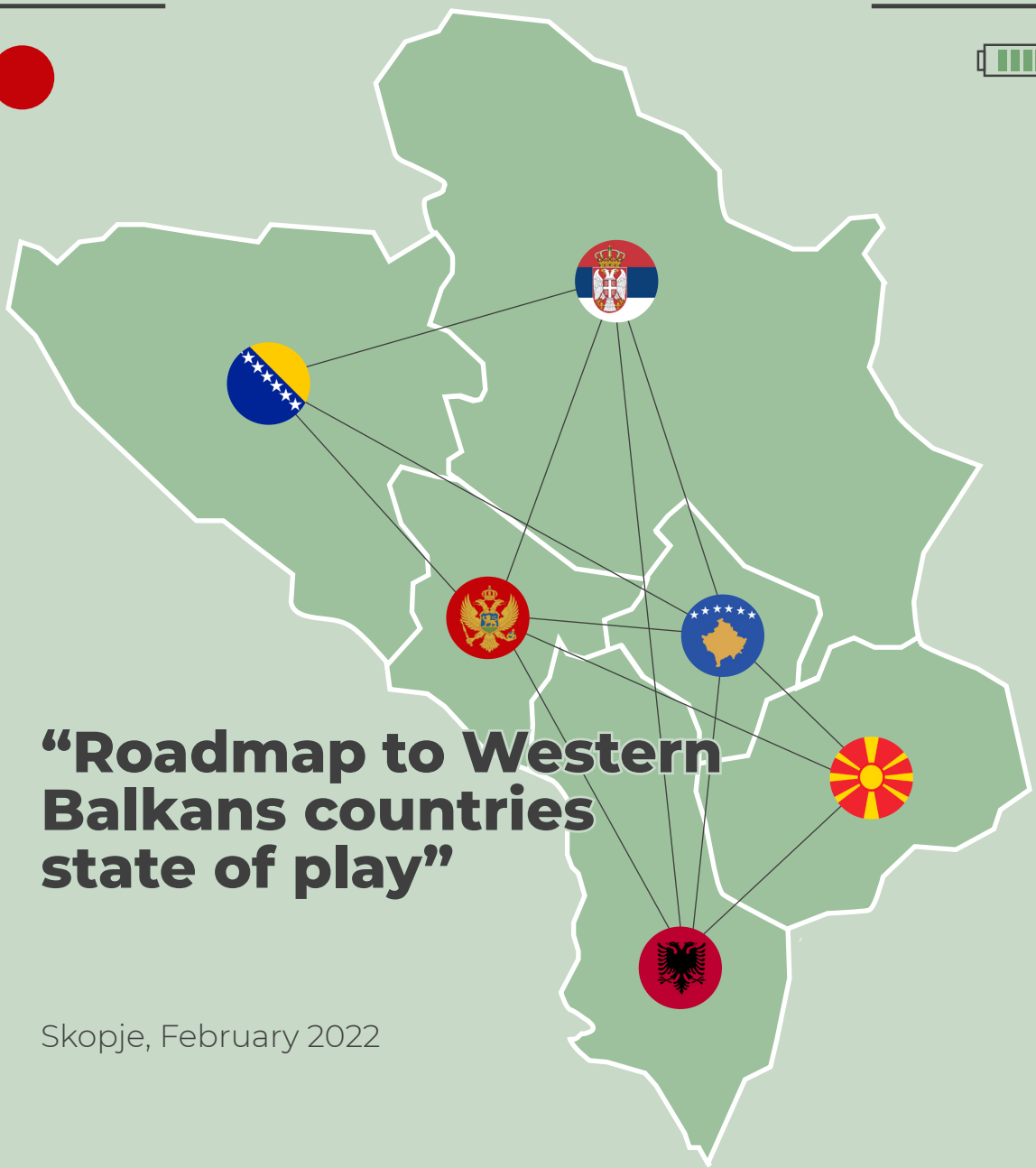
FINANCIAL DRIVERS OF SURVEILLANCE



“Roadmap to Western Balkans countries state of play”

Skopje, February 2022

IMPETUS

ABSTRACT

This research aims to present an overview of the legislation framework and the current challenges in the Western Balkan countries (Albania, Bosnia and Hercegovina, Kosovo, Montenegro, North Macedonia, and Serbia) in the area of surveillance and interception of communications.

It also goes further into documenting foreign surveillance aid in the 6 WB countries as in seeking information on foreign programs and donations to law enforcement agencies, through procurement, capacity building and/or maintenance of communications monitoring.

Video material on Financial Drivers of Surveillance in:

ENGLISH MACEDONIAN SERBIAN ALBANIAN

Disclaimer: The research was done in 2021 by IMPETUS, with collaboration and partnership with BIRN Serbia and SHARE Foundation, supported by Privacy International UK.

CONTENTS

Introduction	4
Scope of this research	6
Methodology	7
Country Findings:	9
ALBANIA	10
BOSNIA AND HERCEGOVINA	21
KOSOVO	34
MONTENEGRO	47
NORTH MACEDONIA	56
SERBIA	79
Summary	95

INTRODUCTION

Surveillance comes in many forms and is performed via several methods. One of those methods is to surveil the electronic communications, or more specifically the telephone communications' content. There is a lawful interception of communications (LIC), which is the legally official access to private communications, such as telephone calls or online communications and e-mail messages. Through the LIC, a network operator or service provider gives law enforcement officials an access to the communications of private individuals or organizations.

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.

As one of the most widely used special investigative techniques, LIC, plays a crucial role in helping law enforcement agencies to combat serious criminal activities among others. LIC is particularly useful when dealing with sophisticated organized criminal and terrorist groups to gather evidence for use in prosecutions. LIC is used also to investigate corruption and to allow the evidence collected to be admissible in courts. LIC is based on national criminal procedure legislation of each country. However, in conducting interception of communications the 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 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 mainly on the technology used. This is especially the dilemma with the privacy experts when seeing the development of new technologies and apps to store users' behavior and location. 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 Rights (ECtHR) provide number of standards, which the national laws of the Council of Europe Member States 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] defines the full compliance with fundamental rights and the guarantee for more transparency, accountability and democratic control as key principles.

1 Adopted by the EU Commission in April 2015, https://ec.europa.eu/home-affairs/system/files/2020-09/eu_agenda_on_security_en.pdf

SCOPE OF THIS RESEARCH

This research aims to present an overview of the legislation framework and the current challenges in the Western Balkan countries (Albania, Bosnia and Hercegovina, Kosovo, Montenegro, North Macedonia, and Serbia) in the area of interception of communications. It also goes further into documenting foreign surveillance aid in the 6 Western Balkan countries as in seeking information on foreign programs and donations to law enforcement agencies, through procurement and maintenance of communications monitoring. Such aid for surveillance comes in five main forms:

- Direct equipping of foreign intelligence and security forces with surveillance tech,
- Training of foreign intelligence and security forces in surveillance techniques,
- Financing of security forces' operations and procurement,
- Promoting legislation or practices which enables surveillance,
- Facilitating exports of surveillance equipment by industry, for example by promoting their business or arranging and underwriting deals.

It will also test institutions in their transparency and openness whilst sending the free access of information (FOI) requests. Latest challenges urged by COVID-19 (mobile applications to monitor the contacts of citizens and methods of collecting data on active cases of infected citizens with a clear connection with foreign support through EU programs etc.) was an interest to the research too.

Project goal

By documenting instances of such surveillance aid, it will be possible to better understand the potential developmental aid of specific programs. In doing so, it will be possible to form policy recommendations aimed at limiting abuses or improving safeguards. The aim is through research/policy analysis:

- **to document** instances using open-source sources where foreign governments or bodies have provided surveillance aid to WB,
- **to document** the effect of this aid in WB countries using open sources, testimonies, and/or interviews,

- **to highlight** shortcomings in the WB countries with regard to safeguards or governance standards that could be improved by donor countries in order to limit abuses,
- **to develop** policy recommendations aimed at their national government or international donors.

METHODOLOGY

The research applied several methods for data gathering:

- **Sending FOI requests to institutions involved in the surveillance system;**
- **Open data from media, institutions, organizations;**
- **Interviews with experts.**

In order to have a deeper understanding of certain aspects of the foreign assistance received by the state institutions, for which no official relevant quantitative and qualitative data can be collected, a semi-structured interviews were conducted. The disadvantage of this method is that the information obtained cannot be generalized and can often be subjective, based on the personal perceptions of the interviewee, but this problem is overcome by combining with secondary methods of collecting information. Thus, the information from the interviews will not be used separately, but in combination with the information obtained from other secondary methods (desk research, provided statistical data, analysis of open source content - media articles, available data, etc.).

The interviews were conducted anonymously, pre-arranged with each respondent separately, in a safe conversation environment, without recording the conversation, but only by noting the points of the conversation. The interview consisted mainly of five questions, to which the interviewees were asked to provide explanatory answers or their opinions as per the expertise. During the conversation with the interviewees, additional questions arose that were asked by the interviewer, in order to extract additional information on different aspects/segments of the topic.

Through the interview, conversations were conducted with a total of 45 persons, of which 23 men and 22 women. Their affiliation is seen in the chart below

Type of entity	Total number interviewed	Women	Men
Media/journalists	12	8	4
NGO/CSO	5		5
Academia	5	2	3
Private sector	1		1
International organizations	3	2	1
Foreign Diplomats/Embassies/ police attaches	2		2
Institutions – Law enforcement	5	2	3
Public Prosecution	12	8	4
ALL	**45**	**22**	**23**

COUNTRY FINDINGS

- ALBANIA
- BOSNIA AND HERCEGOVINA
- KOSOVO
- MONTENEGRO
- NORTH MACEDONIA
- SERBIA

ALBANIA

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 the 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 organized crime. In addition to the enhancement of the interceptions' framework and capabilities, to be used for investigation and prosecution the organized 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 organized 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.

The institutions [3] that have the right to ask/submit request for wiretapping, established by law, need to provide the data necessary for the performance of their legal duties. For the wiretapping to be performed, the institutions need to file a request and one copy of the request needs to be delivered to the Head of the Court of Appeals against Corruption and Organized Crime. All decisions to intercept electronic communications are valid for a period of up to 3 months. As per the right for information[4]: the competent state institutions, within 15 days after receiving the written request of a citizen, must inform him/her if he/she has been intercepted by communications electronically. This information is provided only after the wiretapping is completed.[5]

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

3 State Intelligence Service, intelligence / police services of the Ministry responsible for public order and safety, of the Ministry of Defense, of the Ministry of Finance and the Ministry of Justice, the National Bureau of Investigation, and any other intelligence / police service

4 https://www.shish.gov.al/files/Ligjet/Ligji%20nr.9157,%20dat%C3%AB%204.12.2003.pdf

5 https://www.pp.gov.al/rc/doc/nr_4_1414.pdf

In 2019, a total of 2,714 wiretap warrants have been released by the Albanian courts and carried out by prosecutors in 2019. This facilitated the interception of 5,574 people suspected of being involved in criminal activity.[6] The General Prosecution's annual report states that the wiretapping was carried out in the context of 717 criminal proceedings, 141 of which were Serious Crimes Prosecution cases. The number of wiretap warrants has decreased slightly from 2018, when 3,063 of them were released by courts. The report also states that the wiretapping led to the apprehension or arrest of 713 people suspected of crimes endangering public safety, people's lives, narcotics-related crimes, corruption, abuse of power, and trafficking. Data given by the report also show that wiretap warrants correlate to a 26.4% arrest rate, slightly higher than that of 2018 (23%), though still lower than that of 2017 (29%).

During 2020, the government approved a bill that gave the state police more competences for wiretapping.[7] The proposed changes[8] to legislation were that would allow the police to wiretap, track, photograph, and surveil citizens without a warrant from the prosecution office. This kind of police surveillance may last up to 3 months, and be extended once for another 3 months. The current legislation[9] stipulated that wiretapping, audio and video recording, and listening in on telephone conversation may only take place with the authorization of a prosecution office. An authorization is only granted in cases which "based on available evidence, it is suspected that someone has committed a crime or is planning on committing a crime and this criminal activity cannot be uncovered or prevented in other ways." The Special Anti-Corruption Prosecution Office has opposed[10] the government's proposal as a "serious violation of freedoms and human rights." [11]

In 2021, the Constitutional Court annulled this change. The Ombudsman Office and the Helsinki Committee in Tirana sent the case at the Constitutional Court. Under the existing law, environmental interception, audio and video recording and interception of telephone conversations can only be done with the authorization of the prosecution. This happens only in cases "when based on the available data it is suspected that a person has committed a criminal offense or is planning or organizing to commit a crime and this activity cannot be detected or prevented in other ways."

6 https://exit.al/en/2020/04/30/over-5000-people-wiretapped-by-albanian-police-in-2019/

7 https://exit.al/ministrat-propozojne-policia-te-pergjoje-dhe-gjurmoje-qytetaret-pa-vendim-gjykate/

8 https://www.parlament.al/Files/ProjektLigje/20200207130105SHTESA%20108-2014%20-%20POLICIA.pdf

9 http://www.parlament.al/Files/ProjektLigje/20181212114243ligji%20ekzistues%20per%20Policine%20e%20shtetit.pdf

10 https://shqiptarja.com/lajm/spak-dhe-olsian-cela-kunder-planit-te-policise-per-te-pergjuar-pa-lejen-e-prokurorise-shkelen-te-drejtat-e-njeriut?r=kh22

11 https://exit.al/en/2020/05/28/albanian-government-proposes-law-granting-police-unchecked-surveillance-powers

Based on a study[12], the draft Law on Telecommunications Interception was built on partial support in the tradition so far giving considerable powers to Public Prosecution, but without making the balance with the competencies of control mechanisms of the executive power, the legislation and the institutions of independence.

In these conditions, in addition to the need to be supplemented with clauses to improve the capacity of eavesdropping, taking into account also communications via the Internet, which legislation does not regulate them in any instance, it is necessary to review the entire framework to avoid abusive uses. Thus, the current framework does not have mechanisms for prevention, as well as for verifying some possible abuses, such as:

- **to guarantee** the clause that the system is separate, as technically one part can perform both functions;
- **to avoid** illegal wiretapping if the two main institutions for wiretapping would agree to use the system outside legal requirements;
- **for interceptions** in emergency situations;
- **to ensure** that approved eavesdropping devices belong to the entities under investigation,
- **for wiretapping** at the request of one party,
- **for the appointment** procedures of the staff dealing with wiretapping to ensure that they do not
- **be under pressure** and evade legal requirements,
- **for minimization** procedures in order to prevent their taking and use
- **personal information** that is invalid for the investigation, etc.

Another study[13], questions the effectiveness of lawful interceptions that have been conducted by the Albanian authorities: "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". The study also points out that there have been allegations of unlawful interceptions but there hasn't been any action to address such allegations. The study also emphasizes that there is a risk of abuse where there is a lack of effectiveness. "In the conditions of the lack of an effective accountability

12 published by the Institute for Democracy and Mediation, https://idmalbania.org/wp-content/uploads/2014/11/policy_paper_interceptimin_e_telekomunikimeve_ne_shqiperi_qershor-2010.pdf

13 "Albania's approaches in security provision and accountability of security institutions: the need for further efforts to converge with the EU policy, legislation and practices" by Friedrich Ebert Stiftung and Center for the Study of Democracy and Governance, published in 2018

system there is a risk of abuse of competences and powers and of encroachment on 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".

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 of LI, and the authorities that issue the interception warrants. In order to control the execution of the warrants, the law empowers the Prosecutor General with the competence to have the control of the commanding equipment that enables the interception.[14]

However, no procedures exist for controls to be conducted during the process of the interception. The law provides for the Prosecutor General (PG) to have access to the intercepted materials but only after the interception has been terminated. 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.

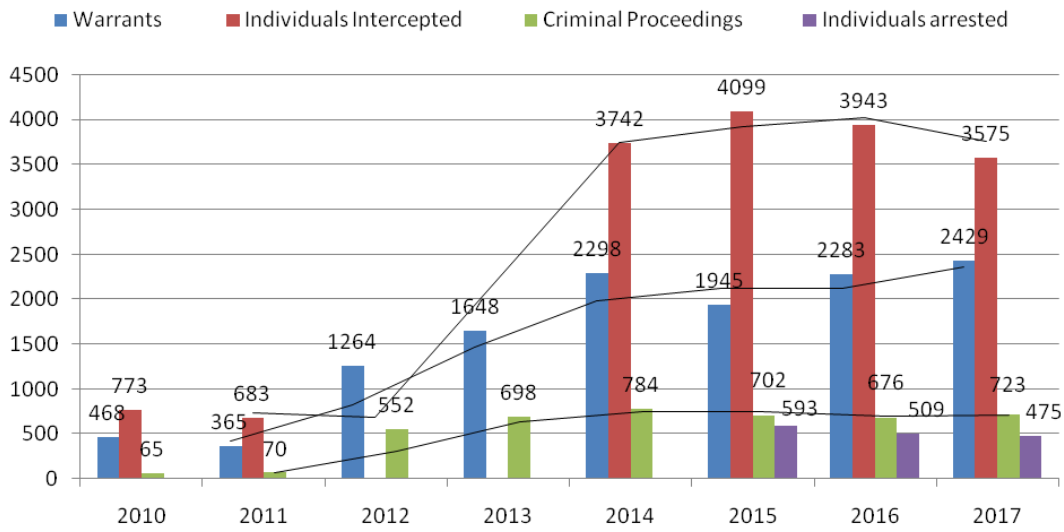
In the case of the judicial interceptions there is some form of parliamentary oversight, as the Prosecutor General reports to the parliament annually. Since 2010 there has been a chapter in the PG's annual report that is dedicated to statistics and issues pertaining to the judicial interceptions. However, 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.

14 Law on interceptions, Article 13

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.

Source:[15]

Albania's approaches in security provision and accountability of security institutions: the need for further efforts to converge with the EU policy, legislation and practices



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.

On 16 September 2021, when the program of the newly formed government was presented, the Minister of Interior, Mr. Bledi Cuci, stated that *"the territory of Albania will be controlled through technology. Once we have transformed the State Police, into one of the most reliable institutions for Albanians, and a worthy partner for the European counterpart police and beyond, we will continue its transformation through the extension of digitalization, on the one hand and high integrity from the other side. The primary role will be taken by the State Police, being the only force responsible for identifying any illegality in the territory", he said during his presentation in the Parliament. "During this mandate we will introduce the use of technology and super-intelligent equipment to combine this control, so that not a single centimeter or square meter of the Republic of Albania is violated as has been commonly done in these 30 years. And according to the principle that the Police will be the only force to identify any illegality in the territory"*, he added.[16]

15 http://csdgalbania.org/wp-content/uploads/2019/06/CSDG-FES-Publication-2018_02_02.pdf

16 https://mb.gov.al/2021/09/16/prezantimi-i-programit-politik-te-qeverise-se-re-siguria-publike/

In July 2021, The Albanian government said that it will buy military drones from Turkey for 8.2 million euros from the Albanian Ministry of Defense.[17]

The interviewed experts presented concerns about the surveillance and the violation of the human rights, as from 2011 to 2017 the number of the orders that were issued to conduct surveillance and the number of arrests that were made during this period do not match, meaning that if the number to conduct surveillance is increased logically the number of conducted arrests should be increased as well. In this period of time this has not happened. Their concern is that there might be a risk of abuse with the wiretaps that have been made, there is a risk of incompetence from the authorities, because there is not a logical explanation for the increase of the orders that have been issued to conduct surveillance. Therefore, *"At this point, the chances of (human) rights being violated are high"*. They also raised another concern about the transparency: *the responsible institutions should annually report about their performance related to national security and surveillance. Not only has there been no positive development, but there has been an attempt to move backwards in this direction"*, related to the issue of transparency, pointing out that institutions used to report about the issues of national security before.

Asked about the capacity (technical, human resources, donations), they said that *"it is difficult for this to be measured, because you can notice it in cases where the state is experiencing a crisis related to the national security or the surveillance capacities"*.

"I don't think that there is a clear legal framework" related to the question of if there is a room for the abuse of the law of interceptions regarding human rights.

For the foreign states which might have helped Albania for the equipment of surveillance, donations, training of the staff, they mentioned Italy and the United States. *"Italian authorities have collaborated with Albanian authorities several times, in cases of organized crime and cultivation of cannabis."*

It was also mentioned that the opposition has claimed that foreign officials based in Albania have been eavesdropped on and a "special equipment" used for surveillance has entered in Albania, but there hasn't been a parliamentary investigation about these claims. *The State Police has said that the equipment was being used for the training of the police officers.*

17 https://www.parlament.al/Files/ProjektLigje/20210624110658RELACION 26 TABELA AKTT 26.pdf

The FOIA requests were sent to institutions which were not answered, stating that the information that was asked was *"confidential"* and also included *"third parties"* (meaning: third states). They said that *"the information could be de-classified after 10 years"*.

As from open data research, several donors were detected mainly donating equipment and training for the MOI to suppress organized crime:

1. OSCE Presence in Albania donates IT equipment to Albanian Border and Migration Police[18]

On 16 June 2021, the OSCE Presence in Albania donated IT equipment, worth €22.000, to the Albanian Border and Migration Police. The donation includes a dozen laptops, 11 multi-media projectors, 8 multi-functional printers and 11 projection screens. The equipment will be distributed among seven Regional Directorates of the Border and Migration Police and three Border Police Commissariats to enhance the training capacities of this police force.

2. EXBS Donation of Equipment to Albanian Border and Migration Police

On defense and matters of security, the U.S. Government's staunch commitment to strengthening law enforcement in Albania is enduring. This donation of this state-of-the-art equipment, worth approximately $170,000, targets the Government of Albania's efforts to battle illicit trafficking and cross-border crime.[19]

3. US donations for Peace and Security Assistance[20]

U.S. security assistance has helped Albania build its capacity and make significant progress in its Euro-Atlantic defense-related integration efforts. The Bureau of Political-Military Affairs (PM) supports NATO interoperability and military modernization in Albania through the provision of Foreign Military Financing (FMF) assistance. In 2018, Albania became one of the first six countries to receive FMF under the European Recapitalization Incentive Program (ERIP) through the provision of $30 million in FY 2017 FMF-OCO for the purchase of

18 https://www.osce.org/presence-in-albania/489758?fbclid=IwAR1YUnmi7gQdr6ZA2XNr9U-WXwQFaz5nTj8lsyREifMkicCngk24nLDEjpuc

19 https://al.usembassy.gov/remarks-by-ambassador-kim-at-the-exbs-donation-of-equipment-to-albanian-border-and-migration-police/

20 https://www.state.gov/wp-content/uploads/2021/08/Albania_FY-2020-Country-Assistance-Fact-Sheet.pdf

UH-60 helicopters. In exchange for the ERIP investment, Albania committed $12 million in national funds to its UH-60 procurement and agreed to divest legacy Russian rotary wing platforms. Additionally, $18.2 million in FMF from FY 2018-2020, provided through the Countering Russian Influence Fund, were committed to improve the Albanian Ministry of Defense's cyber defense capabilities. The PM Bureau also oversees U.S. International Military Education Training (IMET) funding which helped integrate Albanian Armed Forces (AAF) leadership with U.S. and other Western institutions, primarily through U.S. professional military education courses for senior, mid-level, and junior officers. Although Albania does not have the overall resources of many other NATO members, it has continued to enhance its role in NATO with one of the highest percentages of uniformed personnel deployed in support of NATO operations. Albania's military capacity has increased in part because of the AAF's excellent relationship with the New Jersey National Guard. As a result of engagement by U.S. European Command (EUCOM) and the New Jersey National Guard, the AAF's Explosive Ordnance Disposal (EOD) Company recently completed the third iteration of EOD level-2 training and began construction to refurbish existing EOD ranges. Albania also re-committed to send EOD personnel to support United Nations Peacekeeping Operations, in part due to expanded capabilities and equipment provided through U.S. funding. U.S. support to the AAF has helped prepare the military to respond to natural and manmade disasters.

5. EXBS Donation Ceremony to Albanian Border Police (By U.S. Embassy-Tirana)[21]

Through bilateral partnership, funds were devoted to assisting Albania to secure its borders, and today we see some of the equipment purchased with that funding. This donation of handheld thermal imager, night vision goggles, binoculars, and other interdiction equipment, which amounts to over $60,000.00, is further evidence of our commitment to helping Albania reach its EU benchmarks.

4. The US Embassy donates investigative equipment against terrorism and other threats to the Albanian police[22]

U.S. Embassy Tirana donated and delivered $100,000 in #ATA Diplomatic Security Service funded investigative equipment to the Albanian State Police yesterday. The officials from the Embassy said that this equipment will assist their law enforcement partners in

21 https://www.facebook.com/StateINL/posts/exbs-donation-ceremony-to-albanian-border-police-by-us-embassy-tiranathe-export-/323028344486465/

22 https://www.facebook.com/permalink.php?story_fbid=10158499502695838&id=74591195837

defending Albanians by deterring terrorism, cybercrime, and other threats. U.S. Embassy Tirana's Regional Security Officer, Karen Riley and Director of Albanian State Police, Ardi Veliu reviewed and signed memorandums listing the donated items.

5. IPA Projects - EU

IPA II- SDG 16 Promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels The strategy for the Western Balkans also provides a significant contribution to the achievement of SDG 16 through the 'flagship initiative to strengthen the rule of law'; the 'flagship initiative to reinforce engagement on security and migration' and the 'flagship initiative to support reconciliation and good neighborly relations'.

6. Turkey donates Albania MPT-76 and MPT-5523, Armored cars24 and 10 minibuses to Albanian Armed Forces[25]

Republic of Turkey Ministry of National Defense of the Republic of Albania Ministry of Defense signed a technical protocol for the grant of 30 units of light infantry rifle. These weapons, Natural Disaster Supplies Turkey's Albanian Armed Forces are continuously providing grant assistance carried out next. Turkey donated armored vehicles and equipment which will be used by Albanian rapid response teams. In addition to vehicles, Turkey also donated gas masks, various protective equipment, bulletproof vests and other equipment. The minibuses produced by the renowned company "OTOKAR", one of Turkey's leading design and production centers for armored and soft-skinned 4×4 tactical wheeled vehicles, will be used for transportation of military forces to their units.

7. Albania earmarks over $9M for Turkish Bayraktar TB2 UCAVs[26]

Albania's interest in acquiring the Bayraktar TB2s became official after the country's parliament allocated an additional budget of more than 8 million euros for such procurement. The approval came after Albanian Interior Minister Bledar Çuçi and military officials paid a visit to Turkey. After visiting the Bayraktar production facility in Istanbul, Çuçi signaled that his country would likely purchase the drone. *"We are evaluating the possibility of using Turkish UCAVs for civilian and military purposes in Albania,"* he said.

23 https://en.rayhaber.com/2020/04/turkiye-arnavutluka-mpt-76-ve-mpt-55-hibe-etti/

24 https://www.novinite.com/articles/202706/Turkey+Donates+Armoured+cars+to+Albania

25 https://www.ocnal.com/2015/01/turkey-donates-10-mini-buses-to.html

26 https://www.dailysabah.com/business/defense/albania-earmarks-over-9m-for-turkish-bayraktar-tb2-ucavs

Conclusions:

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 practice and the ECtHR case law, and the lack of effective control and oversight mechanisms 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 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.

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 [27].

27 Law on interceptions 2017, article 20/1

BOSNIA AND HERCEGOVINA

In 2011, "Nezavisne novine" claimed[28] the possession of a list of "more than 5.000 mobile phone numbers" tapped over the period of three years (2008, 2009, and 2010) by OSA [*Intelligence-Security Agency of Bosnia and Herzegovina*] and SIPA [*Investigation and Protection Agency of Bosnia and Herzegovina*], "both legally and illegally". The media announced publishing the list of wiretapped numbers in the printed edition of "Nezavisne novine". Previously, Dusanka Majkic, a member of the Joint Commission for Defense and Security of the BiH Parliament, warned about illegal wiretapping in BiH and the fact that the competent commission has never received an answer that is a 'convincing enough'. *"We are sure that a large number of people are being eavesdropped in this country, especially those in politics, and we are sure that it is being done in an illegal way, however, the security agencies must address this. Motives for illegal wiretapping are mostly political."*, said Majkic.

Two days later, the Ministry of Security of BiH published the official position of the Ministry of Security[29] regarding the text published in "Nezavisne novine" on April 12, 2011 entitled "OSA and SIPA eavesdrop on thousands of citizens". The Ministry of Security of BiH claimed to take an extremely serious approach to verifying the allegations and the genuineness of the list published. The Minister of Security of BiH at the time, Sadik Ahmetovic, asked the Prosecutor's Office of BiH to initiate an investigation to determine all the circumstances related to the unauthorized disclosure of data on telephone numbers related to the published text, as well as the responsibility of all persons involved in these activities. Upon conducting an investigation and determining all the circumstances that lead to the publication of the list, the Ministry of Security of BiH stated it will *"inform the public about it in a timely manner"*.

In 2012 the European Commission Progress Report in Bosnia and Herzegovina[30], reported: *"The rules of the Council of Ministers about the participation of the Agency for Personal Data Protection in relevant legislative processes are not satisfactory. The principle of pur-*

28 https://www.nezavisne.com/novosti/bih/EKSKLUZIVNO-Nezavisne-u-posjedu-spiska-brojeva-telefona-OBA-i-SIPA-prisluskuju-hiljade-gradjana/85891

29 http://msb.gov.ba/vijesti/saopstenja/default.aspx?id=5987&langTag=bs-BA

30 https://ec.europa.eu/neighbourhood-enlargement/bosnia-and-herzegovina-progress-report-2012_en

poseful use and by-laws regulating the protection of personal data by the police have still not been fully implemented. The Law on Personal Data Protection does not apply to the Bosnia and Herzegovina Intelligence and Security Agency. Overall, preparations for personal data protection are still at an early stage. It is necessary to ensure the independence of the Agency for Personal Data Protection."

In 2013, Zoran Cegar[31], the Head of the Intelligence Sector of the Crime Police Service of the Federal Police Administration at the time, upon returning from a secret mission in several cities in Hercegovina, said that the police agency illegally monitored and eavesdropped on thousands of politicians, government officials and businessmen -among others - to collect compromising material. He announced an investigation and the filing of several criminal charges against the former administration. *"It is certain that what was done while Zlatko Miletic[32] was the director of the Federal Police Administration (FUP) is no more and will not be done any longer - secret surveillance of politicians and high officials, surveillance of their wives and mistresses, mounting processes...,"* said Cegar. He claimed wiretapping occurred on a large scale: "*FUP illegally monitored a huge number, thousands of people, illegally tapping their telephone conversations and monitoring and cutting off communications. We are investigating all this now, it is not yet time to talk about the details, and when we process everything, we will call the owners of cell phones and telephones who were llegally and illegally tapped to contact me in person and file a lawsuit together to order the perpetrators and actors. The police are not and will no longer be anyone's private means of playing with citizens*". A month after, media reported[33] that Cegar denied these statements and accused journalists of "misinterpreting" his words, despite the fact that he repeated the same claims in several other media after the initial interview for "Dnevni list".

In March 2014, "BH Novinari", the association of journalists in BiH, dedicated their monthly newsletter[34] to wiretapping scandals, especially eavesdropping as a method used by powerful people and political parties to blackmail and intimidate journalists and *"put the media under their paw"* as a well-established practice throughout the region. Many media workers called for those who wiretapped journalists to be prosecuted and punished in accordance with the law and underlined the importance of informing the public about such

31 https://radiosarajevo.ba/vijesti/bosna-i-hercegovina/zoran-cegar-o-tajnom-prisluskivanju-u-fbih/110273

32 https://balkantimes.press/en/shocking-interview-of-zlatko-miletic-a-man-who-knows-everything-about-politicians-i-know-everything-they-have-gone-through-my-investigations/

33 https://www.slobodna-bosna.ba/vijest/7653/afera_prisluskivanje_zoran_chegar_negira_vlastite_izjave.html

34 http://bhnovinari.ba/wp-content/uploads/2012/06/bhn_e-novinar-mart2014.pdf

abuses. The Director of the Agency for Personal Data Protection of BiH warned[35] about general lack of interest in illegal wiretapping occurring in BiH.

WikiLeaks[36] about spying software used in BiH by OSA [Intelligence-Security Agency of Bosnia and Herzegovina].

Fin Fisher spying software is used among 32 countries of the world, including Bosnia and Herzegovina, which has not been officially confirmed. Many unofficial sources say that in the last 10 years the Ministry of interior of Republic of Srpska, The Border Police of Bosnia and Herzegovina together with the Intelligence security agency (OSA) have shown interest in this equipment. According to a study conducted by the Citizen Lab (Department of Research, University of Toronto), Fin Fisher is the most widely used software of government agencies in the world for spying. Unofficial sources say that the Border Police of BiH has already tested the Hacking Team software. Some sources say that Citizen Lab was able to track IP addresses and C&C agencies in ten countries around the world.

Global Information Society Watch (GIS Watch) report for 2014 was dedicated to surveillance topics themed "Communication surveillance in the digital age". The report on Bosnia and Herzegovina, "The continuum of surveillance in Bosnia and Herzegovina"[37] quotes: *"There is a pattern to all these scandals: the existence of parallel systems for intelligence structures that control legitimate security institutions – the result of former war intelligence agencies that never quite went away, and were not brought under the control of the new system*. Regardless how many reforms and new bodies are created, the constant practice of spying on people survives, and the authorities – as well as other interest groups – access the data held by public assets such as telecoms providers without court orders. Eavesdropping appears to be routine, which gives political leaders and their parties material for blackmailing and intimidating rival politicians, their partners and journalists. As Petar Kovacevic, director of the Agency for Personal Data Protection, said in an interview: *"In 2007 the Council of Ministers formed a Joint Committee for the lawful interception of telecommunications, which has the authority to adopt procedures that govern the operation of telecoms operators."* In this way it annuls the power of the Agency. It is important to know that the current chairperson of this committee is the deputy minister of security. When, in 2013, the agency checked on the three telecoms operators (BH Telekom d.d. Sarajevo, Telekom Srpske a.d. Banja Luka, and JP Hrvatske Telekomunikacije d.d. Mostar), to verify the lawfulness of personal data processing, and to understand if interception was taking place

35 https://avaz.ba/vijesti/intervju/127943/izgleda-da-nikoga-u-bih-ne-zanima-nezakonito-prisluskivanje

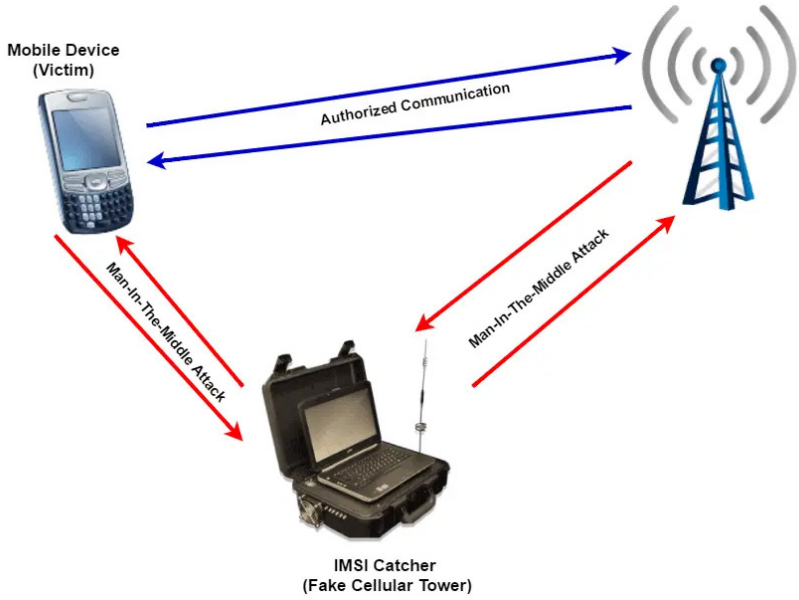
36 https://www.klix.ba/vijesti/bih/wikileaks-i-bih-spijunira/140916096

37 https://giswatch.org/en/country-report/communications-surveillance/bosnia-and-herzegovina

using court orders, the operators simply did not allow access to documents, claiming that they were "confidential". As a result, the agency could not determine anything.

In 2018 Freedom of Information requests (FOI) in Finland have revealed[38] that the Finnish Government granted export licenses for the sale of international mobile subscriber identity-catchers (MSI-Catchers) to governments including **Bosnia and Herzegovina**, Colombia, Indonesia, Kuwait, Macedonia, Mexico, Morocco, Serbia and the United Arab Emirates.

In 2019 The Parliamentary Security Committee of the Federation of Bosnia and Herzegovina announced[39] asking the Federal Police Administration (FUP) on whether it misused the police devices used for wiretapping. This referred to the police simulator of the base station, the so-called "Catcher[40]", which has the ability to change the content of SMS messages, which only a small number of people in the intelligence structures know about, and which is owned by the FUP. The media article suggests that all three security agencies have catchers (example shown in the photo).



In 2019, the media reported[41] on the Intelligence-Security Agency of Bosnia and Herzegovina (OSA) procurement of telecommunications monitoring systems. According to the Information on the implementation of multi-year projects in BiH institutions, which was submitted to the BiH Parliamentary Assembly by the BiH Ministry of Finance and Treasury, OSA is procuring a system for monitoring telecommunications. The document states that the realization of two projects "Renovation of the vehicle fleet" and "Procurement of special

38 https://www.vice.com/en/article/wj75yq/imsi-catcher-exports

39 https://avaz.ba/vijesti/bih/458763/kome-kecer-sluzi-za-nezakonito-prisluskivanje

40 https://en.wikipedia.org/wiki/IMSI-catcher

41 https://www.klix.ba/vijesti/bih/osa-bih-nabavlja-sistem-za-pracenje-telekomunikacija/190513096

equipment" is in progress, and the available funds for these projects on October 1, 2018 amounted to 2 million KM[42].

In 2020 the member of the Presidency of Bosnia and Herzegovina, Milorad Dodik, at the session of the National Assembly of the Republika Srpska (NARS), said[43] that *he participated in the wiretapping of members of the opposition in RS*[44]. Dodik later said[45] that his statement regarding wiretapping the opposition was *"just a performance"*. The Transparency International in Bosnia and Herzegovina (TIBiH) filed a criminal complaint[46] with the Prosecutor's Office of Bosnia and Herzegovina against Dodik on suspicion of committing the crime of unauthorized wiretapping. Branislav Borenovic, president of the PDP party, has filed a criminal complaint with the Prosecutor's Office of Bosnia and Herzegovina against Dodik, for the criminal offense of "Unauthorized Eavesdropping and Sound or Optical Recording", reports Anadolu Agency (AA)[47]. Dario Sandic, a member of the SDP BiH's Main Board from Banja Luka, filed a criminal complaint against Dodik[48], and Dragan Lukac, RS interior minister, based on Dodik's public confession to illegally wiretapping the opposition. A criminal complaint was filed due to a well-founded suspicion that Dodik and Lukac committed criminal acts of unauthorized wiretapping and audio recording, violation of the equality of citizens and abuse of official position or authority. Five months later, Milorad Dodik condemned[49] the wiretapping of the Head of the Prijedor branch of the Republika Srpska Health Insurance Fund, Dalibor Pavlovic, who is also the party's candidate for mayor of Prijedor in the than upcoming elections.

The level of surveillance awareness amongst citizens of Bosnia and Herzegovina is close to non-existent - a large part of it being the *"I have nothing to hide"* state of mind. Though mass-surveillance has never been a public theme as such, it does not mean it is not there; especially considering how little substantial information which are of public interest government institutions (are willing to) offer even when citizens and/or media are calling upon freedom of information rights. Per Transparency International findings[50], Bosnia

42 Convertible mark - KM– official currency of BiH

43 https://www.youtube.com/watch?v=ezXzmNo7nAs

44 https://www.klix.ba/vijesti/bih/milorad-dodik-rekao-da-prisluskuje-opoziciju-u-rs-u-znamo-sta-radite/200520176

45 https://balkans.aljazeera.net/news/balkan/2020/5/21/dodik-o-prisluskivanju-bio-je-samo-performans

46 https://radiosarajevo.ba/vijesti/bosna-i-hercegovina/ivana-korajlic-ocekujemo-saslusanje-dodika-zbog-prisluskivanja/377816

47 https://www.aa.com.tr/ba/balkan/borenović-tužilaštvu-bih-podnio-krivičnu-prijavu-protiv-dodika-zbog-prisluškivanja/1849127

48 https://radiosarajevo.ba/vijesti/bosna-i-hercegovina/sandic-podnio-krivicne-prijave-protiv-dodika-i-lukaca/377927

49 https://mondo.ba/Info/Politika/a996469/Dodik-Neprihvatljivo-prisluskivanje-bilo-koga.html

50 https://ti-bih.org/bih-medju-zemljama-u-kojim-se-stanje-korupcije-najvise-pogorsava-gradjani-zivotno-ugrozeni/?lang=en

and Herzegovina is the most corrupt country in the Western Balkans region, which also makes digital security and privacy of its citizens as fragile as it gets. Activists use the internet and in particular social networks, such as Facebook and Twitter, to engage the public and to organize protests against the political establishment. There are dozens of articles in the media or even statements by government officials on wiretapping and (illegal) interception by intelligence agencies. The information about surveillance equipment in the country, its usage, government's capacity to use it, and ways it has been obtained (public procurement or via donations) are not readily available. Lack of transparency in this matter is rather chilling.

General ICT-related context on infrastructure

Bosnia and Herzegovina approved the first national law related to communication affairs, with a particular focus on electronic communications and ICTs in 2003. The International Telecommunication Union (ITU) in 2018 published a profile[51] for Bosnia and Herzegovina which states that hard infrastructure in the country is quickly evolving, including availability of fixed and mobile broadband connectivity in both urban and rural areas (data or any *information on meaningful connectivity*[52] in the country is *not addressed in this document*).

When it comes to information and communications technologies (ICTs), one of the BiH's milestones is the adoption of Policy of Electronic Communications Sector of Bosnia and Herzegovina 2017-2021[53], which is in line with the Digital Agenda of Europe's "Indicative Strategy Paper for Bosnia and Herzegovina for the period 2014-2020[54]".

In relation to the connectivity agenda, the strategy paper cites "However, further work is needed to identify investment projects in other relevant sectors such as environment, based on prioritization criteria, involvement of key external stakeholders and including the technical and financial abilities for implementing these projects within the medium- (and long-) term budget framework, thus creating a single pipeline of infrastructure projects and considering the available fiscal space. [...] With a view to creating a dynamic for economic and social development in Bosnia and Herzegovina, an integrated approach under ***IPA II*** will aim at strengthening competitiveness and innovation, including through increased research capacity and further development of the telecommunication sector, private sector and tourism sector, as well as through promoting local economic develop-

51 "ITU Measuring Information Society Digital Innovation" https://www.itu.int/en/ITU-D/Innovation/Documents/Publications/eBAT_Brochure%E2%80%93DIP%20BosniaH_431106_.pdf

52 https://gdc.unicef.org/resource/meaningful-connectivity-unlocking-full-power-internet-access

53 http://www.sluzbenilist.ba/page/akt/WBr1TX3CmYY=

54 https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/20190529-bosnia-and-herzegovina-analytical-report.pdf

ment by building local partnerships between municipalities, SMEs, education and training institutes, as well as civil society. Investments in further digitalization of the country are also needed to roll-out for example large-scale broadband infrastructure projects to address low penetration rates, rural-urban divide; but also to prepare the business environment for a digital transformation. Assistance to the trade sector, including state aid, competition and intellectual property rights will follow up to the previous support under IPA. Support to Quality Infrastructure (QI) is conditioned to the existence of a credible and relevant countrywide QI Strategy."

In 2019 Bosnia and Herzegovina has introduced the 4G network but it still lacks a national broadband strategy, which is directly related to the development of broadband infrastructure in the country in terms of both market competitiveness and growth in the ICT sector.

Interviews with relevant institution representatives

During the interview with an interlocutor[55] from the ***Intelligence-security agency of Bosnia and Herzegovina (OSA-OBA)*** the following information have been obtained:

The technical equipment and devices for audio and/or video recording and surveillance have been both purchased from budget funds and donated from a foreign country and/or organization; however, *"much have been purchased from budget funds"*. The United States of America has been indicated as "*the biggest partner*" in terms of foreign assistance and/or support. Staff from the technical departments were trained in Banja Luka, in order to obtain knowledge on techniques for audio and/or video recording/monitoring and technical equipment. *"And I know that these trainings are often organized."*[56]

The interlocutor has stated with certainty that from 01.01.2015., OSA-OBA have not received any foreign financial assistance (engagement of experts) for developing/amending the legal framework related to audio and/or video recording and surveillance.

When it comes to procurement of technical equipment, devices, software or trainings for officers to use and handle such equipment or software, it has been indicated that that such activities happen in closed circles, where a limited number of people from OSA-OBA are invited and where they are presented with these types of equipment.

The state has enough capacity, when it comes to human and even technical resources. However, *"the outcome depends on the courts and prosecutor's offices. If they don't do*

55 *Identity, previous, and current position familiar to the researcher*

56 Question indicated the training taking place from 1.1.2015. till the date

the job properly, we work in vain". The challenge is with the professional staff, particularly their salaries, especially for IT engineers. *"Why would they work for us or some other security intelligence within the structure, for a salary of 1,600 KM*[57] *when they can earn three times more working for the private sector in their industry."*

BiH should seek help from more developed countries, especially the United States, *"which is our biggest and sincerest partner"*.

When it comes to foreign assistance/support in the field of privacy protection in the last five years, the interlocutor has stated that the legal basis already exists. Help from the European countries was present, since domestic laws relied on some European laws. *"It is certainly one of the types of professional help that needs to be upgraded"*.

The special technical devices and equipment and their software that enable the implementation of interception of communications without the mediation of OTA and the operators from Art. 17 of the Law on Interception of Communications (so-called IMSI catchers) are, to the knowledge of the interlocutor, exclusively purchased from budget funds. There are well-developed systems in place for intercepting communication. *"There are signed contracts with Telecom operators (BH Telecom and HT Eronet) and there is a dedicated person working on these interceptions."*

During the interview with an interlocutor[58] from the ***State Investigation and Protection Agency of Bosnia and Herzegovina (SIPA)*** the following information have been obtained:

When it comes to procurement of technical equipment, devices for recording and surveillance are in "99% of cases" purchased from budget funds. The Directorate for Coordination of Police Bodies organizes training for the use of techniques for audio and/or video recording and surveillance and handling of technical equipment. According to the interlocutor, no one *"from my surrounding has attended such training in this period*[59]*"*.

SIPA did not receive any kind of financial aid from 01.01.2015 until now, for developing/amending the legal framework related to audio and/or video recording and surveillance. The existing legislation is good, however in practice it does not work. Staff have access *"to all the bases and have regular controls",* but the biggest problem present telecommunications operators. *"They sell data, which they buy from Viber and other networks."* From the technical point of view, it is estimated that the equipment is below the expected level.

57 *Bosnian currency, convertible mark*

58 *Identity, previous, and current position familiar to the researcher*

59 Period from 01.01.2015. till the date of the interview

"We are not able to penetrate Viber or WhatsApp applications. Cameras at border checks are mostly either turned off or out of order. SIPA does not have access to these cameras, *"and the government is to blame for that"*. The cameras are also poorly maintained. For SIPA, it is difficult to obtain videos from these cameras when they request it. They also do not have access to the ITA data. *"That is one "well-bound system of protection of crime and corruption in this country."* There is a *"total lack of coordination"* between police and other agencies. *"There is a need for improving legislation. Access to personal data is under control. The rest should be improved by asking for foreign assistance. Help should be sought from developed countries that already have developed mechanisms, such as: Germany, Slovenia or other EU countries"*.

When it comes to actually receiving aid/support from foreign countries the interlocutor is not sure but believes this happened. *"I know that the Israelis offered us some base stations to monitor and intercept conversations."* Croatia bought these stations from Israel, *"I don't know about us"*.

The interlocutor knows that SIPA has special technical devices, equipment, software that enable the implementation of interception of communications without the mediation of OTA and the operators from Art. 17 of the Law on Interception of Communications (so-called IMSI catchers). It is possible that these were obtained through the International Criminal Investigative Training Assistance Program (ICITAP- USAID). It is a fact that the Ministry of the Interior of Tuzla Canton received monitoring equipment two years ago, but it has never been installed or trained to use it in the past two years. Per the interviewee, such equipment, devices and software were obtained "from different ICITAP countries". Interviewee does not know if SIPA has received any foreign financial assistance (engagement of experts) to develop a legal framework (laws, bylaws, procedures, etc.) related to interception of communications.

Official statements from foreign country representatives

On his official LinkedIn account, the US Ambassador to Bosnia and Herzegovina wrote that he spoke with BiH Communications and Transport Minister Vojin Mitrovic about the importance of ensuring the security of all data and communications transmitted over 5G networks and the United States government's initiative for "clean network traffic coming to our facilities." Later that year, the US Embassy to BiH via official Twitter account informed the public[60] about the Embassy's meeting with leaders from BiH telecommunication sector where they spoke about safety and security of data and communication services for BiH citizens, businesses, governments, and critical infrastructure. The signing

60 https://twitter.com/USEmbassySJJ/status/1316462411856175108

of the US Government's initiative for *"a clean network, which among other things calls for the use of telecommunication equipment only from trusted providers"* has also been discussed at the meeting[61].

The Ministry of Communications and Transport of BiH published a statement[62] informing the public about a telephone meeting between the minister, Vojin Mitrović, had with the Deputy Chief of Mission at the U.S. Embassy in BiH, Ellen Germian, to discuss second and third phase of digitalization and its spreading to the entire territory of Bosnia and Herzegovina, preceded by a meeting with the U.S. Ambassador, H.E. Mr. Eric Nelson. They also spoke about issues of cyber security, secure data exchange and safe networks. *"They agreed that special attention should be paid to this issue in order to enable the secure exchange of data and information."* Mitrovic noted that the adoption of legislation to define more precisely cyber security area lies ahead of Bosnia and Herzegovina, after which it will be necessary to implement technical solutions that would define and resolve the network security problems.

FOI requests and answers:

State Investigation and Protection Agency, SIPA: *"We inform you that, taking into consideration the specific features of the equipment used for carrying out police work and tasks, we are not able to disclose the type, quantity and value of the equipment or what types of trainings have been attended by state investigation and protection agency police officers, who use the mentioned equipment in their work."*

Ministry of Interior of Canton Sarajevo: *"The request of the Balkan Investigative Reporting Network from Sarajevo for access to information to the Ministry of Interior of Sarajevo Canton, requesting information on training and procurement of audio and video recording equipment, monitoring, handling of technical equipment and devices, is completely rejected."*[63]

61 https://twitter.com/USEmbassySJJ/status/1316462414687342592

62 http://mkt.gov.ba/publication/read/ministar-mitrovi%C4%87-odrzao-telefonski-sastanak-sa-zamjenicom-germain?pageId=48&lang=en

63 Explanation - The Balkan Investigative Reporting Network from Sarajevo submitted a request for access to information in which it requested information regarding the training of persons and the purchase of equipment for audio and video recording, monitoring, handling of technical equipment and devices. Inspecting the submitted request and the documentation available to the Access to Information Officer, it was determined that the submission for requested information is subject to legal exceptions provided for in Article 5 in conjunction with Article 6, paragraph 1, items 1 and 2 of the Law on Freedom of Access to Information in Federation of BiH. Namely, the competence of the Police Administration pursuant to the Law on Internal Affairs of Sarajevo Canton is, among other things, criminal intelligence collection and analysis of information and data related to prevention, detection and investigation of crimes and misdemeanors in the Canton in accordance with law. Accordingly, the provision of information on training of technicians for audio and video recording, monitoring, handling of technical equipment and devices as well as their procurement would cause significant damage to the legitimate goals of the Federation, specifically the goal of public safety, crime prevention and crime detection.

Federal Police Administration/Interior Ministry of Federation: *"Concerning the other questions in your request, in a letter no. 11-11/5-04-3-2505/21 dated November 9, 2021 the Support Sector of the Federal Police Administration submitted the information that the Department for Operational Supervision and Technology of the Support Sector uses the available equipment for audio/video recording etc. in accordance with received orders of competent courts, relating to the active cases. The equipment was purchased from the budget of the Federation of BiH, and in the upcoming period certain donations are expected as well, as part of which a certain training of police officers on the use of the donated equipment has been agreed. Also, the training of police officers of the Department for Operational Supervision and Technology is carried out in accordance with the needs expressed in certain situations, as well as through regular annual trainings organized by the Federal Police Administration for all police officers."*

Interior Ministry of Republika Srpska: *"Concerning your questions, we inform you that the procurement of equipment listed in your query is carried out in accordance with Article 10 of the Public Procurement Law, once the level of secrecy has been established and/or it is about a contract whose execution requires special security measures. Also, in case of a donation, the receipt and recording of donations in the Ministry of Internal Affairs is done in accordance with the Instruction for Donations in the Ministry of Internal Affairs while strictly complying with the above-stated measures referring to the special purposes equipment. The concrete query did not sufficiently clearly specify what technical equipment it referred to, so in connection with all the aforesaid and in accordance with Article 5, Point (a) in conjunction with Article 6, points (a) and (b) of the Freedom of Access to Information Act, there is an exception to the disclosure of the requested information."*

In the procedure of examining the public interest in terms of Article 9, paragraphs 1 and 2 of the Law on Freedom of Access to Information of FBiH, reviewing the applicant's request, and taking into account any benefits and harms that may arise from disclosing information, it was determined that it isn not in the public interest. Namely, the public interest includes the general well-being and well-being of the community, or the benefit realized by all citizens or the vast majority of citizens in the community (local, regional, state or national), and through the activities of certain authorities or organizations powers. As it follows from the Applicant's request that he addressed the request in his personal interest and not in the interest of the community, and that he did not state the circumstances on the basis of which it would be established without any reasonable doubt that the communication of requested information is justified, the officer determined that there is no justified public interest in submitting the requested information, regardless of the exception determined in accordance with Article 8 of the Law. In determining the above, circumstances were particularly appreciated: non-compliance with legal obligations, existence of any offense, injustice, abuse of power or negligence in the performance of official duties, unauthorized use of public funds, as well as danger to health or safety of an individual. the public or the environment.

Having in mind the above, especially the fact that the submission of the requested information is not in the public interest, applying the aforementioned provisions of the Law on Freedom of Access to Information in the FBiH, it was decided as in the disposition of the decision."

Ministry of Defense of Bosnia and Herzegovina: *"Within its scope of its work the Ministry of Defense of Bosnia and Herzegovina has no competence to intercept communications, so we have not procured that type of technical equipment from the budget nor have we received it through donations. We have not sent our members to trainings on handling of such type of equipment. We have not received any sort of financial assistance for drafting/changing the legal framework referring to audio and/or video recording and surveillance. Many units of general IT and communication technical equipment have been procured for the Ministry of Defense and Armed Forces of Bosnia and Herzegovina from the budget, as well as through donations, so we have sent members of the Ministry of Defense and Armed Forces of BiH to various trainings on handling of the general IT and communication technical equipment."*

Ministry of Security Bosnia and Herzegovina: *"The Ministry of Security of Bosnia and Herzegovina has no operational competencies for conducting investigations, therefore there is no need for Bosnian security ministry employees to use the said devices and equipment or attend the mentioned training. Also, the Ministry of Security of Bosnia and Herzegovina hasn't received any other help/donations which would refer to that intent/purpose in the stated period of time.*

Border Police of Bosnia and Herzegovina: *"We inform you that, during the mentioned period, certain equipment for audio and video recording has been donated to the Border Police of Bosnia and Herzegovina by the German Embassy."*

Also, in the period from January 1, 2015 till now police officers of the Border Police of Bosnia and Herzegovina have participated in conducting training sessions organized by the Agency for Education and Professional Training Mostar, as well as other training organizers, including law enforcement agencies in BiH, law enforcement agencies of foreign countries, foreign embassies to BiH, international organizations, organizations within EU projects, as well as technical equipment suppliers. Currently, the International Organization for Migration, IOM, is carrying out activities related to procurement of specialist equipment for the needs of the Border Police of Bosnia and Herzegovina through an IPA 2020 project titled "Special Measures to Support the Response to the Refugee and Migrant Situation in Bosnia and Herzegovina" under which specialist border surveillance equipment has been delivered to the Border Police of Bosnia and Herzegovina.

We would like to mention that the Rules Governing Protection of Secret Data in the Border Police of Bosnia and Herzegovina prescribe that certain data about equipment and other material and technical assets of the Border Police of Bosnia and Herzegovina represent confidential data."

Service for Common Affairs of the Institutions of Bosnia and Herzegovina: *"A part of the technical equipment was procured within the building reconstruction project in the period between 1998 and 2000. All equipment procured after that date has been paid from the budget. Service employees have not participated in trainings on using techniques for audio/video recording and surveillance and handling of technical equipment and devices in the period from January 1, 2015 till now. As for the foreign financial support for drafting/changing the legal framework related to audio/video recording and surveillance from January 1, 2015 till now we would like to point out that there has been none and the Service, being an institution providing services, is not competent for passing/changing laws. Besides that, the Service for Common Affairs is not involved in projects for procurement of some kind of technical equipment, devices for audio/video recording and surveillance or software, or projects for training of officers in the said field."*

Concerns CSO reports

As analyzed[64] by **Privacy International**, in Bosnia and Herzegovina a wiretapping system sold by Swedish tech giant "Ericsson" was provided to the State Investigation and Protection Agency (SIPA), which has a Memorandum of Understanding with other law enforcement agencies in the country allowing them to use the system, including the Border Police. Biometric registration equipment and databases are provided to authorities for border and migration control: for example, fingerprinting devices were provided to authorities in Bosnia and Herzegovina sold by electronics company NEC; while mass-scale biometric databases are provided to numerous countries, including Senegal and Côte d'Ivoire.

While there are no indicators of security cooperation -- greatly due to the NATO engagement in the area of defense and the EU in the area of law enforcement in BiH - there have been indications of notable deals between telecommunications company BH Telecom and China's Huawei for 4G network construction throughout the country. The Clingendael Report[65] from August 2020 notes that the financial parameters are unknown, however it comes down to three solid options:

- **free supply of equipment** in exchange for company shares;
- **acquisition of exclusive rights** over the maintenance of the newly built network;
- and a **contract** that would oblige BiH Telecom to purchase Huawei equipment for the construction of a future 5G network.

64 https://privacyinternational.org/legal-case-files/4286/challenging-drivers-surveillance-eu-access-documents-requests-cepol

65 https://www.clingendael.org/pub/2020/china-and-the-eu-in-the-western-balkans

KOSOVO

In 2011, Pristina-based think tank Kosovo Center for Security Studies (KCSS) said in a report[66] that 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"*. KCSS said that 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 build, 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"*, it added.

In 2015, the Kosovo parliament approved the Law on Interception of Electronic Communications which regulates the procedures and conditions for interception of electronic communications carried out for criminal procedure needs by state institutions established by law, and procedures and conditions of interception for security needs of the Republic of Kosovo and its citizens established by Law. The law determines the rules, obligations and procedures for Network Operators and Service Providers in relation to processing of certain data by them as well as obligations and authorizations of state institutions established by law to safeguard the respect for human rights and freedoms in the process of lawful interception, as well as the oversight of the implementation of interception procedures. The law provides that the respect for human rights and fundamental freedoms recognized and guaranteed by Kosovo Constitution and European Convention for Human Rights as well as prohibition of interception without a respective decision by the court are basic guiding principles in case of interceptions.

According to the Kosovo Law on Interception of Electronic Communications, the Kosovo Police and the Kosovo Agency of Intelligence can conduct surveillance based on the Kosovo Prosecution's office. Based on this law, the authorized institutions to propose a request before the Kosovo State Prosecutor for lawful interception for the purposes of criminal procedure are: Kosovo Police, Kosovo Customs, the Police Inspectorate of Kosovo, Kosovo Tax Administration, as well as the European Mission for the Rule of Law in Kosovo – EULEX,

66 https://qkss.org/en/publikimet/pergjimi-ligjor-i-telekomunikimeve-ne-kosove-implikimet-per-sigurine

pursuant to its competencies delegated with the applicable legislation in the Republic of Kosovo.

In 2020 the latest annual European Commission's Progress Report on Kosovo[67] assesses that implementing legislation on the destruction of data adopted in January 2020 contributes to the implementation of the Law on Interception of Electronic Communications: *"The process of upgrading interception capacity in order to meet the evolving technological demands is under way. Legislation on cybercrime is generally in line with the EU acquis."*

International Support and Agreements that Affect National Security

Governmental Investment - On 30 June 2021, when Prime Minister Albin Kurti's cabinet reported on its first 100 days in office, Defence Minister Armend Mehaj said the government had allocated another 12.2 million euros for military purchases, including drones. *"We have done the review of the budget for 2021, and have re-allocated 7.7 million euros for military purchases, while the government has allocated additional funding for purchases, 4.5 million euros for military purchases alone, specifically drones,"* Mehaj said. Kosovo local media reported that on November 16, 2021, Kosovo Public Health Institute, increased its security by purchasing 45 surveillance cameras that cost 10,000 euros.

European Commission's Instrument for Pre-Accession Assistance (IPA II) (2014-2020) - One of the IPA II objectives includes safety and security, however, there are no direct projects in this field related to Kosovo. However, Kosovo benefits in the field of national security from IPA II due to assistance in regional collaboration and the EU financial assistance continues to provide support in implementing key sector reforms to advance Kosovo on its European path. In 2020 significant reprogramming efforts were undertaken to respond to the emerging needs from the COVID-19 pandemic. Under IPA 2019, EUR 38.36 million was reprogrammed to support social and economic recovery. Under IPA 2020, an amount of about EUR 11.6 million was reprogrammed in order to make available EUR 6 million under the approximation facility for possible emergency use, and EUR 5.2 million for digitalization that in principle will be focused on the economic recovery and resilience of Small and Medium Enterprises (SMEs). Some examples of results achieved by IPA II programs: 10 000 Rule of Law Professionals trained such as prosecutors, judges, barristers and lawyers.

67 https://ec.europa.eu/neighbourhood-enlargement/kosovo-report-2021_en

European Commission's Instrument for Pre-Accession Assistance (IPA III) (2021-2027) Kosovo aims to also be part of IPA III, which also includes security as one of its objectives, from which Kosovo will benefit from assistance for regional collaboration and financing to advance in certain areas, which help Kosovo towards a European path. According to the IPA III program statement "the objective of the instrument is to support the beneficiaries in adopting and implementing political, institutional, legal, administrative, social and economic reforms required to comply with the rights and obligations of Union membership, thereby contributing to their stability, security and prosperity".

Serbia-Kosovo Agreement in the White House (2020) - Both parties will commit to technology upgrades to combat illicit activities by implementing and operationalizing US-provided screening and information systems, including PICES, APIS, ATS-G, and STRP. At the White House, Kosovo and Serbia both committed not to use equipment supplied by *"untrusted vendors"* in their telecommunications networks. No firms were named, but the Trump administration has been campaigning internationally to roll back China and Huawei's role in telecommunications in Europe.

The 9-th point of the Agreement states: *"Both parties will prohibit the use of 5G equipment in their mobile communication networks, which is delivered by an unverified seller. Where such equipment is already present, both parties will commit to its removal and other efforts at mediation to do so in a timely manner."*

Due to the COVID-19 pandemic, the public auction for the 5G spectrum in Serbia has been postponed for the first quarter of 2021. Huawei has had a presence in Serbia for years, increasing its participation in big projects in the last couple of years. The company has a 150-million-euro contract with state-owned Telekom Serbia for the procurement of equipment, services and works for landline network modernization and has also been named as a partner in developing the 5G network with privately-owned Telenor. Additionally, representatives of Huawei and the Serbian interior ministry have a 'strategic partnership agreement' for the introduction of eLTE technologies and solutions for the 'Safe City' in public security systems, which opened the door to a massive surveillance system to be installed in Serbia's capital. According to the Interior ministry's reply to Radio Free Europe, details of the agreement are secret. In 2019, the Ministry of Tourism, Trade and Telecommunications signed with Huawei in a Memorandum of Understanding for the "Smart Cities" project. Same ministry signed with Huawei a strategic partnership agreement for development of the broadband network in Serbia in 2017. But it said that the White House deal had no effect on such cooperation. *"The Republic of Serbia, i.e. the Government of the RS, has*

never bought equipment for operators, neither for fixed nor for mobile, so it will not for 5G either," the ministry told BIRN. *"The agreements signed with Huawei refer only to technological solutions for the needs of state bodies, and not for public mobile systems."*

One month after Kosovo signed the so-called Washington deal, on October 16, 2020, then Prime Minister, Avdullah Hoti, held a meeting with the representatives of the Regulatory Authority on Electronic and Postal Communications. Hoti pledged in this meeting that *"Kosovo will stop the usage of 5G equipment, secured by unreliable sellers, in the communication network. Where there might be such equipment, the relevant institutions of the country will engage in their removal".*

Organization for Security and Cooperation in Europe, OSCE - On 19 November 2018 the OSCE Mission in Kosovo[68] installed indoor and outdoor surveillance cameras in the primary school Ali Hasi in the village Cërmjan/Crmljane, in the municipality of Gjakove/Djakovica, aiming a reduction of violence in schools. This was the 15-th school OSCE Mission in Kosovo equipped with cameras.

OSCE Mission in Kosovo also assists Kosovo police[69] "on legislation, supporting the implementation and revision of their strategies and action plans, and organizing training courses for law enforcement officials, judges and prosecutors on issues such as cyber and economic crimes, corruption, trafficking in human beings, forensic examination, anti-terrorism and violent extremism, illicit trafficking of drugs, hate crime and domestic violence". OSCE also has provided training for Kosovo Police and Kosovo Forensic Agency officials in mobile forensics, meaning in extracting information from mobile phones. The first training was held in April 2014.

United Nations Mission in Kosovo, UNMIK - According to United Nations Mission in Kosovo, UNMIK[70], "since 2013, *UNMIK has made 932 donations of IT equipment; 225 donations of building materials; 221 donations of portable two-way radios; 99 vehicle donations; 86 donations of truckloads of office furniture; 32 container donations; and two donations of pallet-stackers".*

On November 27, 2021, UNMIK donated IT and technical equipment including laptops, desktop computers and printers to the Court of Appeals Division in North Mitrovica.

68 https://www.osce.org/mission-in-kosovo/403556

69 https://www.osce.org/mission-in-kosovo/policing

70 https://unmik.unmissions.org/donations

Technology to Combat COVID-19

Since the first cases of COVID-19 cases in mid-March 2020, Kosovo has also tried different technological solutions to combat COVID-19. Kosovo introduced an e-platform[71] where citizens could set an appointment for themselves, or family members, to receive the COVID-19 vaccine. The platform went live on July 13, 2021. One shortcoming of the platform is that although foreign citizens living in Kosovo could receive a COVID-19 vaccine, they could not register in this platform because it only recognized Kosovo issued ID numbers.

FOI Requests:

Kosovo Police: The Kosovo police informed on one study visit and one training for capacity building of its public officials in using technical equipment for surveillance from January 2015 until September 2021. In the study visit for technical assistance and surveillance 3 public officials of the Kosovo police participated. The visit was organized by an international mission in Kosovo in the territory of another state. The Kosovo police did not specify which was the international mission that organized the study visit, not the state it took place in. Kosovo Police also replied that 15 of its public officials participated in a training for Surveillance with Technical equipment, organized by the police of another state and held at the Kosovo Academy for Public Security. The Kosovo police did not specify which state organized the training.

Ministry of Defense - Kosovo Ministry of Defense said it possesses only cameras of the office for communication with the media and the public; camera for the physical security of the military barracks; and documents which authorize the usage of the cameras and existing equipment in accordance with the needs for the registration of internal activities such as recruitment tests. No additional explanation was received.

EU rule-of-law mission in Kosovo - EULEX – In June 2016, EULEX had trained 40 Kosovo border police officers[72] *"with requirements of professional security behavior in the field, the importance of vehicle and personnel searches and to give an overview how and why the green border surveillance is important"*. EULEX said that its staff regularly participates in training courses, most of which are held by in-house experts. *"For example, the members of EULEX's Formed Police Unit participate in weekly exercises using devices such as GPS"*, an EULEX spokesperson told BIRN via email adding that *"newest international*

71 https://ekosova.rks-gov.net/Service/14

72 https://www.eulex-kosovo.eu/?page=2,11,431

staff members are trained to use handheld radios". Some examples of EULEX staff holding training that include usage of surveillance audio-visual devices include the training of three staff members of the Press Office who participated in a EULEX-organized training course on mobile journalism and learned how to use smartphones to produce video stories. The course was organized by EULEX[73] in 2019 in Pristina. EULEX said that it is not currently involved in any projects related to procurement of some kind of technical equipment, devices for audio and/or video recording and monitoring and/or software, or the training for officers in the use and handling of technical equipment for audio and/or video recording and surveillance and/or software. In 2019, EULEX procured smartphones and mobile journalism equipment. The equipment was donated to the Press Offices of the Kosovo Police, several prosecution offices and several courts. In addition, said they have donated various types of equipment to different Kosovo institutions. *"Most recently, we donated 758 items of IT, security and office equipment to the Kosovo Correctional Service, including 30 handheld GPS devices, 17 CCTV cameras, nine DVR players and 213 handheld and mobile radios[74].. In 2018, EULEX donated to Kosovo Customs[75] eight Contraband Team Inspection Kits, which will be used by the Customs Officers to enhance border and internal control operations,"* the EULEX responded.

In March 2019, EULEX, EULEX's International Police Cooperation Unit (IPCU) facilitated a training attended by colleagues from the Kosovo Police, at the Criminal Intelligence Service in Austria, as part of a program about International Police Cooperation. According to EULEX official websites, the training was part of the framework of a program called "Awareness about International Police Cooperation Principles – Study visit to the Interpol-Europol-Sirene-Single Point of Contact in Vienna, Austria". "*The aim of the project was to familiarize the participants with best European practices in the fields of handling and exchanging information, interoperability of databases and case-management practices used by European law-enforcement institutions. The central objective was to strengthen ILECU's executive capacity and enhance its operational performance, particularly from data-protection and data-security perspectives[76]"*, EULEX had informed in 2019.

In September 2018, EULEX had organized a training for Kosovo Customs and Kosovo Border Police at the Pristina International Airport *"on passenger profiling and selectivity, observation and surveillance, aircraft inspection, drug identification and risk awareness*

73 https://www.eulex-kosovo.eu/?page=2,10,1116

74 https://www.eulex-kosovo.eu/?page=2,10,2438

75 https://www.eulex-kosovo.eu/?page=2,11,764

76 https://www.eulex-kosovo.eu/?page=2,11,952

and analysis, with practical exercises to enable the customs and border police officers to tackle effectively the main security challenges when combating smuggling[77]".

The interlocutors, mainly security experts, expressed the following:

The purchase of special procurement of the wiretapping/ surveillance equipment contradicts the law of procurement because it is difficult to describe (such equipment) because none of those who offer such equipment do not dare to abide by the law of procurement, which presents a competition with at least two offers. Those (states) who offer (surveillance equipment) claim the devices are specific and costly, therefore they do not want to enter in competition with another (state) ally. *In a particular case, a device for phone wiretapping was requested for several years in a row but (international) agencies did not want to because the foreign bidder did not want to go through the public procurement process by providing data to another potential bidder from the competition. Therefore, this (process of purchasing a phone wiretapping device) was left unresolved. Each (foreign provider of surveillance devices) has come in a monopolistic way.*

An important problem, related to devices and surveillance, the police special surveillance unit and also those who operate in Kosovo, have is between the conformity with the legal obligation in the aspect of national security and the prevention of committing a criminal and human rights violation. *There are cases when people have misused their power to use Kosovo Intelligence Agency, KIA; Police or customs to wiretap someone for political needs.*

The problem of choosing the potential stakeholders of committing criminal violations, or terrorists, which relates to national security is the report with the right to privacy. I think there are essential violations of human rights. It comes to the point of presentation of the surveillance material in courts or prosecution. These institutions provide the content of the surveillance to the lawyer (of the suspect) who often publish it in the media. This creates a special, individual scandal especially if involved is a member of a political group or of a discriminated community, such as LGBT. In this case, the defense argument can be created that the person is being wiretapped as a member of the political group of a discriminated social group and not for a potential criminal violation. This makes the surveillance process difficult.

77 https://www.eulex-kosovo.eu/?page=2,11,857

There have been cases, such as the so-called Pronto affair, which has been published in the media but with a positive result because it proved what the public suspected in terms of corruption, nepotism, and tenders. Sometimes it is calculated whether it is more harmful the violation of the privacy of a person or the damage the surveillance prevented from happening, and this is balanced. The individual has a special value that the society estimates as important and it is often difficult to determine if a human right is being violated when someone is being wiretapped as a suspect for a criminal violation when, by the end of the surveillance, it is proved they did not commit. The wiretapping can prove the person is not guilty for a criminal violation they have been a suspect, but if they are a part of a discriminated group of society and the wiretapping material gets published, the group will react. If the wiretapped material gets published the privacy right of this person is violated. When it comes to the interest of the state, where international collaboration is very important to prevent global risks, we should only consider how to protect the suspect from the wiretapping to become public or to be exploited.

In reality, the legislation, especially in the field of cyber security and information technology, needs to be constantly updated due to the new developments that we encounter every day. *We must understand that in terms of the Criminal Code it is not a criminal offense if it is not foreseen, if a criminal offense in cyberspace occurs and it is not seen in the legislation the person who committed that offense cannot be punished.* There are shortcomings because there may be crimes that are not included in the legislation, on an ongoing basis.

We must keep in mind that you do not have the capacity to guard illegal wiretapping, if any person can enter the Republic of Kosovo might have wiretapping equipment and then conduct wiretapping, there is no mechanism that can make a radar to see if anyone is wiretapping. But if we talk about different technologies, for example GSM technology, where the voice is intercepted to the operators is a relatively simple and easily feasible technology with a portable device that can be placed in different places and wiretap on subjects. Kosovo also has a cyberspace challenge because there is no encrypting device for the Kosovo institutions' communications. The Republic of Kosovo does not have a unique communication system, it does not have an encrypted communication system, so the president or the prime minister communicate with security institutions similarly to how we communicate to each other on a daily basis. They do not have a secure communication system or channel (they communicate in the same way we communicate on a daily basis). This is the challenge that has existed for many years. It has not been invested in setting up a communication system. Kosovo does not have secure communication even with embas-

sies, *I am 99.9% sure that it has not yet been thought or invested, it is not budgeted, the construction of a project and the construction of a system and the use of equipment for a secure communication system.*

The lack of a secure communication system severely harms national security in all levels. Even the police institution, as a very important instrument, has attempted for years to receive investments for the creation of a communication system, a project that has been refused for many years to be financed from different donors. At the moment Kosovo police communicate with the analogue system, meaning they can very easily be wiretapped even with simple devices. Kosovo Security Forces has purchased Harris[78] equipment that offer the right security level but even those should be upgraded to offer the secret security level that is a standard of NATO[79]. *I don't think they can be upgraded without Kosovo being at least part of the Partnership for Peace (PFP).*

In the Republic of Kosovo, wiretapping is done in line with the law on electronic surveillance based on the Criminal Procedure Code. Audio-visual wiretapping is different from communication wiretapping. You can put audiovisual wiretapping even via equipment placed in open spaces and communication wiretapping where the wiretapping of mobile phone operators is done. In this case the law and the Criminal Procedure Code specifies the institutions which have the right to build capacities for wiretapping and build capacities for surveillance and the steps needed by clarifying the rooms that should be built as part of the technical mechanisms.

These capacities can be built only by the Kosovo Intelligence and Police, as monitoring rooms. The liaison office is at the state prosecution meaning that all orders for surveillance should come to the state prosecution where the signal for wiretapping is released. In the Republic of Kosovo, no surveillance can be done without a prosecutor's order within 72 hours or of the judge after 72 hours have passed, meaning no surveillance can happen without leaving a trace behind. That is how we worked for this to be (speaking as part of the working group on the law). If the police or intelligence would have direct access they could do constant surveillance and no one would know.

There have been obstacles in implementation, because the mobile operator Vala[80] had obligations to invest in equipment in accordance with the law. The office of the commis-

78 https://www.harrissecurity.com/Commercial/Access-Control-Systems

79 Kosovo cannot become a NATO member state due to not being recognized by four NATO member states

80 https://kosovotelecom.com/en/

sioner oversees the legality of the surveillance and is assigned by Kosovo Judicial Council (KJC), *but until now we haven't seen any activity, any realized report, and no control they have done*. The commissioner has the right to see whether the order has been respected. The KJC should assign a judge for this commissioner, but *I don't know if there has been any activity in this direction.* No response from the KJC so far.

EULEX is the only institution that has the right to wiretap without an order from the Kosovo state prosecution. EULEX can directly send a request for surveillance because their prosecutors are also recognized in the Republic of Kosovo.

The court does not accept proof that has not been taken with legal procedures. There are three handover interphases in wiretapping:

1. **administrative,**
2. **caller data (which connects the call),**
3. **call content (the content of the text or voice).**

The order might only be who called whom without the content. In terms of what is accepted as proof in the court, we always talk in a retrograde manner, meaning how much can you go back, meaning how much do you have the right to surveil someone. If you have been part of a surveillance, you should be notified after it ends. If the prosecution doesn't decide to initiate a case in court, then it should decide to notify the parties. A decision should also be made on what will happen to the surveilling material. In the case the procedure does not go further, the prosecutor would need to decide to delete or destroy the gathered material. *I have not heard of any case where a prosecutor has taken such a decision. In the case of taping a conversation, every material that has nothing to with the indictment should be deleted, but this has not happened and I do not see it as a practice.*

Information and Privacy Agency – The Republic of Kosovo, has regulated the issue of national security and public security for all citizens, the surveillance and the right to privacy by approving special laws and establishing special institutions which have authorization, duties, and responsibilities to deal with the security issue and the compliance with the right to privacy. The law approval for these issues is the first protective measure because it created a legal basis where in the certain laws and codes (for example the Criminal Code, the Criminal Procedure Code, the Law on Kosovo Intelligence Agency, the Law on the Police, the Law on Electronic Communications Surveillance) authorize and regulate procedures regarding the implementation of surveillance or interception measures.

However, from the point of view of the Law Nr. 06/L-082 for the Protection of Personal Data, surveillance via audiovisual equipment-camera and wiretapping, mean processing of personal data and fall within the scope of this law.

The Agency for Information and Privacy (AIP), as an independent institution which is responsible for monitoring the implementation of the Law for the Protection of Personal Data, is an additional mechanism to secure the protection of personal data by taking inspection and controlling actions to monitor the compatibility with the regulations on data protection. AIP, during the inspections and controls, attached the importance to the legality of the processing, taking measures for the security of the data, controlling the access to these data, the purpose of processing up to the destruction after the purpose of gathering data ends. This means that based on the law AIP is authorized for the implementation of the law, to inspect and control the authorities which deal with national security and public security and take actions against them to secure the legality of the processing of the personal data as one of the main principles of processing data. Taking into consideration that AIP, in the recent years, has not taken inspecting actions due to not being fully functional, we do not have data related to the equipment that the authorities of law implementation use for their authorization.

With the appointment of the Commissioner from the Kosovo Assembly as AIP oversight body, we are working on the full functionalization of AIP to exercise the competencies and full legal authorizations and one of our priorities is also the procession of personal data in the sector of security. National security is not specifically defined and as such can be interpreted depending on the situation to be adjusted with the change of the nature of the threats. Such a definition cannot be generalized but can be taken case by case.

The Law on the Personal Data Protection predicts some limitations regarding the subjects of the data when it comes to national security. This limitation must be proportional and implemented only to fulfill an urgent need for the democratic society. Even though privacy is not an absolute right and it can be limited legally for national security purposes, when it does fulfill the necessity and proportional measure the right to privacy remains a basic human right.

The limitations due to national security, defense and public security must not have generalized support or to be applied in a generalized manner, a case by case consideration is needed and that only after all the interferences in privacy and protection of data is taken into account. In accordance with the principle of accountability, the authorities authorized

to use surveillance or eavesdropping equipment must be able to prove and document the reasons for relying on the restriction of certain rights of the subject for the purpose of national security, defense and public safety so that they can demonstrate their compliance with the Law on Personal Data Protection.

Institutions and mechanisms established by wiretapping legislation must implement the rules and procedures provided for the processing and security of personal data.

Concerns

The Kosovo Agency on Information and Privacy has the authority to inspect and control for matters of law enforcement the authorities which deal with state security and public safety and to take action against them to ensure the legality of the processing of personal data as a form of the main principles of data processing. The Agency said that the national security is not specifically defined and as such can be interpreted according to different situations to adapt to changing threats, therefore a division between the importance of national security as opposed to the individual right to privacy cannot be made in general, but must be assessed on a case-by-case basis taking into account all other information.

One important aspect is that under the Law on Interception of Electronic Communications a commissioner to monitor the process of surveillance should be appointed by the KJC, however, there is not report of such a commissioner. Kosovo has an outdated legal framework when it comes to surveillance for national security and a considerable amount of suspicions for human rights violations. Kosovo has not amended its national security strategy since 2010. Moreover, the Law on Interception of Electronic Communications has been in force since May 2015, without any further amendments despite the constant technological developments.

One shortcoming of Kosovo's legal framework is that there is not a proper clarification on the process of purchasing technical equipment for audio-visual surveillance for national security, nor on the process of determining the importance of one equipment over another.

Often many international companies or foreign state agencies do not agree to be prone to the Law on public procurement in order to create monopolies and not provide information to the competitors. Kosovo has had to wait for years in order to be able to even start the negotiations for particular technical equipment for mobile operator surveillance.

Kosovo's technical equipment for physical audiovisual surveillance, but also those for mobile operators' surveillance in the cyberspace are very outdated. For example, Kosovo institutions do not have proper encrypted and secure communication mechanisms, meaning the high state officials, such as the President or the Prime Minister, among one another or even with Intelligence Agencies, or Embassies, do not have proper and secure means of communications.

MONTENEGRO

Not much is known about the surveillance landscape in Montenegro. There is very little comprehensive information available publicly, and the scope of organizations which deal with these kinds of issues is all but nonexistent. During the course of this research, many interlocutors declined to be interviewed, citing their limited knowledge on the subject of the state of surveillance in the country, or financial aid directed towards strengthening capacities in the field in the country. According to the European Commission's Montenegro 2020 Report[81]: "However, the genuine inclusion of civil society organizations (CSOs) in the policy-making process is not sufficiently ensured in practice. An increasingly restrictive approach to public access to information remains a matter of concern".[82]

In a 2015 analysis[83] conducted by the Center for Integrity in the Defense Sector (CDIS) established on the initiative of the Norwegian Ministry of Defense titled *"Montenegro: Building Integrity in the Defense Sector"* assessed that the Ministry of Defense lacks a transparent and well-regulated system when it comes to military human resources management, as well as a balance between free access to information and the protection of personal data. It does not seem that much has changed since in the country, with information on surveillance practices still being scarce in the public.

As part of the Swiss Regional Police Cooperation Program in the Western Balkans, funded through the Geneva Centre for the Democratic Control of Armed Forces and the Democratic Control of Armed Forces (DCAF), the website of the project[84] has pointed out that through the project thermal imaging cameras, laptops and analytical software were procured for border control officers.

In April 12, 2021, the OSCE Mission to Montenegro co-organized a Security Committee meeting with the country's Police Directorate[85] on "Preventing and Countering Terrorist

81 https://eeas.europa.eu/sites/default/files/montenegro_report_2020.pdf

82 This is partly in relation to the previous administrations attitudes towards crime, corruption and transparency on issues of public importance. There have been notable changes since the new administration took office in September 2020. https://www.euronews.com/2020/09/01/montenegro-elections-thousands-take-to-streets-as-opposition-claims-victory

83 https://cids.no/wp-content/uploads/pdf/difi/difi_report_2015_10_montenegro_-_building_integrity_in_the_defence_sector.pdf

84 https://sdc.pageflow.io/spcp-story-of-change#98186

85 https://www.osce.org/mission-to-montenegro/483422

Use of Internet". As is noted, the support of the Mission has allowed the Montenegro Police Directorate to equip themselves with a state-of-the-art digital forensic lab and expanding knowledge on IT forensic analysis. Additionally, OSCE's "Police Reform in Montenegro 2011-2019 – An Assessment and Recommendations for Good Governance in Policing" report, outlines that:

"Within its Service for ICT and Technical Oversight Security and Systems, the Ministry of Interior retained the strategic level of IT systems used by the Police Directorate. This includes the management of police databases such as: the Database of criminal acts, perpetrators and victims, the Fingerprint database (AFIS), the DNA database (CODIS), the Database of missing persons and items, the Database of events and conduct upon them, the Database of arrests, the Confiscated items database, the Registry of crossing the border, the Registry of foreigners' stay up to 90 days, the Database of public order misdemeanors, and the Database of traffic accidents. In addition to these being defined as police databases in several laws (Law on Internal Affairs, Law on Public Order, Law on Foreigners, Law on Border Control, and Law on Road Traffic Safety), management of police databases by the police service is the usual practice in many countries (even when police services are integral parts of ministries), as well as an imperative for international police cooperation. The Police Directorate's Information Security and Data Processing Centre is only in charge of the maintenance of hardware and software and of providing 'help desk' support, without a role in designing and developing the architecture of IT systems used by the police. The Police Directorate should therefore take over police databases and be fully capable of developing and maintaining IT capacities that are used exclusively for operational purposes. Apart from oversight of legality and purposefulness of police conduct, there is no need for another role in this by the Ministry of Interior." (p5)

According to USAID's website data[86], since 2015, Montenegro has received a total of $43,960,153 in funding from the United States. Based on the data collected, the amount of aid going towards the Government and Civil Society sector as well as the Conflict, Peace and Security sector, for activities such as Export Control and Related Border Security Assistance enforcement, DOD - Foreign Military Financing (FMF) programs and International Narcotics and Law Enforcement programs was the biggest. As in the case of Serbia, the amounts of funding for 2020 and 2021 have only been partially reported. For 2020, the current amount stands at $21,370,977, while for 2021 the amount is $71,927. However, there is no more specific information on the programs and donations on the website aside from the tables presented.

86 https://foreignassistance.gov/cd/montenegro/

2020						
$21,370,977	Governance	Department of State [$1,444,464]	$1,400,000	Conflict, peace & security [$1,400,000]	Removal of landmines and explosive remnants of war [$1,400,000]	Conventional weapons destruction and physical security and stockpile management in Montenegro [$1.4m]
		Department of Defense [$19,626,513]	$19,626,513	Conflict, peace & security [$19,626,513]	Security system management & reform [$19,626,513]	Global train and equip program - maritime interdiction capability [$12m]
						DOD- Foreign Military Financing (FMF) Program, Payment Waived [$7.5m]
						DOD- International Military Education & Training (IMET) program/deliveries [$527k]
2021						
$71,927	Administrative Costs	Peace Corps [$71,927]	$71,927	Operating Expenses [$71,927]	Operating Expenses [$71,927]	US Peace corps overseas program support [$72k]

By some estimates, the total number of financial aid that Montenegro has received from the EU from 2007-2020 is around 610 million euros[87]. However, Montenegro still maintains its ties to the East, and more specifically Russia, with reports in 2014 claiming that security agents from Montenegro's NSA were sharing confidential intelligence[88] with the country.

While a list of UN projects in Montenegro is available, there is no additional information on the implemented projects or the grant amounts themselves. This is a continued trend of lack of transparency when it comes to donations and procurement, among other things, of sensitive technologies for surveillance. From the table, it is clear that there are a number of projects which deal with "identification" and dealing with migrants and strengthening border control capacities. Some projects also mention "profiling and forensic/laboratory capacities, as well as evidence collection, information/intelligence management" as well as "strengthening knowledge and skills of law enforcement and judicial authorities".

87 https://www.slobodnaevropa.org/a/pod-istragom-eu-donacija-u-crnoj-gori/31109742.html

88 https://www.slobodnaevropa.org/a/montenegro-russia-and-nato-an-issue-of-double-agents/25464453.html

Project	Agency and contributing partners	Implementing partners	Date
Enhance capacities of law enforcement agencies on identification of vulnerable migrants	International Organization for Migration Bureau of Population Refugees US Department of State		01.01. - 31.12.2017.
Regional and inter-regional law enforcement, and multi-agency coordination and cooperation, to tackle illicit trafficking in drugs and other goods, and transnational organized crime	United Nations Office on Drugs and Crime	CEPOL, Rosfinmonitoring, SEESAC	01.01. - 31.12.2017.
Knowledge and skills of law enforcement and judicial authorities strengthened to better identify, investigate and prosecute cases of trafficking in persons and migrant smuggling	United Nations Office on Drugs and Crime	International Criminal Police Organization, Office for Fight Against Trafficking in Human Beings	01.01. - 31.12.2017.
Law enforcement bodies supported in strengthening their investigative, profiling and forensic/laboratory capacities, as well as evidence collection, information/intelligence management	United Nations Office on Drugs and Crime	CEPOL	01.01. - 31.12.2019.
Regional and inter-regional law enforcement, and multi-agency coordination and cooperation, to tackle illicit trafficking in drugs and other goods, and transnational organized crime	United Nations Office on Drugs and Crime		01.01. - 31.12.2019.
Knowledge and skills of law enforcement and judicial authorities strengthened to better identify, investigate and prosecute cases of trafficking in persons and migrant smuggling	United Nations Office on Drugs and Crime		01.01. - 31.12.2019.
Capacity of customs and border control agencies enhanced to minimize the exploitation of sea, land and air cargo containers for illicit drug trafficking and other transnational organized crime	United Nations Office on Drugs and Crime The European Union	World Customs Organisation	01.01. - 31.12.2019.
Support the national authorities to effectively manage their borders and respond to border security challenges, through the Western Balkans Integrated Border Management Capacity Building Facility (WBIBM)	International Organization for Migration	Danish Ministry of Foreign Affairs	01.01. - 12.31.2021.
Enhance identification of victims of trafficking and raise awareness on the dangers of trafficking, targeting youth with a focus on marginalized groups	International Organization for Migration	SDG Fund	01.01. - 01.12.2021
To strengthen regional cooperation and partnership for safe, orderly and regular migration in the mixed-migration context	International Organization for Migration	Migration MPTF	01.01. - 31.12.2021.

The UN Common Country Analysis (CCA) for Montenegro[89] assesses some of the key development challenges in the country and offers some ways to approach them. For instance, in regards to data and e-Government services, the report notes: *"In addition, there is not yet a strategic vision or comprehensive policy framework, to ensure that e-Governance works for all. Special requirements in other legislative acts hinder the usage of electronic data and electronic communications remain incomplete"*. This suggest that much work needs to be done in order for the country to be able to elevate its digital transformation position.

The European Commission's Instrument for Pre-Accession Assistance (IPA II), which was in effect from 2014 through December 2020, aims to help the candidate states of the Western Balkan countries strengthen their chances at becoming member states of the European Union. The ECs IPA offers financial help to the countries through focusing on certain sectors which seem to be in most need of assistance. For IPA II[90], the Rule of Law and Fundamental Rights sector was selected as one of the relevant sectors for its assistance in Montenegro. Within it, special attention was given to "improve technical equipment, including information technology (IT) databases, adequately train human resources and reinforce inter-institutional cooperation".

The country has been more preoccupied with domestic affairs related to illegal surveillance and wiretapping, with a couple of major scandals occurring in the last couple of years. Additionally, information on the foreign donations for surveillance technologies in the country is scarce, lacking a clear and cohesive frame which would allow for a more thorough investigation into the foreign aid within the country.

In October 2013, two Montenegrin professors filed a case to the European Court of Human Rights (ECtHR) against the country of Montenegro regarding the unlawful use of surveillance footage at the University of Montenegro's School of Mathematics. The professors claimed that they had no oversight regarding the usage of the surveillance cameras as well as the storage of the materials gathered and that this constitutes a violation of their right to private life (Art 8 of the European Convention on Human Rights). The Antović and Mirković v. Montenegro[91] (ECtHR no. 70838/13) case investigated further the differences between public and private spaces and what constitutes legal use of surveillance on citizens

89 https://montenegro.un.org/sites/default/files/2021-06/Common Country Assessment Montenegro 2021 - ENG.pdf

90 https://ec.europa.eu/neighbourhood-enlargement/system/files/2020-08/c_2020_5268_f1_annex_en_v2_p1_1089547.pdf

91 http://hudoc.echr.coe.int/eng?i=001-178904

by the government. The court ruled in the favor of the applicants, which meant that the Montenegrin Government, and its surveillance practices, had infringed on the plaintiffs' right to private life, stating that: *"Given that the relevant legislation explicitly provides for certain conditions to be met before camera surveillance is resorted to, and that in the present case those conditions have not been met, and taking into account the decision of the Agency in this regard (in the absence of any examination of the question by the domestic courts), the Court cannot but conclude that the interference in question was not in accordance with the law, a fact that suffices to constitute a violation of Article 8."* (Antović and Mirković v. Montenegro, no. 70838/13, paragraph 60)

In 2018, a new Law on the National Security Agency[92] was adopted in Montenegro. The law allows intelligence officers to access all databases in Montenegro only by showing official identification cards. Under the new law, the National Security Agency can also have access to all electronic communications of citizens, as well as their personal data, only by the order of the agency's director.

In 2021, following the regime change in the 2020 election, the new director of the National Security Agency (ANB) launched an inquiry into reports of destroying incriminating documents[93] which include wiretapping and surveillance by police officers.

In February 2021, the Prime Minister, Dritan Abazović, and the Secretary of State of the Ministry of Interior, Rade Milošević, announced that more than a million euros had been embezzled[94] in the proqurement of equipment for state border surveillance. The equipment was donated by the European Union through the Schengen action plan. The eqipment that was ultimately procured was said to be cheaper and of lesser quality, and in some cases even technically non-functional. The exposure of such corruption by the MoI came on the wave of a regime change in Montenegro, with newly eleced officials promising to crack down on corruption in the country. The announcement promted an unsealing of previously confidential documents which contained information about other donations and tenders within the Ministry of Interior.

In October of 2021, Montenegrin police arrested the former head of the National Security Agency[95], on allegations of illegal wiretapping of the Special State Prosecutor after sur-

92 https://balkaninsight.com/2015/02/18/montenegoro-s-parliament-adopts-controversial-spying-law/

93 https://balkaninsight.com/2021/01/21/montenegro-security-service-probes-destroyed-documents-on-illegal-spying/

94 https://www.glasamerike.net/a/crna-gora-abazovic-pronevjera-donacija-eu/5783208.html

95 https://www.theweek.in/news/world/2022/02/12/explained-what-is-dna-theft-why-did-macron-refuse-russian-covid-test.html

veillance equpitment was found in his office. Dejan Perunić, the former NSA head, has already faced charges in the past, as he has been said to have illegally surveilled opposition politicans, journalists and religious officials. According to Article 157 of the Criminal Procedure Law, if an individual is suspected of committing a crime, for which evidence cannot in any other way be obtained, the individuals can be subject to measures of control such as: "1) covert surveillance and recording of telephone conversations and other remote communications; 2) interception, collection and recording of computer data; 3) entering the premises for the purpose of secret photography and video and audio recording in the premises; 4) secret surveillance and video and audio recording of persons and objects". The measures detailed in Article 157 can be determined upon a reasoned proposal of the state prosecutor and by a written order of the investigating judge (Art 159).

Montenegro has a fair amount of video surveillance regulation, with regulation of video surveillance in public places, business premises, within residential buildings and work areas all covered through its Law on Personal Data Protection[96] (44/12). The Agency for Personal Data Protection and Free Access to Information is the relevant state body in charge of overseeing compliance with the relevant legal framework. Through the law, citizens are obligated to be informed on the use of the video surveillance through a notification which must include contact information of the person authorized to conduct the surveillance (Art 39). They are also informed that video surveillance is only permitted if it is necessary for the protection of persons or assets or secret information or business secrets (Art 36). Article 37 states that video surveillance may contain records of, among other things, "a photograph of a person (image or sound, or image and sound), date and time recording of entry and exit, and if necessary, the personal name of the recorded person, his/her residence or stay and address, employment, type and number of identification document, reasons for entry, if personal data entered were collected next to the recording or via a recording of the video surveillance system". However, the Montenegrin legal framework does not underline any obligation to undertake analysis of the surveillance system to evaluate its functionality and legal compliance.

When it comes to surveillance technologies and the protection of citizens' privacy and personal data, there is a lot of crossroads which seem to be very difficult to pass. It is important that the state put in enough energy and competent work in order to create transparent and responsible technological solutions in the future. Conversations with experts in the field, with researchers and practitioners, as well as open dialogue with foreign organizations, donors and states, as well as its own citizens are the right way to ensure that step towards better practices.

96 https://www.azlp.me/docs/zajednicka/zakoni/zakon-o-zastiti-podataka-o-licnosti.pdf

COVID related issues

On March 21, 2020, the National Coordination Body for Infectious Diseases of Montenegro adopted the Decision on the publication of names and addresses of individuals who were assigned measures of self-isolation, because due to the previous failure to respect the obligation of self-isolation by some of them and made sure to publish it on the twitter account of the Government of Montenegro[97]. The Agency for Personal Data Protection and Free Access to Information of Montenegro approved the Decision[98], stating that it is not contrary to the Personal Data Protection Act. Because of this, anyone with internet access was able to visit the website of the Government of Montenegro[99] and easily find out the addresses of citizens who were assigned measures of self'-isolation – diligently classified by municipalities for easier and quicker access. The list was later used by private individuals to create a mobile application that allows users to locate people in self-isolation. The crnagorakorona.com app has been created, which, based on geolocation, allows users to locate people on the list in their immediate vicinity, because of their pre-released addresses.[100] Later in December 2021, according to a government statement, the Ombudsman of Montenegro was in charge of concluding an agreement with 2.720 people in the amount of 300 euros each for non-pecuniary damage due to violation of personal rights by publishing personal data.[101]

Policy Recommendations

In order to insure a more transparent and trustworthy policy in relation to its citizens, the government should consider:

- **Opening up government data** and information on public spending and foreign donations, especially for areas such as national security policies, police policies, judicial policies and public service;
- **Facilitate open communication** with its citizens and civil society, especially investigative journalists and researchers working on combating issues such as crime and corruption, abuses of power, bribery and threats to national security;

97 https://www.slobodnaevropa.org/a/30501466.html

98 http://www.gov.me/vijesti/223143/NKT-za-zarazne-bolesti-pocinje-objavljivanje-identiteta-lica-u-samoizolaciji-zastita-zdravlja-i-zivot-gradana-nas-najvisi-priori.html

99 http://www.gov.me/naslovna/samoizolacija

100 https://europeanwesternbalkans.com/2020/03/25/revealing-identity-of-persons-in-self-isolation-in-montenegro-unconstitutional-experts-claim/

101 https://www.slobodenpecat.mk/en/crna-gora-kje-plati-oshteta-po-300-evra-za-2-720-gragjani-poradi-objavuvanje-spisok-za-samoizolacija/

- **Make sure** that its dealings and cooperation is in the best interest of its citizens by informing the public about projects, especially those that deal with sensitive issues such as surveillance, especially if it's in public domains;
- **The government should commission investigations** on the surveillance systems which are in use, in order to better understand their technical capabilities and functioning, the internal procedures, as well as to create more experts who will be able to monitor and point out possible violations of such systems, as well as provide positive practices;
- **Work on implementing good practices** and capacity building of public officials on issues such as personal data protection, anonymization of data, respecting the right to private life and overall improvement of digital skills;
- **Foreign aid donors** can work with the government on laying out standards for responsible implementation of security technologies and discussions on proportionate uses of such technologies;
- **Montenegro's government should work** on aligning its personal data protection legislation with the EU's GDPR in order to ensure better safeguards for its citizens, especially in cases where surveillance technology is being used;
- **The international community** can also help with debating, in agreement with civil society and the government, appropriate legal and institutional frameworks for the regulation of technologies, which if left under regulated, could threaten the privacy and security of citizens.

NORTH MACEDONIA

The Republic of North Macedonia has faced two major wiretapping scandals: the "Big Ear affair"[102] revealed in the year of 2000 and the big wiretapping scandal, the so-called "Bombs", announced in 2015, through 40 press conferences of the opposition political party SDSM[103], titled „The truth about Macedonia"[104].

For the last scandal, the ruling party at the time (VMRO-DPMNE[105]) accused that the wiretapping was carried out by foreign services, potentially using "a yellow van", but without offering concrete evidence. The scandal led to the overthrow of the government in the country, the creation of a Special Public Prosecutor's Office[106]. A number of court cases have been opened against former government officials, including cases involving the procurement and destruction of wiretapping equipment and the prosecution of those who have done the same. A particularly important part was the start of the process of reform of the security and intelligence sector, through new legislation (Law on Interception of Communications[107]) and establishment of new institutions in this sector (National Security Agency (NSA)[108] and Operative –Technical Agency (OTA)[109] in place of the former Security and Counterintelligence Directorate (UBK), which was part of the Ministry of Interior (MoI[110]). Thus, the implementation of interception of communications, as a burning prob-

102 For twenty years, "The Big Ear" has been eavesdropping: the revelation started with Crvenkovski, will it end with Zaev?, December 3, 2018, https://emagazin.mk/dvaeset-godini-golemoto-uvo-prislushuva-otkriva-eto-pochna-so-crvenkovski-e-zavrshi-li-so-zaev/

103 https://sdsm.org.mk

104 http://arhiva.sdsm.org.mk/default.aspx?articleId=11768&mId=55&agId=5

105 https://www.vmro-dpmne.org.mk

106 The full title is Public Prosecutor's Office for Prosecution of Criminal Offenses Related to and Arising from the Content of Illegal Interception of Communications. The Special Public Prosecutor's Office - SPO was established on September 15, 2015, with the adoption of the Law on the Establishment of this Prosecutor's Office and the election of the Special Public Prosecutor by the Council of Public Prosecutors of the Republic of Macedonia. The SPO had a five-year term, which could be extended by a two-thirds majority in Parliament. Its main task was to investigate and prosecute possible abuses stemming from wiretapped material between 2009 and 2015. The SPO has so far opened dozens of investigations and filed charges against numerous politicians and state officials. The SPO stopped working on 30.06.2020, two and a half months before the expiration of the legal deadline, when the new Law on Public Prosecution entered into force and after the public trust in the SPO decreased because in the meantime its chief Katica Janeva was placed under house arrest and sentenced to 7 years in prison for involvement in the "Racket" case.

107 Law on Interception of Communications, "Official Gazette of the Republic of Macedonia" no. 71/2018 and "Official Gazette of the Republic of North Macedonia" no. 108/2019

108 http://www.anb.gov.mk

109 https://ota.mk

110 https://mvr.gov.mk

lem in the past, from the former UBK, as the only institution that implemented it before, shifted to a more complex system of institutions and authorized bodies and bodies, in order to conduct judicial prosecutorial control and external oversight of this system.

For the publication of the political "bombs" in 2015 the European Commission expressed concerns in the Progress reports on Macedonia for 2015[111] and 2016[112] on the massive monitoring of electronic communications. It also issued the Urgent Reform Priorities[113] pointed out serious reforms that are expected to overcome the shortcomings in the legal framework for interception of communications and their implementation. The Commission issued 'Urgent Reform Priorities' based partly on its previous recommendations and partly on recommendations provided by a group of independent senior rule of law experts[114] (Priebe report) brought in to analyze the situation. The independent experts identified significant shortcomings in the areas of interception of communications, the judiciary and prosecution services, external oversight by independent bodies, elections and the media. In parallel, the Commissioner, with the help of three members of the European Parliament, facilitated a political agreement in June/ July.

As a result of that, the Government of the Republic of Macedonia has adopted the PARIRP plan of activities based on the List of the urgent reform priorities[115] (June 2015) which is a list of urgent reform priorities to be fulfilled by the country's institutions, in the fields of rule of law and fundamental rights, de-politicization of the public administration, freedom of expression and electoral reform.

The 2006 Law on interception of communications was amended in 2012, but the 'Urgent Reform Priorities' recommend separating the mandate, regulations and technical facilities for interception in criminal investigations from those for security and intelligence purposes. Working groups were set up to begin to address the issue with external support. Broad consensus was needed to take this forward.

111 https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/pdf/key_documents/2015/20151110_report_the_former_yugoslav_republic_of_macedonia.pdf

112 https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/pdf/key_documents/2016/20161109_report_the_former_yugoslav_republic_of_macedonia.pdf

113 https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/pdf/key_documents/2015/20151110_report_the_former_yugoslav_republic_of_macedonia.pdf

114 https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/news_corner/news/news-files/20150619_recommendations_of_the_senior_experts_group.pdf

115 https://www.sep.gov.mk/data/file/PARIRP/План на активности за реализација на итните реформски приоритети 2015 (Работен документ).pdf

The Law on Electronic Communications (ECC) from 2014 introduced innovations in monitoring the content of communications, as well as in the massive retention of data on the communication traffic of citizens. The law enabled the Ministry of Internal Affairs to have direct and unlimited access to the contents of all electronic communications of all citizens.

In 2017, July, the newly elected Government of the RM has set the course of the reforms, presented in the "Plan 3-6-9"[116] taking into account the Political Agreement of Przhino and the recommendations of the high-level meetings with the representatives from the EU institutions, the guidelines from the European Commission in the Urgent Reform Priorities (2015), The recommendations of the group of senior experts on the systemic issues of the rule of law regarding the interception of communications (2015).

In December 2017/2018 a set of laws have been published on ENER – National electronic system for legal framework with proposed amendments addressing the recommendations of the Senior Expert Group for the systemic issues in the area of rule of law related to the interception of communications (2015), with list of legal acts to be amended.

In 2017 the Personal Data Protection Agency (PDPA) requested for EU support and expertise, through a project[117], to enhance its capacities to perform supervision in the Ministry of Interior - Office of Security and Counterintelligence, and additional external support to prepare a Methodology for performing inspection supervision over personal data processing by the controllers that are related to interception of communications. The PDPA has stated that "no citizen had submitted any request or complaint which would refer to interception of communications revealed in spring 2015, yet in accordance with its mission and legal authorities in the period from 13.06-28.11.2016, ex officio performed regular inspection over the legality of the undertaken activities during personal data processing and their protection in the Ministry of Interior - Office of Security and Counterintelligence (UBK).

Regarding the conducted inspection on 15.12.2016, a File Record was prepared with detected irregularities and violations (withheld documentation about technical and organizational measures to ensure confidentiality and protection of personal data processing, not applying the technical and organizational measures to ensure confidentiality and protection of personal data processing, failure to perform audits to check the established system for personal data protection. A Decision, based on the File, was submitted to the Minister of

116 http://vlada.mk/sites/default/files/Plan3-6-9ENG.pdf

117 EU Project about Support to Access the Right to Protection of Personal Data, which takes place within the IPA TAIB 2012 program (IPA project)

Interior, obliging the Minister to take concrete actions and activities for elimination of the identified irregularities and violations, with the deadline until July 2017.

The DPA during December 2016 began conducting regular inspections about the legality of the undertaken activities during the personal data processing and their protection in the telecommunications sector also, more specifically in both telecommunications operators one.VIP LLC Skopje and Macedonian Telecom AD Skopje, in addition to the already conducted inspection at the Ministry of Interior - Office of Security and Counter Intelligence and in order to obtain a comprehensive picture regarding the means of the personal data processing in this area. Both inspections have been completed at the beginning of 2017. It was established that the two Telecom operators, regarding the safety and integrity of electronic communication networks and services, according to the Interception of Communications Act, applied at least equal level of security and protection, as well as for the data in their electronic communication network, whereupon they have established electronic communication lines with appropriate interface for transmission to the competent authority for interception of communications in their network and apply technical and organizational measures to ensure confidentiality and protection of personal data processing against accidental or unlawful destruction, accidental loss or alteration, or unauthorized or unlawful storage, processing, access or disclosure to unauthorized persons. [118]

In that period there was also a new Law proposed on Protection of Privacy which establishes protection of the privacy of the citizens of the Republic of Macedonia, guaranteed by the Constitution and the European Convention on Human Rights, in relation to materials arising from illegal interception of communications made in the period from 2008 to 2015. This law was passed in the package of laws that were agreed upon by the political leaders with the Przhino agreement. The Venice Commission proposes a thorough revision of the Law on Protection of Privacy. *"This law has a legitimate aim, but does not strike a proper balance between the private interest and the interest of informing the public."*[119] The PDPA did not publish their own position on this.

In 2018, the Parliament adopted a new Law on Interception of Communications and amending the Law on Electronic Communications that removed the power of the Administration for Security and Counterintelligence (UBK) to conduct surveillance activities and intercept communications. The new law allows for the interception of communications for the purpose of detecting and prosecuting perpetrators of crimes, as well as for protection

118 https://dzlp.mk/sites/default/files/u4/annual_report_2016_eng.pdf

119 https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2016)008-e

of the country's interests in defense and security. The competent bodies for interception of communications in criminal investigations are the public prosecutor and the justice police that are to act upon judicial order. The operators are required to submit metadata on request by authorized bodies for the needs of security and defense. The period for keeping the data collected from interception of communications in the interest of security and defense was reduced from the previous five years to three years.[120]

In 2019 another Law on National Security Agency (NSA) was adopted to cease the UBK's operations and replace it with the NSA. The Agency should collect, process, analyze, assess, exchange, keep, and protect data and information with the aim to detect and prevent activities related to safety threats and risks to national security. The Agency shall permanently monitor telecommunication lines, electronic communications, audio recordings in rooms, and audio, video and photographing at open spaces; inquiry in the communication metadata of citizens; as well as collect data and information from natural and legal entities and other relevant parties.

Instead of the UBK, the Law on Operational Technical Agency (OTA) provided for the creation of a new body, which should serve as a mediator between the authorized bodies for interception of communications and the telecom operators. This was done to avoid concentration of power in one authority and to ensure that interception is solely based on laws and relevant court decisions.

The model was borrowed from Croatian legislation and security practice. However, valid concerns were raised when it became widely known that the equipment used by the UBK will be transferred to OTA, and some UBK staff might become a part of the newly created agency. The positive effect of the new model is the existence of an additional layer of oversight. Experience thus far has shown that partisan and political influences over the security services sometimes determine their work. This brings into question the professionalism of the services and undermines the citizens' trust. Regarding oversight and control, the positive legislative step is too slowly being implemented in practice.

From a responsibility perspective, the former head of the North Macedonia secret police has been sentenced to 12 years in prison in part for leading a decade - long illegal wiretap-

120 https://metamorphosis.org.mk/wp-content/uploads/2019/08/Legal-framework-on-interception-of-communication_eng.pdf; Biljana Karovska-Andonovska, Analysis of the Content and Practical Implementation of the Law on Operational Technical Agency and the Law on Interception of Communications, February 2021, https://www.dcaf.ch/sites/default/files/publications/documents/ENAnalysisLawOperationalTechnicalAgencyLawInterceptionComms.pdf

ping program. In addition, the Skopje Court sentenced former Interior Minister Gordana Jankulovska to four years' imprisonment for allowing the technical bugging equipment that used to be destroyed. Two agents[121] were also sentenced to 15 years each, in absentia for procurement, unlawful interception and damaging the equipment. According to prosecutors, the secret police had tapped almost 5,000 telephone numbers, and over 20.000 persons[122], between 2008 and 2015 without any judicial control.[123]

Surveillance equipment

Today, in accordance with the Law on Interception of Communications (Article 4, paragraph 1, items 6 and 7), the authorized bodies for conducting the special investigative measure of interception and recording of telephone and other electronic communications are: the public prosecutor and the judicial police, determined in accordance with Law on Criminal Procedure[124] (composed of members of the Ministry of Interior, the Financial Police Directorate, the Customs Administration and the military police), and the authorized bodies for implementing measures for interception of communications in order to protect the interests of security and defense of the state are: the National Security Agency and Ministry of Defense - Military Service for Security and Intelligence, and in the part of the frequency spectrum of radio waves at high, very high and ultra-high frequencies (HF, VHF и UHF), The authorized body for implementing a measure for interception of communication is the Center for Electronic Reconnaissance of the Army of the Republic of North Macedonia, which is designated for the needs of the defense.

The monitoring and recording of telephone and other electronic communications is done through access to the technical equipment of the operators[125] through OTA or by applying special technical devices and equipment without the mediation of OTA and the operators and at the same time creating a technical record for the content of the communication, with the possibility to be reproduced.

121 https://sdk.mk/index.php/makedonija/izbeganiot-eksnachalnik-na-pettata-uprava-goran-grujevski-se-vrabotil-vo-kujna-vo-restoran-na-grchki-ostrov/

122 https://akademik.mk/zaev-prislushuvani-se-nad-20-000-gragani-3/

123 Former North Macedonia police chief sentenced for leading phone-tapping scandal, Euronews, February 26, 2021, https://www.euronews.com/2021/02/26/former-north-macedonia-police-chief-sentenced-for-leading-phone-tapping-scandal

124 Закон за кривичната постапка, „Службен весник на Република Македонија“ бр. 150/2010, 100/2012, 142/2016, Одлука на Уставен суд објавена во „Службен весник на Република Македонија“ бр. 193/2016 и „Службен весник на Република Северна Македонија“ бр. 198/2018

125 Operator of public electronic communication network and / or provider of public electronic communication services, which provides the monitored communication through electronic communication network and means to the bodies authorized to implement measures for interception of communications mediated by OTA. Art. 4, p. 1, t. 11, Law on Interception of Communications, "Official Gazette of the Republic of Macedonia" no. 71/2018 and "Official Gazette of the Republic of North Macedonia" no. 108/2019

OTA is established by law[126] as an independent and autonomous state body that provides technical connection between the operators and the authorized bodies. The OTA acts as an intermediary body that establishes a technical passage between the operator and the authorized authorities, without the possibility to activate or conduct the recording of the intercepted communications. OTA does not have the technical ability to access the content of the intercepted communication, but does this through mediation devices to monitor communications. OTA specifically is competent for:

- **enables technical connection** between the operators and the mediation device (LEIMD[127]) housed in the OTA;
- **enables technical connection** between technical devices (LEIMD и LEMF[128]) house in OTA;
- **provides a technical connection** between the technical device (LEMF) located in the OTA and the workstations[129] used to conduct interception of communications located in the premises of the authorized bodies.

A few days before the OTA started functioning (November 1, 2018), the Government of the Republic of Macedonia at the session held on 26.10.2018[130] made a decision to establish a Commission for transfer of technical devices for interception of communications and technical documentation from the Ministry of Interior - UBK to OTA. The commission had the task to determine the factual condition of the technical devices for interception of communications, as well as the technical documentation, which are transferred from the Ministry of Interior - UBK to OTA, to make an inventory of all active measures for interception of communications, as well as to compile a report on the task performed.

126 Law on Operational-Technical Agency, "Official Gazette of the Republic of Macedonia" no. 71/2018 and "Official Gazette of the Republic of North Macedonia" no. 98/2019

127 "Mediation device (LEIMD)" is an intermediary technical equipment and appropriate software support that enables the activation of the measure of monitoring and recording of telephone and other electronic communications. Art. 4, p. 1, t. 18, Law on Interception of Communications, "Official Gazette of the Republic of Macedonia" no. 71/2018 and "Official Gazette of the Republic of North Macedonia" no. 108/2019

128 "Communications monitoring equipment (LEMF)" - means of interception of communications to which the content of the intercepted communication and the information related to the intercepted communication are transmitted from the technical equipment of the operators through OTA to the workstations owned by the authorized bodies. Art. 4, p. 1, t. 20, Law on Interception of Communications, "Official Gazette of the Republic of Macedonia" no. 71/2018 and "Official Gazette of the Republic of North Macedonia" no. 108/2019

129 Personal computer with appropriate software support related to the communications monitoring equipment (LEMF), which accesses the content of the intercepted communication with the possibility of its download and the information related to the intercepted communication. Art. 4, p. 1, t. 21, Law on Interception of Communications, "Official Gazette of the Republic of Macedonia" no. 71/2018 and "Official Gazette of the Republic of North Macedonia" no. 108/2019

130 https://vlada.mk/node/15617

The technical devices and equipment, which enable the conduct of wiretapping without the mediation of OTA and the operators, are kept in the Basic Public Prosecutor's Office for Prosecution of Organized Crime and Corruption.

According to this, technical devices and equipment for interception of communications are available in the following institutions:

- **OTA** (mediation device (LEIMD), technical device (LEMF)),
- **Authorized bodies** (workstations),
- **Basic Public Prosecutor's Office** for Prosecution of Organized Crime and Corruption (technical devices and equipment that enable wiretapping without the mediation of OTA and operators).

Equipping of security and intelligence services in North Macedonia with surveillance tech

Through the latest wiretapping scandal in Macedonia, during the disclosure of the so-called "Bombs" revealed that a large number of citizens were illegally wiretapped, including: journalists, politicians, senior government officials. In some of the telephone conversations, one could hear the former director of UBK, the head of UBK and a person from Israel agreeing on a transfer of money for a bribe from an Israeli company, in order to enable the purchase of wiretapping equipment in 2011.[131]

The British government, in turn, in 2015 and 2016 issued licenses for the export of various equipment, including devices for recording telephone conversations and text messages, as well as hardware for monitoring Internet traffic. These eavesdropping products are exported to countries from all continents of the world, and in Europe they end up in only three countries: Czech Republic, Serbia and Macedonia.[132]

Map of all deals of British companies made by Motherboard[133] is based on data published by the British Department of International Trade. These figures include only export licenses issued since 2015, the same year when the so-called export licenses began to be disclosed in Macedonia. "Bombs". Apart from the division by equipment and land, the map also distinguishes between temporary and permanent licenses. The first are licenses issued

131 https://www.slobodnaevropa.mk/a/28886218.html

132 https://off.net.mk/vesti/makedonija/kakva-oprema-za-prislushuvanje-britanija-isporacha-vo-makedonija

133 https://www.cobham.com https://cdn.off.mk/files/statija/2017/04/04/2014-cobham-tcs-catalog.pdf

for the product to be exported from the UK for fairs or demonstrations of the product to customers, and last 12 months. According to the map for Macedonia, a temporary license for telecommunication equipment has been issued, specifically for the product "Evolve-4 Nimbus" from the company Cobham[134]. It is about "IMSI catcher" (International Mobile Subscriber Identity-catcher)[135] a device used to eavesdrop on cell phone conversations and track the location of the phone. The device basically "plays" an antenna of a mobile operator to which the victim's cell phone is attached. Of the 148 licenses to export from Britain, 16 were for the Evolve-4 Nimbus.

British weekly magazine „Computer Weekly"[136], on 27.11.2017 announced that the Government of the United Kingdom had approved a license to sell surveillance equipment in Macedonia, at a time when the country was involved in an illegal program to eavesdrop on its citizens. The survey found that export licenses were issued at a time when Macedonian security services were heavily involved in massive illegal surveillance of communications.[137]

The research contains source documents[138] which show how the UK has approved the export licenses of Gamma International UK for the supply of sophisticated mobile phone monitoring equipment, known as IMSI catchers, to the former Yugoslav Republic of Macedonia. The survey contains extensive documentation, which includes, inter alia, responses from the UK Ministry of Foreign Affairs, internal electronic communication between the British Embassy in Skopje and the Ministry[139], written communication between the company "Gamma International" and "Gamma Group" and the Ministry of Foreign Affairs, the price list of the company "Gamma" for the surveillance equipment "Finfisher", their catalog for the performance of the equipment for interception of mobile phones, etc.

The written communication reveals that the license to export the sophisticated equipment was issued to Gamma International UK Limited on October 3, 2012, for six units of their surveillance equipment, for which a senior British government official was consulted.

134 https://www.cobham.com https://cdn.off.mk/files/statija/2017/04/04/2014-cobham-tcs-catalog.pdf

135 https://www.techtarget.com/whatis/definition/StingRay?_gl=1*1hzd124*_ga*MTM3ODYzN-jgyMC4xNjI2NzcwNjAy*_ga_TQKE4GS5P9*MTYyNjc3Mjc0MC4yLjAuMTYyNjc3Mjc0MC4w&_ga=2.1077426.2016178533.1626770602-1378636820.1626770602

136 Prelec, T., UK sale of surveillance equipment to Macedonia raises questions over export licence policy, 27.11.2017, https://www.computerweekly.com/feature/UK-sale-of-surveillance-equipment-to-Macedonia-raises-questions-over-export-licence-policy

137 https://www.computerweekly.com/feature/The-Macedonian-surveillance-scandal-that-brought-down-a-government

138 https://www.computerweekly.com/ehandbook/Gamma-International-The-Macedonia-files

139 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/641794/FOI_0678-17_Digest.pdf

The documents also indicate that the Macedonian government had already purchased monitoring equipment from the British company "Gamma" a year earlier, in 2011, but did not specify what equipment it was.

The British company "Gamma International" is often on the front pages of the British media, primarily because of the controversial equipment it offers on the market. According to Reporters Without Borders, the UK-based firm, which also has subsidiaries in Germany, Southeast Asia and the Middle East, sells equipment to government wiretapping agencies, and their finisher software is considered one of the most advanced. at the market.

Regarding whether the British surveillance equipment is still in use, Macedonian journalists asked for an answer from the Ministry of Interior, and for the writings of the British weekly, they asked for a comment from the British Embassy in Skopje.[140] Otherwise, the Ministry of Interior has adopted a bylaw, Rulebook on the types of technical means that will be used for audio and visual recording by the Police[141], which describes the technical characteristics of the device for mobile system for audio and video recording.

In the case „Treasure"[142] opened by the former SPO, three MoI officials are charged with abuse of office and authority, and another with aiding and abetting. In his closing remarks, the Prosecution pointed out that instead of the Ministry of Interior making a direct procurement of electronic communications equipment for the needs of the Fifth Directorate at UBK from the company GAMA from Great Britain, as the most economical way, they agreed to procure through another company - intermediary Finzi DOOEL Skopje, which managed to misuse funds from the state budget. More than three years after the opening of the case, on April 13, 2021, the court passed verdicts by which the former head of the secret police was sentenced to a single prison sentence of 8 years, and the former head of the Fifth Directorate in the Ministry of Interior, who was tried. on the run, was sentenced to a single prison sentence of 15 years. The former assistant minister in the Ministry of Interior, and the former head of the director's office, received prison sentences of 5 years each. The court obliged the defendants, if the verdict is confirmed, to jointly compensate the damage to the state budget in the amount of over 21 million denars. The verdict also confiscates funds from the company "Finzi".[143]

140 https://meta.mk/britanskite-vlasti-i-dozvolile-na-gama-grup-%DA-prodade-oprema-za-sledene-na-makedonija/

141 https://mvr.gov.mk/Upload/Documents/PRAVILNIK ZA AUDIO I VIDEO.pdf

142 https://www.mkd.mk/makedonija/sudstvo/deneska-presuda-za-nabavkata-na-opremata-za-prislushuvanje-prvoobvinet-sasho

143 DTZ, Case "Trezor" (Treasury): Mijalkov condemned to 8 years imprisonment, 13.04.2021, https://p.dw.com/p/3rwti

In mid-2016, a new mobile system was promoted and introduced in the traffic police[144], with which the traffic police were equipped with video cameras to record their actions. The purpose was to ensure the legality of the police action, to eliminate shortcomings in the work, then control the work of police officers by their superiors, prevent abuse and corruption and determine the merits of complaints from citizens. This is a joint pilot project of ICITAP - US Department of Justice in Macedonia and the Ministry of Interior. The donation is worth $ 65,000.

Within the frames of the annual Program for Export Control and Border Security, prepared by the Bureau of International Security and Non-Proliferation within the US Department of State, intended for the countries of the region, including Republic of Macedonia, the Ministry of Economy had need for equipment to effectively equip the Department for international trade co-operation, whose mandate is to control the export of goods and dual-purpose technology. Considering that the Ministry of Economy is responsible for applying the TRACKER system (single system for electronic submission/exchange of confidential documents and requirements of the companies that perform import of goods and dual-purpose technology), which is unified worldwide and used since 2007, it was necessary to support the system with new equipment. The first donation of IT equipment from the State Department was conducted in June 2015 at a cost of 8,840 Dollars, and the second, delivered in June 2016 at a cost of 11,648 Dollars. The total value of both donations is 20,488 Dollars.[145]

A donation of 100,000 euros, consisting of equipment and advisory assistance, was promoted in July 2021 at the Kjafasan border crossing, North Macedonia, by the US Ambassadors to North Macedonia and Albania and customs officials from the two neighboring countries. Mobile scanners, densitometers and cameras are part of the equipment donated by USAID to the customs administrations to facilitate trade and transport and improve cross-border cooperation between the two countries in order to establish a joint border crossing and joint controls at the Kafjasan border crossing.[146]

In March 2021, the OSCE Mission to Skopje launched a new project aimed at assisting North Macedonia in reducing the risk of trafficking and misuse of small arms and light weapons

144 Police will video monitor with mobile cameras 16.06.2016, https://sdk.mk/index.php/makedonija/politsijata-ke-snima-so-mobilni-kameri/ Traffic Police shall video monitor, 16.06.2016, https://fokus.mk/soobrakajnata-politsija-ke-ne-snima/

145 Minister Kuqi accepted donation of IT-equipment from the American State Department, 02.06.2016, https://economy.gov.mk/vest/40

146 https://www.ohridnews.com/amerikanska-donaci-a-vo-oprema-i-tehnichka-pomosh-za-granichniot-premin-afasan-aftane/

(SALW), which pose security risks to the country and the wider region. The project, based on input from the government of North Macedonia, builds on the results of a previous project, which the Mission delivered over the last four years. The European Union and the German Foreign Office provided financial support for both projects. Within the initial project, the Mission helped the Ministry of Internal Affairs upgrade the security infrastructure at 15 border posts throughout the country, establish standard rules of procedure for SALW stockpile management, and strengthen the role of the National SALW Commission.[147]

On August 26, 2021, at the Ministry of Interior[148] new computer equipment was promoted that will enable more efficient monitoring and control of small arms and light weapons in the country. The equipment consists of 74 computers, 52 printers and 50 scanners, which will be deployed in the Sectors for Internal Affairs and police stations, in order for the smooth and efficient functioning of the information system of the Ministry of Interior. The donation is realized as part of the project "Improving national practices for the control of small arms and light weapons and building resilient communities", which UNDP implements with the financial support of the German Embassy in Skopje. The project is part of the "Roadmap for the Control of Small Arms and Light Weapons", of which North Macedonia is a signatory. The implementation of the project will enable the Ministry of Interior to collect and analyze data on small and light weapons in the country faster and more accurately. In the first year, the new police information system will be used by about 3,500 police officers at various levels, which will contribute to faster exchange of information between sectors, and thus to a more determined and comprehensive fight against the illegal arms trade.

This is the second IT equipment donation under the project since 53 computers, 16 printers, 10 scanners and 25 special weapons licenses printers were delivered in October 2020. In addition to the donation of equipment, the development of appropriate software for monitoring and control of small arms and light weapons is underway. Additionally, during September, trainings will be held for 250 employees in the Ministry of Interior who will work in practice in this security segment.

UNDP is implementing this project as part of the regional initiative "Roadmap for the Control of Small Arms and Light Weapons" whose main goal is to establish a system of control of small arms and light weapons in the Western Balkans, in accordance with European and international standards.

147 OSCE Mission to Skopje launches new project to reduce misuse of small arms and light weapons in North Macedonia, 10.03.2021, https://www.osce.org/mission-to-skopje/480811

148 https://mvr.gov.mk/vest/16918

Examples of successful IPA projects implemented in North Macedonia in 2019: Modern customs and quality border control system, resulting in more effective customs controls, decreased administrative costs for citizens and business and improved transit traffic and cargo shipments along the European corridors 8 and 10. The EU invested EUR 6.5 million in a new electronic system for processing transit declarations and two new border terminals and modern customs clearance facilities of a total of 13,500 m2, equipped with the latest technology inspection equipment, the necessary access and exit roads, parking and service support space. The time for completing border crossing procedures for passengers and cargo shipments shortened due to one stop border crossing point ensuring clearance for both Serbia and North Macedonia.

IPA indicative allocations 2007-2020 (million EUR)													
2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
58.5	70.2	81.8	91.7	98.0	105.1	117.2	85.7	88.9	91.6	94.9	97.6	100.9	104.6

Source: Secretariat for European Affairs, Government of the Republic of North Macedonia

The EU allocated around 100 million EUR annually for North Macedonia within IPA I and IPA II instruments in the post-economic crisis period. However, there have been oscillations in the allocated sums, which range from the lowest 58.5 and 70.2 million EUR in 2007 and 2008 respectively up to 117.2 million EUR in 2013. The EC assessed in its North Macedonia 2018 report that although the implementation IPA II instrument is well underway, "urgent measures are needed to improve the planning, programming and management capacities in the national IPA structures."[149]

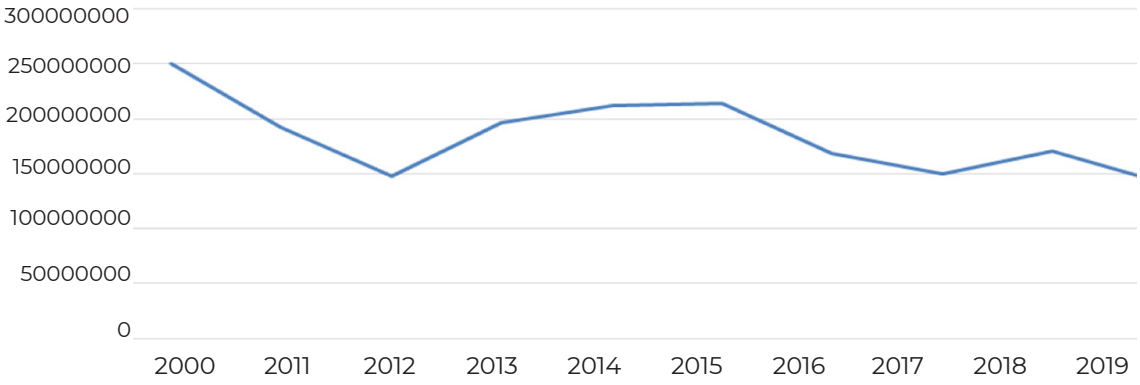
According to World Bank data[150] the Net official support (USD dollars) for North Macedonia is slightly decreasing from 2000 onwards:

2000	2011	2012	2013	2014	2015	2016	2017	2018	2019
250850006.1	192289993.3	147710006.7	196729995.7	211919998.2	214320007.3	168350006.1	149949996.9	170179992.7	141800003.1

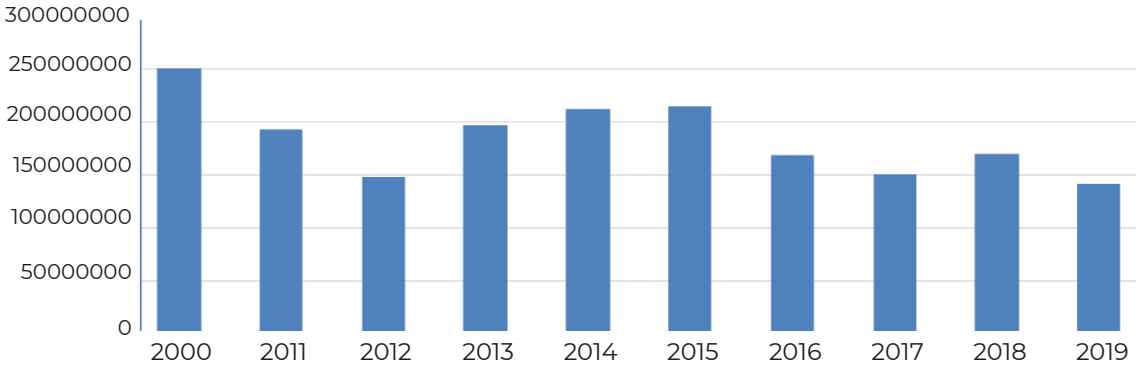
149 European Commission, The Former Yugoslav Republic of Macedonia 2018 Report.

150 https://databank.worldbank.org/reports.aspx?source=2&country=MKD#advancedDownloadOptions

Net official development assistance and official aid received (current US$)



Net official development assistance and official aid received (current US$)



USAID support has drastically changed during these six years. Specifically, if we compare financial support from 2016 onwards, in the area of Conflict, peace and security. Moreover, during political (and Balkan route migrants) crises in 2015-2016, USAID support was 6.813 M dollars for the Conflict Peace and Security[151], with additional 6.786 M dollars spent on CSOs and Government at the time, knowing the pressure[152] and the role of the CSO after the political crises. In 2017 that amount was increased in 7.383 M dollars to Governance Sector[153] – and additional 7.248 M dollars in the area of Civilian peace building and conflict prevention. To compare, in 2020[154] this support has decreased, as seen: only $2.467M for Government and Civil Society, and only $1.032M - Conflict, Peace, and Security.

151 https://foreignassistance.gov/cd/north%20macedonia/2016/obligations/1

152 https://ifex.org/civil-society-under-pressure-in-macedonia/

153 https://foreignassistance.gov/cd/north%20macedonia/2017/obligations/1

154 https://foreignassistance.gov/cd/north%20macedonia/2020/obligations/1

Migrant's crises – North Macedonia: between international legal obligations and political opportunism

The refugee/migrant crisis of 2015 at the Macedonian – Greek borders, and its aftermath in 2016 wasn't a 'typical' refugee crisis. The development of the crisis led to the conclusion that Europe and the world face a phenomenon of refugee migration or movement of peoples unprecedented in recent history. The divisions in the EU and the lack of a united approach affected all Balkan countries, small in territory and resources but, more importantly, weak in institutional capacity.

The Republic of North Macedonia, a country with weak and fragile institutions, a problematic rule of law and already in deep internal political crisis since 2014, found itself on the 'brink' of the 'battlefield'. The Greek-Macedonian border became a symbol for the desperate attempts of thousands of men, women and children trying to cross the border and continue to their dream destination in the European Union.

The response of the Macedonian authorities to the crisis was as chaotic and disorganized as the common EU approach to the crisis appears to be. Local crisis management entailed actual day-to-day decisions, very often varying between desperate efforts to get international European support in dealing with the crisis, situations of clear disregard for international legal obligations and political opportunism for internal purposes.

In May 2020, an internal Council survey[155] of EU member states' assistance for Western Balkans countries[156] shows that the emphasis is very clearly on migration control measures, with "the majority of bilateral support, provided in two areas, namely border management and combating the smuggling of migrants (over 50% of all MS activities)".[157]

The mapping results show that 15 Member States provide support in the region. As regards the fields of support, the results of the mapping clearly indicate that the majority of bilateral support is provided in two areas, namely border management and combating the smuggling of migrants (over 50% of all MS activities). At the same time, the results indicate a very low level of general support in the field of integration (2%) and the legal mi-

155 In order to establish a stepping-stone for future strategic plans to strengthen migration capacities in the region, the Croatian Presidency initiated and undertook a comprehensive mapping of Member States' non-EU-funded cooperation and activities in the area of migration management.

156 _

157 https://www.statewatch.org/news/2020/july/eu-support-for-migration-management-in-the-western-balkans-squarely-focused-on-control-measures/

gration scheme (4%), as well as a relatively low level of support in the fields of asylum (6%), reception (8%) and return (7%).

The mapping results also show that 15 Member States provide support in the region through either expert assistance, equipment or financial assistance. Overall, 67% of all the assistance provided takes the form of expert assistance (see *Chart 2*)

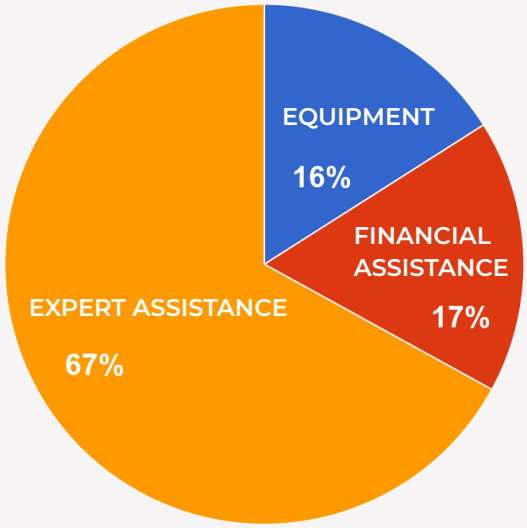


Chart 2

Support is not distributed equally among the Western Balkan partners. Member States' assistance is focused mostly on the partners bordering the EU, i.e. North Macedonia and Serbia (almost 50% of all MS activities), while Kosovo is the partner with the lowest percentage of Member States' activities (9%) see Chart 3.

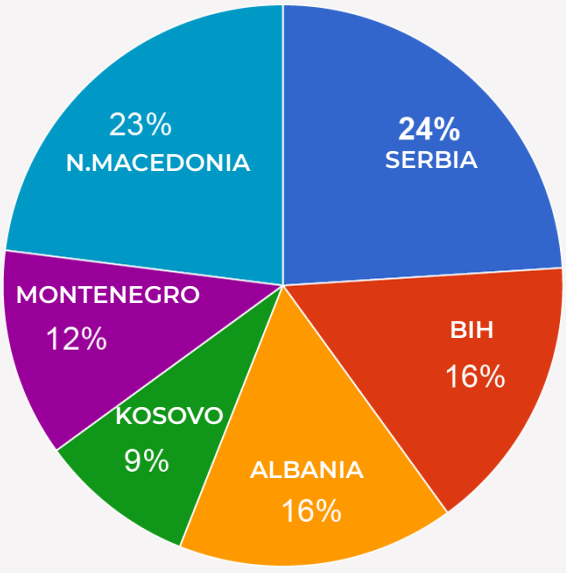


Chart 3

According to the results of the mapping, a substantial proportion of all the Member States' activities are directed towards information exchange between MS and specific partners in the region. However, some delegates expressed concerns regarding the unsatisfactory level of unified information flow and the need for enhancement. In addition, it can be seen that the activities of Member States and EU Agencies in their respective fields of competence tend to be directed at specific fields of interest, and are thus most likely to overlap as regards the relevant Western Balkan partners as well as the scope of support provided.

In December 2020, the Council of the EU has adopted Conclusions on enhancing cross-border law enforcement cooperation[158]. Under this umbrella, various EU donor supported activities were undertaken, specifically for increasing the capacities and equipment of the WB countries for information exchange. Much of this support is distributed through the sector for migration and trafficking with human beings or units for suppressing crime.

A great donation the Ministry of Interior received 1,061,000 US dollars – to fully equipped with a total of 593 cameras of all Sectors of Internal Affairs, i.e. the Traffic Safety Units and the Department of Border Affairs - a project of the ICITAP program of the Department of Justice of the Government of our friends the United States of America.[159]

COVID related issues

North Macedonia has become the first country in the Western Balkans to launch a contact-tracing app to tackle the spread of COVID-19, with the government at pains to stress user data will be protected. StopKorona! went live on April 13, 2020, as a Bluetooth-based smartphone app that warns users if they have come into contact with someone who has tested positive for the novel coronavirus, based on the distance between their mobile devices. The app, downloaded more than 5,000 times on its first day, it was developed and donated to the Macedonian authorities (Ministry for Information Society and Administation) by Skopje-based software company Next sense. The same company afterwards received a tender to operate with the city parking system, that cost 345.000 euros.[160]

However, the experts pointed out several important issues regarding the privacy of people, but also the transparency of the process, especially in the area of non-use of open source

158 https://www.statewatch.org/media/1444/eu-council-draft-police-cooperation-draft-conclusions-11516-20.pdf

159 https://relevant.mk/2022/makedonija/19146/

160 https://emagazin.mk/nekstsens-go-dobi-tenderot-na-gradski-parking-skop-e-za-odrzhuva-e-na-sistemot-za-zonsko-parkira-e-vreden-345-000-evra/

software, as the only way to ensure trust in technological measures.[161] The same company that made the app in North Macedonia, "Next Sense[162]", and donated the StopCorona application, announced that they had also donated an app to Hungary called VirusRadar. "VirusRadar" mobile application uses "Next sense" technology to track contacts to detect potentially exposed Covid19. *The mobile application is a contribution of Nextsense to the Hungarian authorities in support of the fight against the pandemic.*

Some media[163] in 2020 even proposed to Government to publish names of persons in self isolation. Experts immediately informed and reminded the Montenegro decision and ECHR rigyhts and obligations that the country has ratified and has to implement.[164]

Very recent activities:

Macedonian software company **Cytrox**, which was **blocked by Facebook** late December 2021, due to spying on users, produces a spy application called Predator - one of the most powerful and current spying tools in the world. The investigation made shows that the company "Cytrox", which is a subsidiary of a Hungarian company, is associated with Israeli capital and former members of the special forces of the Israeli army. It is also quoted article in "Forbes" from 2019[165], which says that the company "Cytrox" was "rescued" by **Tal Dillian**, a former commander of Unit 81 of the Israeli Defense Forces, who invested in a Macedonian startup in 2018, and later joined a powerful alliance of spyware makers called **Intellect**. Cytrox Predator software used to attack Egyptian politician, former presidential candidate and dissident **Ayman Nur**, showed research by Citizen Lab. The Macedonian company, said to be "previously little known" in the "mercenary hacker" sector, sells its services to governments around the world, and its "Predator" in Nuri's case was used by its client, an Egyptian state institution. At the same time, the phone was "infected" with another application, Pegasus, developed by rival NSO Group and used by another Egyptian state institution, the study said. In addition to Nur's case, it has been proven that the phone of a well-known Egyptian TV host and journalist, who wished to remain anonymous, was hacked with "Predator".

161 https://pina.mk/3443-preku-aplikatsijata-stopkorona-se-ushte-ne-e-otkrien-sluchaj-na-korona-virus/

162 https://pina.mk/3243-nekstsens-izvorniot-kod-na-stopkorona-e-predaden-vo-sklop-na-donatsijata-no-ne-e-za-javna-distributsija/

163 https://kanal5.com.mk/predlog-od-kanal-5-do-vladata-na-makedonija/a414362

164 https://respublica.edu.mk/mk/blog/how-covid-19-affects-the-right-to-privacy

165 https://www.forbes.com/sites/thomasbrewster/2019/08/05/a-multimillionaire-surveillance-dealer-steps-out-of-the-shadows-and-his-9-million-whatsapp-hacking-van/

Cytrox, the company that says it sells "cyber-intelligence systems designed to offer security" to governments and companies, was founded in Skopje in 2017. According to data from the Central Registry, the founder of this software development company is a Hungarian company, founded in Budapest and named "Cytrox Holdings Limited Joint Stock Company" with a cash investment of 25 thousand euros. The main activity of the Skopje company[166] is computer programming, and its manager is **Ivo Malinkovski**[167]. After the publication of the Citizen Lab research, Facebook said[168] that the Macedonian IT company that develops malware for smartphones, is blocked due to the abuse of the social platform for espionage of users. It is one of seven companies that have used its platform to spy on 50.000 people in 100 countries.[169] There is complete silence from institutions and media on continuing the stories about Cytrox.[170]

Interviews:

Almost all interviewees agreed that the subjects of the security-intelligence community are increasingly using new technologies to realize their tasks and fulfill their goals. Many of them, and the case is similar with the state services, have significantly increased their capacity and modernized the methods for collecting, storing and analyzing data through the application of modern technologies for tracking and recording, as well as the use of drones and artificial intelligence.

Specifically for North Macedonia, everyone agrees that *the state does not have sufficient protection mechanisms*, and that even for those protection mechanisms that are in place, there are still easy ways to bypass and/or abuse them by certain individuals for gain. There

166 https://www.slobodnaevropa.mk/a/31614163.html

167 Ivo Malinkovski, according to publicly available information, is the son of Ilija Malinkovski - owner of the Kamnik winery, better known by the company Micei-International DOO Export - Import Skopje, and even better known as Consul of the Kingdom of Morocco in RSM. Mikei -International is a medium-sized company established in the nineties and in its priority activity mediates in trade in various products, and the Ministry of Interior of RSM has granted the company Approval for repair of weapons of category B, C and D no. 10.2-2064 / 2 from 30.05.2014. Mikei-International DOO import - export Skopje is a company that trades in military and police security equipment, hunting, fishing and pyrotechnic equipment, cameras, camcorders and other raw materials. This company is one of the few in the region and Europe that on its website does not have information about the types of systems it offers, and refer to police, security and intelligence systems and equipment that remains unknown to those interested

168 https://www.slobodenpecat.mk/en/fejsbuk-blokirashe-makedonska-firma-poradi-navodno-shpioniranje-na-korisnici/

169 https://www.slobodenpecat.mk/en/shpionski-softver-predator-na-makedonskata-kompanija-sajtroks-e-oruzhje-za-hakiranje-politichari-i-novinari/

170 https://remenski.com/en/one-blocked-for-cyber-spying-second-renovated-two-days-before-the-blockade-the-state-as-a-spy-nest-and-silance-by-the-institutions-series-25

are capacities and resources quantitatively, but not qualitatively enough. Also, there is a perception that *large amount of drones is noticed to be possessed by private persons/ entities*.

Memories of the recent past of abuse of state institutions and powers for political purposes are still fresh. If there is political will and hidden goals, any opponent of the ruling party can be the target of wiretapping and surveillance by state institutions.

They locate problems/challenges in several key areas. First is the legislation that does not correspond to the real challenges in this area. The next problem is the lack of quality educated staff, i.e. insufficient human potential that has the necessary skills to respond to the challenges that exist in protecting privacy. The main reason for the poor quality of human potential is associated with the *lack of a merit system in state institutions and a clear career system* - partisanship in the public sector in employment that entails a number of other problems (ignorance and disregard for the scope of tasks, lack of strategic approach in development and lack of desire and personal motivation for self-improvement; not attractiveness and non-competitiveness of the public sector versus the private sector for people with exceptionally developed skills, etc.). All this contributes to the citizens' lack of trust in the specific institutions that should ensure their safety due to previous testimonies and experiences of their abuse in order to gain political, legal, and financial power. Therefore, a transparent, accountable and efficiently managed security system is an important part of democratic processes, especially for the protection of citizens' privacy. Timely detection, identification and signaling of certain weaknesses, inconsistencies and problems by the control and supervisory bodies provides a timely and appropriate response to protect citizens from intrusion into their privacy.

All interviewees indicated that they could not comment because they did not know what technical equipment and software the security services had. However, based on their personal perception, which they gained through monitoring the completed court cases and the huge number of publicly available quality recordings of illegally tapped conversations, they believe that they are on a solid level, ie that the state/or political party entities has quite good technical equipment with which it can at the same time to monitor a large number of citizens and to provide quality materials. According to media articles, some respondents indicated that they had received information about the existence of special equipment for interception of communications, ie. equipment that is usually placed in vehicles and that mimics the base stations of mobile operators. It can monitor the communications of the mobile telephony, but also the locations of the mobile phone users. Furthermore, they

pointed to *other controversial monitoring technologies,* such as FinFisher, which, according to media reports, the country also allegedly has, and which provides access to data and communications from mobile phones, computers, computer networks, equipment of telecommunications operators and others.

The next aspect discussed with the interviewees was whether the state needs foreign assistance / support to modernize the existing systems for monitoring / monitoring of citizens, but also to improve the mechanisms for protection against abuse (legal framework, institutional network, organizational structure, ...)?

All respondents agree that the country is in need and that it is already receiving assistance from other countries to modernize the existing surveillance systems, but also that it is not properly implemented. Some respondents indicated the need for the assistance to take the form of improving protection mechanisms and abuses by state institutions. *Unfortunately, through continuous inadequate security sector reforms and deep policy interference in all areas of security services, everything that was positive in the old system of security structures has been systematically destroyed and we are now dependent on foreign donations (wiretapping equipment, vehicles, foreign border police, drones and thermal cameras, etc.).*

Some respondents gave examples of the existence of *transport cameras that record the border area (van with built-in camera with the ability to record at night),* in support of dealing with the migrant crisis and illegal migration, as well as other such vehicles brought temporarily and/or donated to assist and support the state security system. They see the need for assistance from strong and stable foreign countries in presenting their security and surveillance systems in order to establish and set up a proper and more efficient system for monitoring and protecting citizens.

Another group of respondents pointed out that it would be very useful to use the good practices of European countries that are much more developed in this area, in terms of improving legislation, increasing the functionality of institutions and strengthening internal and external control and oversight mechanisms to increase and selective response to possible risks of abuse.

However, since North Macedonia is a NATO member country and a country with candidate status for EU membership, most of the respondents emphasized that the country, based on its own SWOT analysis of security risks and threats, strategic goals and environ-

ment, *should always first formally address NATO and EU member states to seek assistance from there*.

Furthermore, the respondents were asked whether the state receives assistance / support from foreign countries / organizations in various forms (equipment, training, financial assistance, expert support, etc.) in the field of monitoring / monitoring of citizens for different purposes in the last five years?

All respondents agree that the state receives assistance in the form of training, by foreign experts through projects by international NGOs operating in the field of good governance and security sector accountability. The reason for that is that there are not enough experts in the country in various segments in the field of security, hence the need to share foreign experiences. However, *the respondents do not know whether the state receives assistance specifically for the field of monitoring, but given that the country receives a lot of financial assistance for development through various forms and in various areas, it is likely that in this area the state will receive financial assistance, but also assistance in the form of equipment and training*.

Regarding the finances, some more informed respondents informed that the services are allowed open funds that they would use for various purposes, without great opportunities for their control and / or audit, hence, they can be easily misused. Suspicions about the procurement of equipment by certain surveillance and surveillance companies should be a top priority for the investigating authorities given the several criminal cases being prosecuted against certain individuals who have held senior positions in various security sector institutions.

The reasons behind why the country is receiving foreign aid is the weak budget, non-priority area for investment, lack of capacity, resources and knowledge, but also corruption, while the reasons why there is a foreign donor state is a strategic goal and interests, imposition of own resources (companies, experts, ...), influence, but also not having reliable and real information from the field for the needs of the state.

There are several respondents who believe that, although foreign aid may be present, *it still does not reach the end user directly,* ie the citizens do not feel its benefits directly.

At the end of the interview, respondents were asked to assess the effects of foreign assistance/support to the country in the field of privacy protection in the last five years: Ev-

eryone agrees that any support is welcome and the state must work to attract donors through whose projects the quality of existing work can be improved. The harmonization with the EU law is especially important, especially in the field of protection of privacy and human rights. One group of respondents believes that the effects of foreign aid and support are minimal or poorly visible to citizens due to the fact that there is still suspicion that remains from past cases where the right to privacy and protection is violated. Despite the reforms in the security-intelligence sector (legislative, organizational, structural, etc.) there is still not enough capacity of the state to be able to independently deal with and ensure the protection of privacy without the help of foreign donations. *Reforms in the country's security and intelligence sector have begun but not been completed. They are partial and therefore changes are needed that will provide greater professionalism and more substantial protection of citizens' privacy, through more serious action of the competent independent control and supervisory bodies, bodies and institutions, and of course increase the involvement of civil society in control mechanisms and oversight of this sector will help improve the protection of citizens' privacy.*

However, several respondents also emphasized that no one helps without receiving something in return. Thus, some of the foreign experts and helpers, ie implementers of programs supported by foreign aid are intelligence officers who collect information from the field and who have already mapped all the capacities and weaknesses in various areas of the country.

SERBIA

According to a report, published by the Belgrade Center for Security Policy (BCSP) in November 2020 titled Many Faces of Serbian Foreign Policy[171], the main drivers of foreign and security policy in the country are the EU, China, the US and Russia. This represents the country's efforts to maintain favorable relations with both the East and the West. As one journalist interviewee noted for this research, the country has set its sights towards many different foreign governments in order to develop its surveillance and overall technological capabilities. Connections with Russia, the US, Great Britain, the EU and Israel were all mentioned.

In Serbia, China has managed to establish itself as the dominant foreign aid supplier for often controversial projects as well as those projects[172] that usually shy away from prioritizing human rights and freedoms. Despite public perceptions, the European Union remains the countries' main financial aid provider[173]. Based on the information collected, it is safe to say that the amount of foreign aid supplied by the EU and organizations like USAID to Serbia, since 2015 has steadily increased. While for instance, USAID's total amount of funds donated to government and civil society and conflict, peace and security sectors in 2015[174] was $27,319,292, in 2020 that amount rose[175] to $33,744,148 (it should be noted that both the 2020 and 2021 financial reports are only partially reported). Overall, according to the data, Serbia has received a total of $189,046,207 in foreign financial aid from the US from the period of 2015 through 2021.

Although there are no definitive descriptions of where this funding is going towards, combating terrorism and rule of law initiatives are mentioned, as well as IT services operations and maintenance, border security assistance and military financing for education and training.

171 https://bezbednost.org/wp-content/uploads/2020/11/MANY-FACES-OF-SERBIAN-FOREIGN-POLICY.pdf

172 https://www.clingendael.org/pub/2020/china-and-the-eu-in-the-western-balkans/1-chinas-approach-to-the-western-balkans/

173 https://europa.rs/eu-assistance-to-serbia/?lang=en

174 https://foreignassistance.gov/cd/serbia/2015/obligations/0

175 https://foreignassistance.gov/cd/serbia/2020/obligations/0

2020						
$33,744,148	Governance	US Agency for International Development [$26,592,312]	$12,690,720	Government and civil society [$12,559,849]	Democratic participation and civil society [$7,587,036]	Competitiveness systems strengthening [$3.9m]
					Public finance management [$1,700,000]	Government accountability initiative [$2.2m]
	Administrative Costs		$5,153,293	Operating expenses [$5,156,678]	Operating expenses [$5,156,678]	Cooperation for growth activity [$2.1m]
						UNICEF MCH umbrella grant [$1.4m]
						Miscellaneous [$1.1m]
	Governance	Department of defense [$4,651,932]	$4,651,932	Conflict, peace and security [$4,651,932]	Security system management and reform [$4,651,932]	DOD - Foreign military financing (FMF) program, payment waived [$4.4m]
						DOD - international military education & training (IMET) program/deliveries [$217k]
						US department of defense, institutional capacity building programs: US European command (USEUCOM) ECJ5 directorate [$18k]
						US department of defense, institutional capacity building programs: strategy, plans and programs [$10k]
						US department of defense, institutional capacity building programs: George c. Marshall European center for security studies [$5k]

Among other notable donors that contributed to the country's technological development in the areas of police and border security, the Kingdom of Norway has stood out. The Kingdom of Norway has thus far provided help to Serbia's Ministry of Interior with donations amounting to approximately €12.4 million[176] through various projects. Within these project donations, the two countries signed a Memorandum of Understanding[177] in 2019 which aimed to raise the MOI's internal capacities, especially in the field of criminal investigations, with a donation of € 3.7 million which was used to raise the capacities of the Ministry of Interior, primarily the Criminal Investigations Directorate. The NCIS agreement was signed on September 16, 2019 by the Deputy Prime Minister and Minister of the Interior, Nebojša Stefanović, Minister of Justice, Nela Kuburović, Minister of Finance, Siniša Mali, Republic Public Prosecutor, Zagorka Dolovac, Deputy Organized Crime Prosecutor, Jasmina Milanović Ganić, Director of the Anti-Corruption Agency, Dragan Sikimić and Director of the Office of the National Security Council and Classified Information Protection, Goran Matić. The Kingdom of Norway has also donated equipment to the MOI in order to allow officers to "analyze content found on mobile telephones and computers".

Title	Date	Donation amount	Donors	Beneficiaries
Contribution to Strengthening Serbian Police Capacities in Fight Against Crime	March 29, 2019	€ 3,700,000	The Kingdom of Norway United Nations Office for Project Services (UNOPS)	Ministry of Interior of the Republic of Serbia
New Forensic Equipment for the MOI	June 22, 2019	600,000 €	The Kingdom of Norway	MOI Serbia

The Kingdom of Norway United Nations Office for Project Services (UNOPS) were contacted in regards to the project, and were responsive and offered to submit information on donations to Serbia, citing that: In 2018, *two traffic control devices (cameras) for the PU Smederevo were purchased and installed by the MoI and integrated into the existing systems. Therefore, no training was conducted in relation to the use of the cameras. In 2019, video monitoring systems were purchased and installed on five storage containers*

176 https://www.norveskapodrskamup.rs/en/vtext/nova-forenzicka-oprema-za-mup-od-kraljevine-norveske

177 https://www.norveskapodrskamup.rs/en/vtext/potpisan-memorandum-o-razumevanju-koji-ce-doprineti-jacanju-kapaciteta-srpske-policije-u-borbi-protiv-kriminala

for psychoactive substances delivered within the Project to PU Uzice, PU Nis, PU Novi Sad, PU Grad Beograd, and UKP. The video systems are integrated into the existing internal monitoring systems and connected to the intranet. There was no training organized for these systems except user instructions provided to the respective members of Emergency services (Dežurna služba), except in PU Užice where the surveillance was connected with the system of Border police (Granična policija)".

During the signing of the Serbia-Kosovo Agreement at the White House in 2020, both parties committed to technology upgrades to combat illicit activities by implementing and operationalizing US-provided screening and information systems, including PISCES, APIS, ATS-G, and STRP. The Personal Identification Secure Comparison and Evaluation System (PISCES) is a border security control database largely based on biometric data developed in the US. The system is primarily used by immigration, police and intelligence headquarters.

The system collects and retains personal information of all persons crossing the border in a downloadable format. Although no official information is available on the uses of intrusive surveillance technologies at the borders, testimonies of people attempting to go over the Serbia-Hungary border crossings allege that technologies such as drones and thermal cameras[178] have come into use. Through the UN's International Organization for Migration (IOM) projects such as the EU Support to Border Management program[179] (EU Ref no. CRIS 2018/400-805; November 2018 – October 2019), which aims to support Serbian border and migration management capabilities, the contract allocates € 20,000 for the purchase and installation of 100 video surveillance cameras, € 99,500 for two heartbeat detectors, € 71,700 for 30 long range night observation devices, € 22,600 for two digital video endoscopes and € 36,500 for unmanned aerial devices. Additionally, the names of the contractors are available, but no further specifics on the equipment is.

For instance, one of the companies, Damiba[180], which is a grant beneficiary for procuring 30 long range night observation devices and unmanned aerial devices in the EU Support to Border Management project, for a total amount of € 108,200, has an almost entirely empty website, with its about us page written in lorem ipsum text. The rest of the page is unresponsive or empty, but the company does mention that it allegedly offers specialized courses "in the domain of infrared thermography and thermos-vision".

178 https://www.norveskapodrskamup.rs/en/vtext/potpisan-memorandum-o-razumevanju-koji-ce-doprineti-jacanju-kapaciteta-srpske-policije-u-borbi-protiv-kriminala

179 https://serbia.iom.int/sites/g/files/tmzbdl1126/files/projects/documents/Summary Template EU funded contracts - Special Measure Phase 3 2019.pd

180 https://damiba.rs/o-nama/

Grant/procurement contract's details EU Support to Border Management - Phase 3			
Title of grant/procurement contract:	**Name of grant beneficiary or contractor**	**Date of grant/ procurement contract**	**Amount of grant/ procurement contract and currency**
Purchase and installation of 100 video surveillance cameras	Smart Building Technologies	25/2/2019	€ 20,000
Purchase of 2 heartbeat detectors	Trokut test	24/5/2019	€ 99,500
Purchase of 2 digital video endoscopes	XOPYC doo	19/05/2020	€ 22,600
Purchase of 30 long range night observation devices	Damiba	05/08/2019	€ 71,700
Purchase of unmanned aerial devices	Damiba	06/10/2019	€ 36,500

On the EU's Serbia chapter website[181], a number of projects funded by the European Union are listed, totaling around 18 million euros (the projects listed run through 2018-2023). In addition to this, there are a number of projects and donations that are funded through various European countries, but not EU members, such as Switzerland, Norway, the UK etc. However, the information for these projects is mostly inconclusive, with very few project reference numbers being provided, as well as exact donor and beneficiary information usually lacking. Most of the interviewees agreed that there is not enough publicly available information on surveillance technologies used by the state. Because of irrational fears, as is stated, the government is very secretive about their procurement of such technologies and software, which only increases the publics distrust.

181 https://www.euzatebe.rs/en/projects

Project	Funding	Amount	Implementation period	Beneficiaries
Regional Support to Protection-Sensitive Migration Management in the Western Balkans and Turkey – Phase I	European Union (EBCGA, EASO and UNHCR)	n/a	2016-2019	Ministry of Interior, Border Police Directorate
Strengthening the capacity of the first HBRN response and regional cooperation in Southeast Europe, the South Caucasus, Moldova and Ukraine	United Nations Belgium, Poland, Slovakia, The Netherlands	€3,500,000 (€500,000 per country)	2015 - December 2017	Ministry of Interior, Sector for emergency situations Serbia, Montenegro, Bosnia and Herzegovina, North Macedonia, Albania, Moldavia, Ukraine, Armenia
Providing specialized and technical training to improve the reaction ability of so-called first line defense officers	European Center for Chemical, Biological, Radiological and Nuclear Materials and Explosives at the University of Umeå in Sweden.	€400,000	2015	Ministry of Interior, Criminal Police Directorate, Emergency Situations Sector, Police Directorate, Traffic Police Directorate, Border Police Directorate, Gendarmerie, PTJ, SAJ, negotiating team, possibly a helicopter unit. Region of Southeast Europe, Caucasus, Moldova and Ukraine, Albania, Croatia, Serbia, Montenegro, Macedonia, Bosnia and Herzegovina, Armenia, Georgia and Ukraine.
EU Support to Border Management	European Union	€3,000,000	November 2018 - June 2020	Border Control
EU grant: Strengthening the capacity of the Serbian administration (Commissariat for Refugees and Migration, Ministry of Labor, Employment, Veterans and Social Affairs and Ministry of Interior) to respond effectively to increased migration flows	European Union	€1,499,940	12 months	Commissariat for Refugees and Migration, Border Police (MOI)
Future Trust	European Union	n/a	36 months	MOI, Sector for Analytics, Telecommunications and IT

In 2020, the Strategy for the Development of Digital Skills[182] was introduced in the country which promotes improving the public's digital capabilities as well as enhancing inter-sector cooperation. The Strategy is aligned with the European Initiative on AI[183], which underlines the European Commission's stance on Artificial Intelligence. The Strategy covers the period from 2020 to 2025 and is being implemented through collaboration between the Presidential Cabinet, the Ministry of Education, Ministry of Agriculture, Ministry of Trade, Tourism and Technological Development, Ministry of Finance, the Office for Information Technology and E-Government, the National Science Fund, University representatives (Faculty of Electrical Engineering, Faculty of Mathematics, Faculty of Mechanical Engineering, Faculty of Organizational Sciences, Teaching Faculty, Institute Mihajlo Pupin) as well as representatives of the economy dealing with the development and application of Artificial Intelligence and representatives of the Vojvodina ICT Cluster Association, the Petlja Foundation, the Chamber of Commerce of Serbia and the World Bank. According to the Government Artificial Intelligence Readiness Index for 2020[184], Serbia ranked 43 ahead of all other countries in the Western Balkans. Montenegro ranked 70, North Macedonia 73, Albania 85, Bosnia and Herzegovina 100 and no data is available for Kosovo.

The Serbian Strategy for the Development of AI (2020-2025)[185] aligns the development of an AI framework with the existing regulatory legal frame through 12 laws which entail the Law on Electronic Communications ("Official Gazette of the Republic of Serbia", no. 44/2010, 60/2013, 62/2014, 95/2018), Law on Information Security (6/2016, 94/2017, 77/2019), Law on Higher Education (88/2017, 27/2018, 73/2018, 67/2019), Law on Data Protection (87/2018), Law on the Fundamentals of the Education System (88/2017, 27/2018, 10/2019), Law on Primary Education and Upbringing (55/2013), Law on Dual Education (101/2017), Law on the Dual Education Model in Higher Education (66/2019), Law on Science and Research (49/2019-3), Law on Innovative Work (110/2005, 18/2010, 55/2013), Law on the Science Fund of the Republic of Serbia (95/2018-353), Law on Electronic Administration (27/2018). The Strategy aims to improve the education system, the economy, higher education, the ethics of AI use as well as the legislative framework. Additionally, the Strategy is also the first of its kind in the region[186]. While biometric surveillance or any surveillance capabilities and systems are not explicitly mentioned in the Strategy, it is assumed that its implementation will foster the need for biometric databases and that AI will be used to collect, store and process personal data.

182 http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/strategija/2020/21/2/reg/

183 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN

184 https://www.oxfordinsights.com/government-ai-readiness-index-2020

185 http://www.mpn.gov.rs/wp-content/uploads/2019/11/1-Nacrt-strategije-razvoja-ve%C5%A1ta%C4%8Dke-inteligencije-u-Republici-Srbiji-za-period-2020.-2025.-godine.pdf

186 https://novaekonomija.rs/vesti-iz-zemlje/prvi-u-regionu-vlada-srbije-donela-strategiju-razvoja-ve%C5%A1ta%C4%8Dke-inteligencije

European Commission's Instrument for Pre-Accession Assistance (IPA II) (2014-2020)

The European Commission's Instrument for Pre-Accession (IPA) presents a means by which the EU offers support for EU candidate countries in terms of financial and technical assistance. The current beneficiaries of IPA II for 2014-2020 are the Western Balkans, more specifically, Albania, Bosnia and Herzegovina, Kosovo, Montenegro, North Macedonia, Serbia and Turkey. The EU's financial assistance through IPA helps counties align their legislative frameworks, as well as their practices with the expected EU standards, in order to ascend to membership status. The first IPA took place from 2007 to December 2013, and focused on five key areas: transition assistance and institution building, cross-border cooperation, regional development, human resource development and rural development. The second, IPA II agreement[187], which is currently relevant, underlines strengthening capacities in the police cybercrime and special prosecution departments. The extent of the assistance is currently unknown, except the total funding allocated from 2014-2020 is €1.539,1 billion. The document notes that "In the field of cybercrime, there is a need for further resources, specialist tools and capacity-building for authorities to manage the increasing volume and complexity of the task". As part of IPA II, the EU-funded TWINNING project for "Support to Strengthening Fight Against Trafficking in Human Beings" notes that "Special investigative techniques such as wiretapping, surveillance, investigation of money flows, financial investigations, undercover investigators, etc. are being used in few cases. There is a lack of specialized technical equipment for using special investigative techniques and professional training for police officers right for delicate operations using special investigative measures". IPA II has been completed on December 31st 2020, however the implementation of the funds is still ongoing. IPA III, which will be in place from 2021 through 2027, has been established[188] in June 2021.

Safe City project with Huawei (2014-)

The question of widespread mass surveillance has been of increasing relevance in Serbia in the past few years. Especially during the coronavirus lockdown, the number of surveillance cameras installed by law enforcement officials on the streets had exponentially increased.

In December 2014, the Serbian Ministry of Interior signed a Memorandum of Understanding with Huawei which stipulated the implementation of the "Safe City" project. The Chi-

187 http://www.evropa.gov.rs/Documents/Home/DACU/12/74/235/ISP%20Serbia.pdf

188 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/1820-Multiannual-Financial-Framework-IPA-III-Regulation_en

nese government backed Huawei project stipulates the implementation of mass biometric surveillance across the Serbian capital Belgrade and eventually the whole country. The official justification of the project is described as beneficial in curbing crime across the country and upholding the rule of law.

On March 7 2019, the Serbian Ministry of Interior responded to SHARE Foundations FOI request in regards to then-Minister Nebojsa Stefanović's statement on the rollout of the surveillance technology. In the response, the MOI refused to answer the questions that were posed, such as the proposed regulatory framework for analyzing and storing collected data, as well as any information regarding the tenders and procurement of the surveillance technologies. All of the documentation surrounding the procurement of the equipment is labeled **CONFIDENTIAL**. The Ministry also stated that a Data Protection Impact Assessment (DPIA) was not conducted since this regulation is still not applicable because the Serbian legal framework does not regulate facial recognition and biometric data processing.

In December 2016, the Government gave consent for signing the Agreement on the Strategic Partnership[189] of the MOI and Huawei for introducing eLTE technologies and "Safe City" solutions in the systems of public security. The agreement was signed[190] in February 2017.

There are three types of cameras that are being used within the program:

- **IPC6625-Z30 2-Megapixel 30x Intelligent IR High-Speed PTZ Dome Camera[191]**
  As is noted on Huawei's website, the Dome Camera can reach a distance of up to 150 meters and features functions such as image stabilization, intelligent video analysis methods and metadata backhaul. It is also susceptible to various weather and outdoor events.

- **IPC6225-VRZ-ES 2.0-Megapixel IR Bullet IP Camera with a Motorized Zoom Lens[192]**
  The Bullet Camera reaches up to 80 meters distance and contains a built-in infrared lamp, and is capable of producing high-quality images, even in poor lighting conditions, both inside and outside.

189 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/1820-Multiannual-Financial-Framework-IPA-III-Regulation_en

190 https://bit.ly/3aWRz7m

191 https://e.huawei.com/en/products/enterprise-networking/video-surveillance/hd-ip-cameras/ipc6625-z30

192 https://e.huawei.com/en/products/enterprise-networking/video-surveillance/hd-ip-cameras/ipc6225-vrz-es

- **IPC6285-VRZ 4K Low Light Network IR Bullet Camera[193]**
  Unlike the previous two camera models, the IPC6285-VRZ product information is not available on the Huawei website. The only available information is that the model is also a part of the Huawei Software-Defined Cameras (SDC) Series of Professional AI High-end series[194] which possess intelligent vehicle analysis, crowd flow analysis, behavior analysis as well as person capture and personal feature extraction.

There are currently over 1000 cameras[195] that have been installed on the territory of Belgrade.

Additional Surveillance in the Country

In October 2021, information became available that the city of Novi Sad, the second largest city in Serbia, was setting up surveillance cameras on some of its biggest markets[196]. Even though the acquisition of the surveillance technology itself is nothing new, the equipment in question raised some issues. Apparently, the acquired surveillance technology contains facial recognition and license plate software and also allows for creating a vast database of faces, which can be cross-referenced.

The concerning aspect of the implemented technology is the fact that it does not belong to any intelligence agencies or the police, but rather is in the jurisdiction of a public company in charge of taking care of the city markets. The project is valued at around €40,000. The market surveillance case is similar to the mass biometric surveillance deployment project in Belgrade in that it has no legal basis in Serbian jurisdiction as of currently, therefore, the procurement is highly disputable.

Smart Serbia (2021-)

In early June 2021, the Serbian Office for IT and eGovernment announced the "Smart Serbia" project, which, for now has been presented as a centralized platform of all citizens' personal data. The platform will aim to cross reference all publicly available information and data of citizens which was collected prior for different purposes, such as through the

193 https://support.huawei.com/enterprise/en/intelligent-vision/ipc6285-vrz-pid-22034864

194 https://support.huawei.com/enterprise/en/doc/EDOC1100172551?idPath=7919749%7C7919735%7C250985939%7C22034864

195 https://hiljade.kamera.rs/en/home/

196 https://www.021.rs/story/Novi-Sad/Vesti/287549/Novosadjani-ce-biti-snimani-i-na-pijacama-Trznica-nabavila-spornu-opremu-za-identifikaciju-lica.html

eHealth or eEntrepreneur portals. In the press release it is mentioned that the platform was developed on Microsoft technologies, with the support of Azure Stack Hub, and that it will be located in the State Data Centre in Kragujevac. The Government of the Republic of Serbia is the first in Southeast Europe to own and use Azure Stack Hub technology in this capacity. No further information was provided in regards to the project so far. The project does resemble previous ones developed around the world such as the Indian Aadhaar, the world's largest biometric ID database system, which has garnered a lot of controversy due to its security breaches[197]. However, its implications definitely pose a potential threat, as such a massive centralization of citizens data is unprecedented in the country, and given the governments previous track record of data leaks[198] and ransomware attacks[199] on state servers and technologies, it seems as though the country does not as of currently have a sustainable system for ensuring that the data will not be compromised.

As of November 2021, no additional information has been provided in regards to the project, the data center or the system itself. Although official information on public procurement is scarce, the interviewees for this project agreed that information technology seems to be an area of interest and that a lot of funding is being directed towards it in the past couple of years.

Circles & Hacking Team

In December 2020, the University of Toronto's Citizen Lab research center identified about two dozen countries that are likely users of the Israeli surveillance company Circles' software[200]. Serbia's Security Intelligence Agency (BIA) was identified as a likely customer of the surveillance system, which allows for phone tapping, message monitoring and phone location tracking through its services by exploiting weaknesses in mobile telecommunication infrastructures.

This wasn't the first time that Serbian intelligence agencies were implicated in shady deals with surveillance companies. In 2015, a leak of internal documents, client lists and emails revealed that BIA had engaged in negotiations with Hacking Team[201], a well-known Italian

197 https://techcrunch.com/2019/01/31/aadhaar-data-leak/

198 https://resursi.sharefoundation.info/en/resource/personal-data-of-more-than-5-million-citizens-of-serbia-unlawfully-published/

199 https://emerging-europe.com/business/novi-sad-cyber-attack-highlights-need-to-take-data-security-seriously/

200 https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/

201 https://labs.rs/en/hacking-team-the-italian-job-of-serbian-security-services/

surveillance software vendor in an effort to purchase the company's surveillance software. However, there was no evidence that the software was purchased in the end.

The BIA has notoriously been silent about its dealings with foreign surveillance companies, but also with its internal procedures with domestic telecommunication companies. According to the Law on Electronic Communications, internet service providers and telco companies in Serbia are obligated to retain all communication metadata of citizens on their systems for 12 months. The competent authorities can then request access to the metadata for the purposes of investigating crimes and protecting national security. Even though a decision by the Constitutional Court declared that a court order is necessary for the relevant authorities to access communication metadata, SHARE Foundation has through its research discovered that intelligence agencies such as BIA gain access to citizens' metadata through "applications for independent access"[202]. Through these applications, the police, as well as military and intelligence agencies can directly access metadata by way of software that connects the telecommunications firm with the relevant state body and grants it full access to the mobile carrier's database. Another example is the "direct access" mechanism, which provides BIA with its own special connection to the telcos infrastructure and allows the agency to surveil and intercept communications in real time on the carrier's network. Clearly, the direct access route is in conflict with the country's legal framework on electronic communications and presents a clear and intrusive violation of civil liberties for the citizens of Serbia.

According to Article 130a of the Law on Electronic Communications, network operators must submit annual records of access to retained data to the Commissioner for Information of Public Importance and Personal Data Protection, which must contain the number of requests, the number of granted requests and the number of days between the initial data retention and the time of requested access. However, every year less information is being submitted to the Commissioner, with some telecommunications companies submitting no information at all. Instances of wiretapping and surveillance have been most notable against journalists, activists and opposition politicians. In 2018, the national ombudsman ordered BIA to respond[203] to the allegations that it had released personal information of investigative journalists Stevan Dojčinović to government affiliated tabloids, such as his personal correspondence via text messages. The agency never filed any response nor commented on the allegations.

202 https://labs.rs/en/hacking-team-the-italian-job-of-serbian-security-services/

203 https://www.krik.rs/en/serbian-ombudsman-issues-order-intelligence-agency/

FOI Requests

Thus far, the Serbian government agencies which were contacted have been unresponsive to the freedom of information requests sent by researchers. As seen previously in the report, this is not unusual when it comes to inquiries about government funding or plans for pursuing modern and invasive technologies or legislative changes to a certain extent. Hence, no information was obtained from the Ministry of Interior or the Ministry of Defense. The Ministry of European Integration responded to the request, stating it has not been the recipient of any foreign aid nor is the Ministry currently involved in any projects that deal with procuring surveillance equipment or revising the current legal framework as it pertains to surveillance practices in the country.

As for the interviews conducted for this project, the overall agreement was that public information is lacking when it comes to the procurement and implementation of surveillance technologies in the country. Another worry is that these systems and equipment are not being used to enhance citizen's security, but rather focus on crime prevention. The problem however, as one interviewee points out, is that citizens seem to be unaware of the level of security threats that demand these kinds of invasive technologies to be implemented, and especially in such a covert manner. Additionally, one of the main issues is that there is a lack of education when it comes to the use of these systems by government officials. As has been noted in this report, there has been a number of mishandlings of these and similar systems, which indicates a greater need for education in order to handle and properly use such technologies and systems.

Regulations

The current Serbian framework in the area of surveillance practices is very unspecific, but changes have been starting to arise. As was previously mentioned in the report, the Huawei affiliated project which includes the deployment of a mass biometric surveillance system throughout Belgrade primarily for the time being, has caused the administration to consider changes to current legislation.

However notably, in 2018, Serbia adopted its own variation of the General Data Protection Regulation or the GDPR, or the Law on Personal Data Protection[204] (87/2018), which is highly compliant with the EU's version. Despite the implementation of this comprehensive framework, the opportunity was missed to more closely regulate the specific area of

204 https://www.paragraf.rs/propisi/zakon_o_zastiti_podataka_o_licnosti.html

surveillance technology use within the country. There are some provisions which concern video surveillance for example, but they are scattered throughout various laws, mainly the Law on Police and other intelligence agencies. Article 52 of the Law on Police[205] (87/2018) which relates to video recording in public places states that the police are allowed to conduct surveillance of public spaces, through the use of audio-video equipment. However, it is noted that the police are obligated to "publicly announce that they are carrying out the surveillance, except when a covert recording is carried out in accordance with the Code of Criminal Procedure". Additionally, the data collected through this surveillance are stored in line with the prescribed records, while the data that cannot be used in the procedure is to be destroyed within a year. "The manner of recording in a public place and the manner of announcing the intention of that recording shall be prescribed by the Minister". Alongside the police, municipal police is also authorized to use video-audio surveillance equipment, as per Article 25 of the Law on Municipal Police[206] (49/2019).

According to Article 12 of the Law on Security Intelligence Services[207] (55/2012), the Military Security Agency (VBA) and the Military Intelligence Agency (VOA) agencies have the authority to use equipment for observation, surveillance and recording purposes. The powers allocated to BIA are similarly regulated. It is important to underline the difference between the police and secret services here – the police have permission to set up and use audio-video equipment in public, while the secret services are authorized to conduct secret surveillance of citizens, with appropriate permissions granted by the competent authority. In relation to this legal framework, the set-up of a surveillance system warrants a Data Protection Impact Assessment by which the Commissioner for Information of Public Importance and Personal Data Protection can assess the effects of such a system on the rights of citizens. If it is determined that such a planned system would be too invasive in regards to citizens' right to privacy, the Commissioner will recommend the project be adjusted in such a manner to diminish the impact on citizens' privacy and other rights.

In September 2019, in accordance with the newly adopted Law on Personal Data Protection, the Ministry of Interior conducted a DPIA on the new surveillance system but did not publish it, claiming that it was internally sent to the Commissioner for Personal Data Protection for review. The DPIA became publicly available in November 2019, but was seen as unable to provide a justification for the system's implementation. Additionally, the Commissioner agreed and also gave an opinion on the DPIA, claiming that it was not in ac-

205 https://www.paragraf.rs/propisi/zakon_o_policiji.html

206 https://www.paragraf.rs/propisi/zakon_o_komunalnoj_policiji.html

207 https://www.paragraf.rs/propisi/zakon_o_vojnobezbednosnoj_agenciji_i_vojnoobavestajnoj_agenciji.html

cordance with the law. In regards to the mass biometric surveillance project in Belgrade, given the fact that the assessment was ordered only after the implementation of the project was well under way, clearly indicates that there was not enough awareness of this institution the need to act in full compliance with the obligations from the Law on Personal Data Protection.

In May 2021, during a public hearing, representatives of the MOI claimed that the biometric capabilities of the surveillance system were not yet being used on the streets of Belgrade, and that this was still not in accordance with the Law on Internal Affairs, which was going to be reformed.

On September 15, 2021 the new draft of the Law on Internal Affairs was released on the Ministry's website pending public debate. The new law outlines the use of systems for data processing, as well as expands the capabilities of the police to use biometric data for suspect recognition. The discussions on the proposed revised law took place on September 17 and following the public debate, the Ministry of Interior reviewed the comments and concerns and was set to proceed with the law's introduction. After a public debate on the draft law, and much criticism by civil society actors, on September 23, the Minister of Interior, Aleksandar Vulin announced that the decision had been made to withdraw the controversial draft law[208].

Despite the confidential nature of the government's procurement of such softwares and surveillance equipment, certain information does become available from time to time and allows for CSOs, journalists, advocates and citizens to take a look into the state's attitudes and approaches to surveillance technologies. Stories that concern mass biometric surveillance practices in Belgrade, as well as proposed surveillance equipment installment in other cities in the country tend to draw a lot of attention from the public. This shows that citizens are willing to engage and learn more about these technologies, but as the interviewees agreed, there is a big need for the state to allow a level of participation from the public for these projects. Citizens need to understand the depths of these technologies, and be assured that they are not being used to compromise their rights, their privacy, security and dignity.

208 https://www.sharefoundation.info/en/draft-withdrawal-a-step-towards-moratorium-on-biometric-surveillance/

Policy Recommendations

Given that the current legal framework does not support biometric facial recognition technologies as well as the non-transparent approach of the government towards such issues, some recommendations that should be considered should deal with:

- Currently, **the government and the Ministry of Interior should move towards a ban on mass biometric surveillance** in Belgrade and all other planned cities in the country in order to comply with the European Convention on Human Rights, as well as the European Parliaments resolution[209] on banning mass biometric surveillance;
- **Legal regulation should be put in place** which deals with the use and implementation of surveillance technologies, through detailed provisions for the types and locations in which the surveillance might be put in place as well as aligning this regulation with the existing Law on Personal Data Protection;
  Providing adequate protections for any personal information that might be compromised in the use of such invasive technologies, and holding subjects accountable for misuses of such systems;
- **The government should be more responsive** and develop procedures in conjunction with civil society organizations and journalists working on these issues, and consider their questions and concerns, as well as the concerns of the broader public;
- **The government should take a more transparent approach** in their procurement of surveillance technologies and their usage, such as educating public officials and data protection officers, which can guarantee the necessity and proportionality of the use of such technologies;
- **International bodies should advocate** for stronger stances when it comes to issues of mass arbitrary surveillance practices being imposed in the country in order to help raise awareness of the potential detrimental effects of these technologies;
  National data protection bodies need to increase their oversight on issues related to mass surveillance and personal data processing within the country across all sectors;
- **Donors and international bodies should be more hands on** when it comes to vetting and evaluating the companies which are awarded aid, especially in the realm of potentially invasive technologies and equipment.

209 https://www.europarl.europa.eu/doceo/document/A-9-2021-0232_EN.html

SUMMARY

The data from the conducted research show that in the countries of the Western Balkans there are more donors in the field of law enforcement, through capacity building or donation of different equipment, with indication as "for the fight against organized crime, migration or good governance". The USA and EU are the greatest donors, yet there is Turkey and China, that show willingness to increase their influence in the region, but specifically for one or two countries at most.

EU appears to be a major donor, but on the other hand there are also EU member states operating outside the Western Balkans Investment Framework[210] (WBIF), like Sweden[211], but also non-EU countries which through various projects, through international or inter-governmental organizations (OSCE Missions, DCAF), long-term programs and strategies, which are specifically designed for the development of the Western Balkan countries (Norway[212], Sweden, UK, Switzerland). In total, by the end of 2020, Bilateral Donor contributions reached €107.31 million, including €5.17 million transferred from the EBRD Western Balkan Fund at the inception of the WBIF. The largest individual cumulative pledges to date have been made by Norway, Sweden, Austria, Germany, Italy, and United Kingdom. Austria is the current WBIF Co-Chair.[213]

There are already enough challenges in the policy area of unlawful interception of communications. Countries have history of scandals and reform processes which are supported by foreign countries in the format of expertise. There is a lack of institutional transparency to be more specific of foreign aid in surveillance. Further deficiency exists in the level of knowledge for privacy protection and information on risks from new digital technologies and possibilities for interception of communication.

210 https://www.wbif.eu/#:~:text=Welcome%20to%20Western%20Balkans%20Investment,Montenegro%2C%20North%20Macedonia%20and%20Serbia

211 https://www.swedenabroad.se/pt/embaixada/north-macedonia-skopje/current/news/the-swedish-government-adopts-a-new-reform-strategy-for-the-western-balkans-and-turkey-for-2021-2027/#

212 https://www.unops.org/serbia

213 https://wbif.eu/about/bilateral-donors

www.impetus.mk