilities will make control and oversight even more complicated. Since the law provides for separation of the processes of electronic authorization of the warrant into the system and the execution of interceptions it is not clear which authority will control the multiple electronic authorisation units and how, as both processes will be conducted by the prosecution offices.



Graph 1. Number of interception warrants, intercepted individuals and criminal proceedings in the period from 2010 to 2017.
Source. Compiled with data from the General Prosecutor reports to the Parliament.[26]

24 Prokuroria e Përgjithshme. Raporte të Prokurorit të Përgjithshëm (2010-2017).http://www.pp.gov.al/web/Raporte_te_Prokurorit_te_Pergjithshem_353_1.php
25 Prokuroria e Përgjithshme Raporti Vjetor mbi Gjendjen e Kriminalitetit. Viti 2014 http://www.pp.gov.al/web/fiinal_final_raporti_pp_06_03_2015_1093.pdf
26 Prokuroria e Përgjithshme. Raporte të Prokurorit të Përgjithshëm (2010-2017). http://www.pp.gov.al/web/Raporte_te_Prokurorit_te_Pergjithshem_353_1.php

In the case of SPAK the issue of control and accountability is more complicated as the SPAK will have both investigative and judicial powers, while there is no clearly defined internal separation within the agency. In addition the risk of abuse is doubled because the SPAK will have the control of both the commanding equipment and the listening equipment and will have the competence to conduct both security interceptions and judicial interceptions,[27] two processes that so far have been separated and carried out by different institutions.

Lawful interception and unlawful interception

One particular omission in the legislation, which has posed challenges to the accountability of the interceptions, is the lack of a clear definition of unlawful interception.

Unlawful interception is treated as a criminal offence in the Albanian Penal Code (PC). The interception of telephone communications or any other means of communication is punishable with prison sentence up to 3 years or a financial penalty. The Penal Code defines also the unlawful interception of computer data as a criminal offense, punishable with a prison sentence of 3 to 7 years. For similar offence against public computer systems the CP provides for prison sentence of 7 to 15 years.[28]

However the law on interceptions does not define what unlawful interception specifically entails, except for the violations of the procedures of the lawful interception. The consequences of this omission have made it almost impractical to establish the truth on such procedure on a number of occasions (see Box 1). The most recent case was the 'IMSI Catcher Case', which led to a clash between the police, the prosecution, and the intelligence services (Box 2).

Box 3. The allegations on unlawful interception by the Albanian State Police (ASP)

On 11 March 2016, an IMSI Catcher, model Vortex Aircube produced in Israel, was shipped into Albania through the port of Durres by a car with Italian diplomatic plates. The Albanian Intelligence Service (SHISH) alerted the Prosecution Office which initiated a formal investigation in June2016 charging the General Director of the ASP and two other police officials for illegally importing into the country an IMSI-catcher interception device.[29]

The General Director of the ASP Haki Çako was suspended from his position by Court Decision and the Court sentenced him with house arrest for the pre-trial period. However the decision was overturn by the Court of Appeal and Çako was reinstated to his position.

The Prosecution had collected evidence from the interrogation of police officers

27 Law on interceptions, Articles 8, 13, 23.
28 Kodi Penal iRepublikë ssë Shqipërisë. http://www.qbz.gov.al/Kode/Kodi%20Penal-2017.pdf
29 Prokuroria e Përgjithshme. Çështja "IMSI Catcher", pezullohet nga detyra Drejtori I Përgjithshëm i Policisë, i dyshuar për "Shpërdorim detyre". "Arrest në shtëpi" për dy zyrtarë të tjerë 07.06.2016 http://www.pp.gov.al/web/Ceshtja_IMSI_Catcher_pezullohet_nga_detyra_Drejtori_i_Pergjithshem_i_Policise_i_dyshuar_per_Shperdorim_detyre_Arrest_ne_sht_969_1.php#.WvBJDpqxWUk

that suggested that the device had entered Albania illegally in March 2016 and was used for interception purposes, including within the prisons.[30]
The Prosecution issued a sequestration warrant for the device but it was never able to get hold of it. The ASP Director Çako refused the Prosecution the request maintaining that the item was destined for a diplomatic post and had a diplomatic immunity so it could not be examined by Prosecution. The IMSI-catcher device was transferred by the ASP to the Italian Embassy in Tirana. The Prosecution demanded the Italian authorities to access the device but it never received any reply so the Albanian prosecutors have not been able to examine it and establish for what purposes the device was used.[31]
The IMSI-catcher case became a hot political issue and a parliamentary investigative commission was established to examine the case for a four months mandate.[32] The opposition claimed that the ASP Director had used the device to intercept the politicians of the opposition and foreign diplomats. The commission summoned 17 high officials from the Intelligence Service, the ASP, the Ministry of Interior, including the minister, and the Prisons. The work of the investigative commission did not lead to any meaningful result as the cooperation of the summoned official was minimal and they refused to give evidence with the claim that the case was under investigation by the Prosecution and therefore any statement would lead to breach of the secrecy of the investigative procedures.[33]

The case was investigated by the Prosecution for two years, by postponing the investigation every three months, in accordance with the Criminal Procedure Code. The latest postponement ended in May 2018, and since no evidence was collected due to inability of the Prosecution to access the device, the case was closed by the Court.[34]

Allegations of unlawful interception have been advanced by various high state officials. In June 2016 the Minister of Interior registered a case to the prosecution offices on allegations that he had been electronically surveilled in his office.[35] One year earlier, the President of the Republic had made a similar claim (Box 3).

Box 3. Allegations on illegal eavesdropping of the office of President Nishani

In October 2015 President Bujar Nishani declared publically on the television that the government had been spying on him and his family.[36] One month later he claimed to have found an eavesdropping device in his office and officially requested an investigation to be led by the Prosecutor General's office. Few months before leaving the office, President Nishani repeated publically his claims of illegal eavesdropping, pointing to the Ministry of Interior as responsible for such action.

30 Lapsi. Dëshmitëpër IMSI CATCHER/ Oficerët e policisë "tradhtuan" HakiÇakon. 15 Gusht 2016. http://lapsi.al/2016/08/15/deshmite-per-imsi-catcher-oficeret-e-policise-tradhtuan-haki-cakon/
31 Top Channel. Hetimi për pajisjen përgjuese, prokuroria nuk bën dot ekspertizën. 11 Janar 2018. http://top-channel.tv/2018/01/11/hetimi-per-pajisjen-pergjuese-prokuroria-nuk-ben-dot-ekspertizen/
32 Kuvendi i Shqipërisë. VendimNr. 66/2016. Për Ngritjen e Komisionit Hetimor të Kuvendit për të Kontrolluar Zbatimin e Legjislacionit në Fuqi për Përdorimin dhe Administrimin nga Strukturat e Ministrisë së Brendshme dhe Policisë së Shtetit të Pajisjes Përgjuese "IMSI Cathcer" dhe Realizimin nëpërmjet saj të Përgjimeve të Paligjshme. https://www.parlament.al/wp-content/uploads/2016/07/VENDIM-pajisja-pergjuese.pdf
33 Ministria e Brendshme. Raportimi i ministrit Tahirinë Komisionin Hetimor për përdorimin e "IMSI CATCHER". 12 Dhjetor 2016.http://www.mb.gov.al/al/newsroom/lajme/raportimi-i-ministrit-tahiri-ne-komisionin-hetimor-per-perdorimin-e-imsi-catcher
Top Channel. "IMSI Catcher", Çako hesht për pajisjen: Ka njëhetim nga prokuroria. 22 Nentor 2016. http://top-channel.tv/2016/11/22/imsi-catcher-cako-hesht-per-pajisjen-ka-nje-hetim-nga-prokuroria/
34 Klodiana Lala. Gjykata pushon hetimet për "Imsi catcher", Prokuroria: S'kemi mundësi të bëjmë ekspertimin. Balkanweb, 22.05.2018. http://www.balkanweb.com/site/gjykata-pushon-hetimet-per-imsi-catcher-prokuroria-skemi-mundesi-te-bejme-ekspertimin/
35Balkanweb. "Përgjues në zyrën e Tahirit, ministry bën kallëzim në prokurori. Dyshohet se ja vendosi një punonjës:
02 Qershor, 2016.
http://www.balkanweb.com/pergjues-ne-zyren-e-tahirit-ministri-ben-kallezim-ne-prokurori-dyshohet-se-ja-vendosi-nje-punonjes/
36 Top Channel. Presidenti Nishani: Po përgjohet jeta private e imja dhe e familjarëve të mi. 29 Tetor 2015. http://top-channel.tv/2015/10/29/presidenti-nishani-po-pergjohet-jeta-private-e-imja-dhe-e-familjareve-te-mi/

Conformity with the ECtHR case law and the EU policy

The interception of electronic communications is inherently linked to the right to privacy and personal data protection. Such rights are enshrined in the European Convention of Human Rights and Fundamental Freedoms legal issues arising from interceptions that may infringe on the human rights of individuals are subject to review by the European Court of Human Rights.
The specific technical nature of the processes can give rise to quality of law issues. In its case-law on secret measures of surveillance the ECtHR has developed a number of minimum safeguards that the legislation should include in order to avoid abuses of power (Box 4).[37]

Box 4. ECtHR case law: quality of the law.[38]

It is therefore essential to have clear, detailed rules on interception of telephone conversations, especially as the technology available for use is continually becoming more sophisticated [...]. The domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures [...]. Moreover, since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive or to a judge to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference."
ECtHR, Weber and Saravia v. Germany, No. 54934/00, 29 June 2006
"In its case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law to avoid abuses of power: the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed."
ECtHR, Weber and Saravia v. Germany, No. 54934/00, 29 June 2006

37 ECtHR, CASE OF ROMAN ZAKHAROV v. RUSSIA. No. 47143/06. 4 December 2015. https://lovdata.no/static/EMDN/emd-2006-047143.pdf
38 European Union Agency for Fundamental Rights. "Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU - Volume II: field perspectives and legal update". Luxembourg 2017. http://fra.europa.eu/en/publication/2017/surveillance-intelligence-socio-lega

So far, the approach taken by the Albanian law, with regard to the authorization of interception has not been in line with the ECtHR case law. In the case of Popescu v. Romania, the ECtHR considered that the Romanian authority which ordered the interception (the prosecutor) was not independent from the executive.[39] It stated that the authorizing body must be independent and that there should either be judicial control or independent control over the issuing body's activity.

With the amendment of the law on interceptions in 2017 this issue has been resolved as the authorizing power for the interception warrants is the Court. However the law doesn't specifically provide for follow up controls. In the Iordachi vs. Moldova case,[40] and the Ekimdzhiev vs Bulgaria case,[41] the ECtHR has stressed that independent controls should exist at both the authorization stage and the follow-up stage.

Apart from the authorisation, both the law on interceptions (2017) and the CPP (2017) do not provide for follow up procedures.

The requirement of establishing effective accountability mechanisms is highlighted also in the EU policies. According to the Treaty on European Union, security remains the responsibility of each member state,[42] so the EU lacks the competence to legislate in this area. However the EU members are required to maintain a balance between the needs of law enforcement authorities and respect for the fundamental rights to privacy, and personal data protection.

In the Action Plan for the Implementing the Stockholm Programme, the European Commission stresses that 'the Union must resist tendencies to treat security, justice and fundamental rights in isolation from one another'.[43]

In this respect the EU has legislated mainly in the area of data protection. According to the Directive 95/46/EC member states are required to ensure the rights and freedoms of natural citizens with regard to the processing of personal data, and in particular their right to privacy.[44] The Directive 2002/58/EC provides for the harmonization of the national provisions required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communication sector.[45]

Directive 2006/24/EC lays out provisions concerning the obligations of the providers of publicly available electronic communications services, or of public communications networks, with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined in national law.[46]

The EU legislation has spurred the strengthening of the mandates of independent expert bodies that that perform important watchdog functions. In seven EU member states (Austria, Bulgaria, Croatia, Finland, Hungary, Slovenia, and

39 ECtHR, Dumitru Popescu V. Romania. Application nos. 49234/99 and 71525/01. 26.4.2007 https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwiXk_za-tDcAhUFyqYKHdp9C9QQFjAAegQIAhAC&url=https%3A%2F%2Fhudoc.echr.coe.int%2Fapp%2Fconversion%2Fpdf%2F%3Flibrary%3DECHR%26id%3D003-1995439-2103500%26filename%3D003-1995439-2103500.pdf&usg=AOvVaw0LD6XytJT34dXOhnVmPP81

40 ECtHR, Case of Iordachi and others V. Moldova. Application no. 25198/02. 24 September 2009 https://rm.coe.int/168067d212

41 ECtHR, Association for European Integration and Human Rights and Ekimdzhiev V. Bulgaria. Application no.62540/00. 28 June 2007.http://hrlibrary.umn.edu/research/bulgaria/AEIHR_M_Ekimdjiev_en1.pdf

42 Treaty on European Union (TEU) art. 4, para. 2, 2016 O.J. (C 202) 1, 13, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2016.202.01.0001.01.ENG&toc=OJ:C:2016:202:TOC#C_2016202EN.01001301

43 European Commission. Action Plan Implementing the Stockholm Programme. Brussels, 20.4.2010 COM(2010) 171 final. https://ec.europa.eu/anti-trafficking/sites/antitrafficking/files/com_2010_171_action_plan_implementing_stockholm_programme_en_1.pdf

44 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

45 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications) art. 5, 2002 O.J. (L 201) 37, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML

46 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC, 2006 O.J. (L 105) 54, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF

Sweden) Data Protection Authorities have the same powers over national intelligence services as they do over any other data controller. In nine EU member states (Belgium, Cyprus, France, Germany, Greece, Ireland, Italy, Poland, Lithuania), Data Protection Authorities have the power to issue non-binding recommendations on general matters related to interceptions.[47]

Despite the increased relevance of the data protection and privacy related to the interception processes in the EU context, the Albanian legislation on interceptions makes no reference to personal data protection. The law specifies the individual right of citizens to require information on the data collected, but this is not mandatory for the institutions that have conducted LI to provide such data.[48]

The table below provides the conformity of the Albanian legislation and practices with the ECtHR case law and practices in EU member states.

EHtCR minimum safeguards	Security interceptions	Judicial interceptions
The law defines the nature of the offences which may give rise to an interception order	Not specified	Crimes punishable with prison sentence up to seven years. Any crime committed by means of telecommunications and information technology. Active and passive corruption of public officials Illegal benefits of interests
The law defines the categories of people liable to have their telephones tapped	Not specified	No specified in the CPP. Guidelines issued by the PG on the implementation of the CPP specify as people liable to interceptions :[49] - suspects for committing a criminal offense; - a person suspected of receiving or transmitting communications from the suspects; - a person who participates in transactions with the suspect, - a person whose interception may lead to the detection of the suspect's whereabouts or identity.
The law defines a limit on the duration of telephone tapping	Three months limit but no limit to extensions	15 days limit but no limit to extensions

47 European Union Agency for Fundamental Rights. "Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU - Volume II: field perspectives and legal update". Luxembourg 2017. http://fra.europa.eu/en/publication/2017/surveillance-intelligence-socio-lega

48 Law on interceptions 2017, article 20/1

The law defines the procedure to be followed for examining, using and storing the data obtained.	Intercepted materials are destroyed within 10 days from the termination of the interception. Procedures for storing and destroying the intercepted materials are provided in bylaws.	The Courts rule on the destruction of the intercepted material
The law defines the circumstances in which recordings may or must be erased or the tapes destroyed.	The intercepted materials may be preserved upon request of the intercepting agency and approval of the Court	The prosecution keeps the intercepted materials until the court gives the final ruling. The court decides on the destruction when case is ruled or closed.
CoE and EU standards and practices	**Security interceptions**	**Judicial interceptions**
Intelligence, security and law enforcement agencies use interceptions only when provided by law.	Law on electronic surveillance	Code of Penal Procedure
Validity in a judicial process	Intercepted material may not used as evidence in court	Intercepted material is used as evidence in court
Ex ante control	Authorization of warrants by the Court of Appeal	Intercepted material can be used as evidence in court.
Ex post oversight	None	None
Independent expert body are established	None	None
The data protection agency has access to control the compliance of intercepted data with the law on data protection	None	None
Provisions on treatment of “privileged communications”.	Not specified	The intercepted material resulting from communication of persons obliged to preserve professional secrecy may not be used as evidence in court.
The law defines precautions to be taken when communicating the data to other parties.	Not specified	Not specified
The law defines precautions to be taken when communicating the data to other parties.	Not specified	Not specified
Specific procedures exist for the parliament to conduct oversight of interceptions.	None	Partially. The Prosecutor General report to the parliament on the effectiveness of the use of interceptions.

Internal controls (paper trails, structural controls within the agency, factors promoting good professional ethics etc.) are in place.	Yes, but no reports are produced to assess effectiveness	Yes, but no reports are produced to assess effectiveness.
Executive Control	Ex ante ministerial control	Minister of Justice may activate
	through authorization of applications for interception warrants. Not applicable for the State Intelligence Service	inspections.
Regular reporting by Ombudsman and Data Protection Commissioner on adequacy of legislation and lawful use on SMI.	Not in place	Not in place
Reporting of Intelligence, security and law enforcement agencies to the Parliament	Not in place	Not applicable
Dedicated parliamentary (sub)committee on security and intelligence	Not in place	Not in place
Dedicated parliamentary (sub)committee on oversight of use of special measures of investigation	Not in place	Not in place
Complaint mechanism Complaints mechanisms. Under the ECHR, a state must provide an individual with an effective remedy for an alleged violation of his or her rights.	Citizens may file a request for information but the intercepting institution may refuse the request on breach of operational activity and security of individuals.	The citizen may complaint to the Court in case he/she has learned about the interception.

Table 2. Conformity of the Albanian legislation and practices with the ECtHR case law and practices in EU member states.[50]

49 Prokurori i Përgjithshëm. Udhëzim Nr.1 Datë 21.04. 2006, "Për Përgjimet"
50 The red and orange coloured boxes in the table indicate the omissions in the legislation

Conclusions and Recommendations

While considered to be one of the most effective tools in preventing and investigating criminal activity, the interception of communications is a subject of controversy due to its intrusiveness and potential for negative impacts.

In Albania the inherent controversy of interceptions is exacerbated by an evident lack of trust into the system which is caused primarily by the inadequate and poorly performing accountability mechanisms. The legislation, for both security and judicial interceptions, provide some form of accountability, mainly in the phase of the authorization of interception warrants.

According to EHtCR, and the EU standards, effective accountability systems entail the involvement of a plurality of actors and require a continuity of controls and oversight before, during and after the utilization of interactions. The general approach of the Venice Commission is that oversight should be a combination of: executive control; parliamentary oversight; expert bodies; judicial review.[51]

However, the mere existence of such mechanisms is not sufficient, as the bodies involved should be provided with adequate resources and expert knowledge, and should be accorded sufficient competences, as well as be transparent.

A positive development in this respect is the introduction of a judicial scrutiny in the law on interceptions. However, being limited to only the authorization phase of the interception procedure this will not enough to prevent the potential abuses that may occur in the follow up stages of the process.

There is a very fine line between lawful and unlawful interception and this is primarily dependent on the legal and regulatory framework, but not only as it should be followed by the policies and procedures involved in monitoring of interception processes and its use.

The eroded trust in the security and judicial institutions, due to the frequent corruption and abuse of power will require much more efforts to be restored.

As shown in the Table 2, the legislation on interceptions fails to fully meet the minimum quality of law requirements set by the EHtCR and if not addressed this may lead to negative consequences for both the effectiveness of the interceptions and the legitimacy of the processes.

Against this setting the following recommendations may be drawn.

> The law on interceptions should be further improved to meet at least the minimum safeguards defined by the EHtCR.

> The law on interceptions should define the nature of the offences which may give rise to an interception order.

> The law on interceptions should define categories of people liable to be subject to interception of communications.

51 European Commission for Democracy through Law (Venice Commission). Update of the 2007 Report on the Democratic Oversight of the Security Services and Report on Democratic Oversight of Signals Intelligence Agencies adopted by the Venice Commission at its 102nd Plenary Session (Venice, 20-21 March 2015). CDL-AD(2015)006-e. Strasbourg, 7 April 2015. http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)006-e

> The law on interceptions should clearly establish the distinction between lawful and unlawful interceptions in order to avoid any interpretation and allow for abuses.
> The law on interceptions should include safeguards on the interceptions of so called privileged communications that might involve journalists, whistleblowers, lawyers, etc.
> The legislation for both security and judicial interceptions should be improved to address the vacuum on the use of interceptions of oral communications in privately owned locations.
> The legislation should clarify the use of interceptions by SPAK, given that this institution is expected to use both security and judicial interceptions while these two processes have so far been conducted separately.
> Given that the improved legislation alone is not sufficient to guarantee its proper implementation accountability should be strengthened by improving the existing control mechanisms and by establishing the required oversight ones.
> The Venice Commission's general approach is that oversight of institutions conducting interceptions should be a combination of different institutional layers that include: executive control; parliamentary oversight; expert bodies; judicial review.[52] Therefore steps must be undertaken to address the omissions and shortcomings identified in the four components.
> The executive should exercise ex post control of the activities of the agencies entitled to use interception of communications and to prepare and made public annual reports covering activities involved, statistics, policy issues, etc. The report should be presented to the parliament by the government for debate.
> The parliament should establish the parliamentary committee in charge of ""overseeing the implementation of the interception legislation.
> The parliament should make efforts to adopt legislation to establish expert independent body in charge of exercising regular ex post controls over the implementation of the laws and regulations. The French "Commission nationale de contrôle des techniques de renseignement",[53] the British "Investigatory Powers Commissioner",[54] or the Belgian "Comité permanent de controle des services de renseignement et de surete",[55] could be taken as examples.
> The independent institutions, namely the Peoples' Advocate and the Information and Data Protection Commissioner, should be engaged to exercise ex post controls to ensure that the existing legislation is implemented adequately and to propose legislation improvements according to their mandates.
> The judiciary should ensure involvement in the ex post oversight of the processes following the authorisation of the interception warrants.

52 European Commission for Democracy through Law (Venice Commission). Update of the 2007 Report on the Democratic Oversight of the Security Services and Report on Democratic Oversight of Signals Intelligence Agencies adopted by the Venice Commission at its 102nd Plenary Session (Venice, 20-21 March 2015). CDL-AD(2015)006-e. Strasbourg, 7 April 2015.
http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)006-e
53 https://www.cnctr.fr/
54 https://www.ipco.org.uk/
55 www.comiteri.be

References

Articles

Arjan Dyrmishi. “Interception of Telecommunications in Albania: Legislation and Practice”, Policy Series II, Institute for Democracy and Mediation 2010.http://idmalbania.org/wp-content/uploads/2014/10/interception-of-communications-in-Albania_June-2010.pdf

Jason Norman. "Taking the Sting Out of the Stingray: The Dangers of Cell-Site Simulator Use and the Role of the Federal Communications Commission in Protecting Privacy & Security." Fed. Comm. LJ 68 (2016): 139

Laws and regulations

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications) art. 5, 2002 O.J. (L 201) 37, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri= CELEX:32002L0058:en:HTML

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC, 2006 O.J. (L 105) 54, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF
EURALIUS. Justice Reform.http://www.euralius.eu/index.php/en/library/justice-reform
European Commission. Action Plan Implementing the Stockholm Programme. Brussels, 20.4.2010 COM(2010) 171 final. https://ec.europa.eu/anti-trafficking/sites/antitrafficking/files/com_2010_171_action_plan_implementing_stockholm_programme_en_1.pdf

European Commission. (2015, April 28). Communication from the commission to

xxxxxxxxxxxxxx

the European parliament, the council, the European economic and social committee and the committee of the regions – the European agenda on security. Brussels: COM(2015) 185. https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf
Kodi Penal i Republikës së Shqipërisë.
http://www.qbz.gov.al/Kode/Kodi%20Penal-2017.pdf

Kuvendi i Shqipërisë. Vendim Nr. 66/2016. Për ngritjen e komisionit hetimor të kuvendit për të kontrolluar zbatimin e legjislacionit në fuqi për përdorimin dhe administrimin nga strukturat e Ministrisë së Brendshme dhe Policisë së Shtetit të pajisjes përgjuese "IMSI Cathcer" dhe realizimin nëpërmjet saj të Përgjimeve të Paligjshme. https://www.parlament.al/wp-content/uploads/2016/07/VENDIM-pajisja-pergjuese.pdf

Law Nr. 9157, date 4.12.2003, On the interception of the Telecommunication

Law Nr.9885, date 3.3.2008, On some amendments to the law On the interception of the Telecommunication

Law Nr.10 172, date 22.10.2009, On some amendments to the law On the interception of the Telecommunication

Law Nr. 116/2012, date 13.12.2012, On the interceptions of electronic communications

Law Nr. 69/2017, date 27.04.2017, On the interceptions of electronic communications

Law 95/2016, date 6.10.2016. On the Organization and Functioning of Institutions for Combating Corruption and Organized Crime
Prokurori i Përgjithshëm. Udhëzim Nr.1 Datë21.04. 2006, Për Përgjimet
Treaty on European Union (TEU) art. 4, para. 2, 2016 O.J. (C 202) 1, 13,
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2016.202.01.0001.01.ENG&toc=OJ:C:2016:202:TOC# C_2016202EN.01001301

xxxxxxxxxxxxxx

Reports

ECtHR, CASE OF ROMAN ZAKHAROV v. RUSSIA. No. 47143/06. 4 December 2015. https://lovdata.no/static/EMDN/emd-2006-047143.pdf

ECtHR, Dumitru Popescu V. Romania. Application nos. 49234/99 and 71525/01. 26.4.2007 https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwiXk_za-tDcAhUFyqYKHdp9C9QQFjAAegQIAhAC&url=https%3A%2F%2Fhudoc.echr.coe.int%2Fapp%2Fconversion%2Fpdf%2F%3Flibrary%3DECHR%26id%3D003-1995439-2103500%26filename%3D003-1995439-2103500.pdf&usg=AOvVaw0LD6XytJT34dXOhnVmPP81

ECtHR, Case of Iordachi and others V. Moldova. Application no. 25198/02. 24 September 2009 https://rm.coe.int/168067d212

ECtHR, Association for European Integration and Human Rights and Ekimdzhiev V. Bulgaria. Application no.62540/00. 28 June 2007.http://hrlibrary.umn.edu/research/bulgaria/AEIHR_M_Ekimdjiev_en1.pdf

European Union Agency for Fundamental Rights. "Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU - Volume II: field perspectives and legal update". Luxembourg 2017. http://fra.europa.eu/en/publication/2017/surveillance-intelligence-socio-lega

European Commission for Democracy through Law (Venice Commission). Update of the 2007 Report on the Democratic Oversight of the Security Services and Report on Democratic Oversight of Signals Intelligence Agencies adopted by the Venice Commission at its 102nd Plenary Session (Venice, 20-21 March 2015). CDL-AD(2015)006-e. Strasbourg, 7 April 2015. http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)006-e

European Union Agency for Fundamental Rights. "Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU - Volume II: field perspectives and legal update". Luxembourg 2017. http://fra.europa.eu/en/publication/2017/surveillance-intelligence-socio-lega

European Union Agency for Fundamental Rights. "Surveillance by intelligence

99 Ministry of Justice, 'Mission' <http://www.drejtesia.gov.al/misioni/>

services: fundamental rights safeguards and remedies in the EU - Volume II: field perspectives and legal update". Luxembourg 2017.
http://fra.europa.eu/en/publication/2017/surveillance-intelligence-socio-lega

European Commission for Democracy through Law (Venice Commission). Report On The Democratic Oversight of the Security Services. Strasbourg, 15 December 2015, CDL-AD(2015)010
http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)010-e

Kuvendi i Shqipërisë. "Komisioni për Sigurinë Kombëtare, Procesverbal 14.04.2017" (Minutes of Committee on National Security meetings).
http://www.parlament.al/Files/Procesverbale/Procesverbal-dat---14.04.2017.pdf

Kuvendi i Shqipërisë. "Komisioni për Sigurinë Kombëtare, Procesverbal 19.04.2017" (Minutes of Committee on National Security meetings).
http://www.parlament.al/Files/Procesverbale/Procesverbal-dat---19.04.2017.pdf

Ministria e Mbrojtjes. "Intervista e ministres së Mbrojtjes, znj. Mimi Kodheli në emisionin "Top Story" në Top Channel". 02 Maj 2014.http://www.mod.gov.al/index.php/newsroom-2/ministri-ne-media/401-intervista-e-ministres-se-mbrojtjes-znj-mimi-kodheli-ne-emisionin-top-story-ne-top-channel

Ministria e Brendshme. "Raportimi i ministrit Tahiri në Komisionin Hetimor për përdorimin e "IMSI CATCHER"". 12 Dhjetor 2016.http://www.mb.gov.al/al/newsroom/lajme/raportimi-i-ministrit-tahiri-ne-komisionin-hetimor-per-perdorimin-e-imsi-catcher

Prokuroria e Përgjithshme. "Çështja "IMSI Catcher", pezullohet nga detyra Drejtori i Përgjithshëm i Policisë, i dyshuar për "Shpërdorim detyre". "Arrest nështëpi" për dy zyrtarë të tjerë". 07.06.2016.
http://www.pp.gov.al/web/Ceshtja_IMSI_Catcher_pezullohet_nga_detyra_Drejtori_i_Pergjithshem_i_Policise_i_dyshuar_per_Shperdorim_detyre_Arrest_ne_sht_969_1.php#.WvBJDpqxWUk

Prokuroria e Përgjithshme. Raporte të Prokurorit të Përgjithshëm (2010-2017).
http://www.pp.gov.al/web/Raporte_te_Prokurorit_te_Pergjithshem_353_1.php

Prokuroria e Përgjithshme. Raporte të Prokurorit të Përgjithshëm (2010-2017). http://www.pp.gov.al/web/Raporte_te_Prokurorit_te_Pergjithshem_353_1.php

Prokuroria e Përgjithshme. Raporti Vjetor mbi Gjendjen e Kriminalitetit. Viti 2014 http://www.pp.gov.al/web/fiinal_final_raporti_pp_06_03_2015_1093.pdf
Wikileaks. "US Embassy Tirana. Overview of the Albanian Intelligence Services". 2007 December 31. https://wikileaks.org/plusd/cables/07TIRANA1090_a.html

Media articles

Balkanweb. "Përgjuesnëzyrën e Tahirit, ministry bën kallëzim në prokurori. Dyshohet se javendosinjëpunonjës". 2 Qershor 2016. http://www.balkanweb.com/pergjues-ne-zyren-e-tahirit-ministri-ben-kallezim-ne-prokurori-dyshohet-se-ja-vendosi-nje-punonjes/
Klodiana Lala. "Gjykata pushon hetimet për "Imsi catcher", Prokuroria: S'kemi mundësi të bëjmë ekspertimin". Balkanweb, 22.05.2018. http://www.balkanweb.com/site/gjykata-pushon-hetimet-per-imsi-catcher-prokuroria-skemi-mundesi-te-bejme-ekspertimin/
Lapsi. "Dëshmitë për IMSI CATCHER/ Oficerët e policisë "tradhtuan" Haki Çakon". 15 Gusht 2016. http://lapsi.al/2016/08/15/deshmite-per-imsi-catcher-oficeret-e-policise-tradhtuan-haki-cakon/
Opinion. "Përgjimet". http://opinion.al/tag/pergjimet/
Respublica. "Mungesa e teknologjisë bllokon hetimet për serverin e tatimeve dhe aparaturën e përgjimit në Ministrinë e Mbrojtjes. Prokuroria fajëson Policinë Shkencore". 3 Shkurt 2015. http://www.respublica.al/content/mungesa-e-teknologjis%C3%AB-bllokon-hetimet-p%C3%ABr-serverin-e-tatimeve-dhe-aparatur%C3%ABn-e-p%C3%ABrgjimit-n%C3%AB
Top Channel. "IMSI Catcher", Çako hesht për pajisjen: Kanjë hetim nga prokuroria". 22 Nëntor 2016. http://top-channel.tv/2016/11/22/imsi-catcher-cako-hesht-per-pajisjen-ka-nje-hetim-nga-prokuroria/
Top Channel. "Presidenti Nishani: Po përgjohet jeta private e imja dhe e familjarëve të mi ». 29 Tetor 2015. http://top-channel.tv/2015/10/29/presidenti-nishani-po-pergjohet-jeta-private-e-imja-dhe-e-familjareve-te-mi/
Top Channel. "Hetimi për pajisjen përgjuese, prokuroria nuk bën dot ekspertizën". 11 Janar 2018. http://top-channel.tv/2018/01/11/hetimi-per-pajisjen-pergjuese-prokuroria-nuk-ben-dot-ekspertizen/
Shqiptarja.com. "Përgjimi i opozitës, PD e Ylli Zyla abuzime nën emrin e NATO-s". 25 Mars 2014. http://shqiptarja.com/lajm/pergjimi-i-opozites-pd-e-ylli-zyla-br-abuzime-nen-emrin-e-nato-s?r=pop5s