European Parliament
2019-2024

Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware

20.10.2022

MISSION REPORT

following the delegation to Warsaw, Poland 19 - 21 September 2022

Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware

Members of the mission:

Jeroen LENAERS	(EPP) - Leader of the Delegation; PEGA Chair
Sophia IN 'T VELD	(Renew) - Rapporteur
Vladimír BILČÍK	(EPP)
Bartosz ARŁUKOWICZ	(EPP)
Juan Ignacio ZOIDO ÁLVAREZ	(PPE)
Katarina BARLEY	(S&D)
Łukasz KOHUT	(S&D)
Róża THUN UND HOHENSTEIN	(Renew)
Dominik TARCZYŃSKI	(ECR)
Marcel KOLAJA	(GREENS)

Introduction

The mission was the second fact-finding mission of the PEGA Committee after Israel in July 2022. The PEGA Committee delegation was composed by ten Members of six nationalities and from five political groups.

This first visit to an EU Member State was of paramount importance for the PEGA Committee.

Indeed, the plenary decision establishing the PEGA Committee specifically refers to Poland as one of the Member States to investigate as a priority, to gather information and facts on the use of Pegasus spyware.

The decision foresees that the committee of inquiry shall "investigate the scope of alleged contraventions, or maladministration in the implementation, of Union law, resulting from the use of the Pegasus and equivalent surveillance spyware, collect information on the extent to which Member States, including but not limited to Hungary and Poland, or third countries use intrusive surveillance in a way that violates the rights and freedoms enshrined in the Charter, as well as assess the level of risk this poses to the values enshrined in Article 2 TEU, such as democracy, the rule of law and respect for human rights" (P9_TA(2022)0071).

The PEGA delegation met with various persons to gather information and facts on the use of Pegasus spyware such as members of the Polish Senate's extraordinary committee on Pegasus, members of the Sejm, representatives of the Supreme Audit Office and the Ombudsman's office. The delegation also met judges with focus on judicial control of surveillance, heard from experts on Poland's security services, met with victims of spyware to hear their testimonials, and interacted with representatives of NGOs and civil society, journalists and other experts.

It should be stressed that, in the interest of a well-balanced approach for the work of the PEGA Committee, the delegation also sought to meet with representatives of the Ministry of the Interior and the Ministry of Justice as well as with the Polish Central Anticorruption Bureau (overseen by the Ministry of the Interior) but these requests were declined.

Summary account of meetings

I. MEETINGS ON MONDAY 19 SEPTEMBER

14:30 - 16:00 **MEETING WITH MEMBERS OF THE EXTRAORDINARY COMMITTEE ON PEGASUS WITHIN THE SENATE OF THE REPUBLIC OF POLAND**

Meeting with ***MPs Marcin Bosacki*** *(Chair of the Committee)****; Gabriela Morawska-Stanecka; Sławomir Rybicki; Magdalena Kochan; Jacek Bury; Wadim Tyszkiewicz***

Chair Bosacki gave an overview of the **extraordinary committee's work and findings**.

The Senate extraordinary committee was set up in January 2022 and has held 14 meetings and questioned 27 witnesses and experts. It has managed to gather a number of unquestionable facts confirmed by experts.

The Polish Central Anticorruption Bureau (CBA) bought the Pegasus software in 2017 to the Israeli company NSO Group through a private company for an amount of 25 million Polish Zlotys. The purchase was made using money from the Justice fund, which is replenished by a charge payable by anyone convicted for a crime. The funds money should, according to its statutes, be used for support to victims of crimes.

The Senate extraordinary committee has so far obtained confirmation of ten cases of phone infection by Pegasus. The earliest known case of Pegasus-use in Poland dates back from March 2018, the victim, Andrzej Długosz, CEO and co-owner of Cross Media PR agency, had been wiretapped 61 times by November 2019. The last known case dates from August 2021 and the victim was Prosecutor Ewa Wrzosek, a member of the Lex Super Omnia association, which fights against the politicisation of the prosecutor's office. The committee's findings also show that in 2019, during the parliamentary election campaign, the account of Senator Krzysztof Brejza, at the time the campaign manager of the opposition Civil Platform party, was hacked several times using Pegasus. The information obtained in this way - after being manipulated - was aired by public television to serve a massive disinformation campaign.

On the legal aspects regarding the use of Pegasus, members of the Senate extraordinary committee explained that the use of surveillance tool such as Pegasus against citizen is only permitted for security reasons under Polish law.

The CBA being a special service primarily responsible for combating corruption in public and economic life, particularly in public and local government institutions, does not address public security an could thus not use a tool such as Pegasus to perform any of its duties. Polish law was therefore violated as soon as this tool was acquired. The allocation of funds from the Ministry of Justice to CBA and the purchase of Pegasus through an illegal procurement procedure were breaching the very nature of the law.

The law on the use of surveillance tools has been amended several times but rather to extend the power of the police forces than to protect citizens from abuse.

Moreover, while CBA declined to confirm whether it has used Pegasus against any individuals but repeatedly argued that for any use of the surveillance tool, it had obtained legally required consents, serious concerns can be raised as regards the context in which the consents are given.

Indeed, it was stressed that Polish courts are not informed whether the requested surveillance would be carried out with the use of the Pegasus system or not. No time frame or detailed justification are required for surveillance requests under the law.

The members of the extraordinary committee added that they had no certainty as to where the data servers are located but that they had indications that the treatment of such data had been delegated to NSO, which would constitute another breach of the law and the right to privacy.

On the cooperation of the Polish authorities with the extraordinary committee, they underlined a total lack of cooperation. All government officials invited to testify before the committee had refused, including the Head of CBA. The illegality of the procurement procedure for the purchase of Pegasus did not trigger any investigation.

In the **Q&A session** with the Members, it was pointed out that the extraordinary committee had to be formed in the Senate as neither the State authorities, nor the Sejm had taken any action to clarify the matter. The Senate extraordinary committee does not have investigative powers, which allows those invited to appear before the committee to decline. The lower house (Sejm) has investigative powers and could open a committee of enquiry but is unlikely to do so given the majority of the ruling party in that house.

Members were informed that the Senate committee was currently working on two documents: a report on its findings and a proposal - based on the recommendations of the study "how to saddle Pegasus"- for legal solutions that would protect citizens from illegal surveillance and ensure control over the special services. They however stressed that, given the majority in the Sejm, such proposal had poor chances of success. They concluded stating that greater judicial control and parliamentary oversight will only be possible with a change of government.

16:30 - 18:00 **MEETING WITH MEMBERS OF THE SJEM OF THE REPUBLIC OF POLAND**

Speakers:

Polska 2050 Circle*: *Michał Gramatyka *(Member of the Digitization, Innovation and Modern Technologies Committee)**; Michał Kobosko*** (*1st VP of Szymon Hołownia's Polska 2050 Party*)

The Left Coalition Club (New Left, Partia Razem): Krzysztof Gawkowski *(Chairman of the Left Coalition Club, Member of the Digitization, Innovation and Modern Technologies Committee)**; Maciej Gdula*** *(Member of the Intelligence Committee)**; Wiesław Szczepański*** *(Head of the Administration and Internals Affairs Committee*)

Parliamentary Club of the Civic Coalition*: *Konrad Frysztak *(Member of the Digitization, Innovation and Modern Technologies Commission)**; Kamila Gasiuk-Pihowicz*** *(Vice-Chairwoman of the Justice and Human Rights Committee)**; Robert Kropiwnicki*** *(Vice-Chairman of the Civic Coalition Parliamentary Club)**; Maciej Lasek*** *(Member of the National Defense Committee)**; Arkadiusz Myrcha*** *(Vice-Chairman of the Legislative Committee)**; Tomasz Szymański*** *(Vice-Chairman of the Administration and Internal Affairs Committee)**; Witold Zembaczyński*** *(Member of the Legislative Committee)*

The various interlocutors explained their **concerns as regards the rule of law in Poland** and presented the Pegasus scandal as an illustration of Poland's slide towards an authoritarian

regime. They highlighted the disappearance of any system of checks and balances, the lack of cooperation of the executive branch with the legislative branch, the unacceptable illegal spying on citizens by the government as well as collusion between services, decision-makers and the judiciary.

The **absence of judicial oversight over the secret services** was stressed, so was the lack of scrutiny over CBA's expenses and activities. It was recalled that Pegasus was bought by CBA using money from the Justice Fund aimed at compensating victims of crime whereas CBA can only be financed from the state budget.

On the legal aspects regarding the use of Pegasus, the interlocutors pointed out that such tool could only be lawfully used to fight terrorism or organised crime but by no means to spy on political opponents or members of the civil society. It was stressed that judges are not given access to all data regarding requests (sometimes the name of the target is not even mentioned) and that the authorisation process does not imply any verification on the necessity and proportionality of the requested surveillance.

On discussions relating to the **legality of the last election process**, they confirmed that the use of Pegasus against Krzysztof Brejza, chief of staff of the opposition Civil Platform party in the 2019 electoral campaign, may have impacted the electoral results. When asked about their expectations on the fairness and transparency of the upcoming elections, they acknowledged that there were reasonable doubts about the legality and transparency, if a tool such as Pegasus would be used again.

It was further pointed out that it could not be excluded that Pegasus or other surveillance tools were still in use in Poland today. They added that the use of Pegasus to spy on people close to the ruling party could not be excluded either.

II. MEETINGS ON TUESDAY 20 SEPTEMBER

8:30 - 10:00 **MEETING WITH THE SUPREME AUDIT OFFICE (NIK)**

Meeting with ***Janusz Pawelczyk; Marcin Marjański; Grzegorz Haber*** *(Advisors to the President of the Supreme Audit Office)****; Łukasz Pawelski*** *(NIK press officer)*

The interlocutors explained **how the purchase of Pegasus was discovered by the Supreme Audit Office** (NIK).

In the framework of the 2018 state budget execution audit, NIK's auditors discovered an invoice covering 25 million PLN to purchase the Pegasus surveillance system for the Central Anticorruption Bureau (CBA).

The auditors found that the software was paid for with the resources from the Justice Fund, which pools money from court fines and is earmarked for helping victims of crimes and preventing further crimes by rehabilitating criminals. As CBA can only be funded from the state budget, the auditors assessed the purchase of Pegasus using money from this fund as illegal.

NIK therefore informed the responsible authorities and requested an enquiry to be opened on violation of budgetary procedure by high-ranking officials. After years, the investigation was dismissed: the Head of the Public Finance Discipline Office admitted that the purchase was made but authorised the invoice on the ground that there had been minor social harm.

After this first inspection, the President of the Polish Supreme Audit Office requested a second follow-up audit on how the funds were used. All identified irregularities have been notified to the Ministry of Justice but none of the actions required has been carried out. NIK nevertheless hopes to finalise this audit by the end of the year. NIK's inspections being confidential, no elements of the ongoing audit can currently be disclosed but some of the findings will be made public.

The interlocutors explained that the conduct of several audits unfavorable for the government and its agencies have put NIK in a difficult situation: they have for instance been informed by their operator that there were attacks on the office IT infrastructure as well as strong presumptions of surveillance and hacking of NIK employees and President Marian Banaś' close advisers' mobile phones.

The speakers further stressed that NIK was facing major difficulties impeding the proper conduct of its audits and the performance of its mission. Among the challenges: difficulties for NIK's auditors to successfully go through the vetting process run by special services; understaffing of the NIK Council as the requests to appoint new Members are not granted (the NIK President addressed 34 motions to the Speaker of the Sejm since 2019, out of which only 7 led to the appointment of new Members); systematic rejection of NIK's annual activity reports impeding their publications; lack of cooperation from audited services; rejection of auditing agenda, etc.

The President now considers that the NIK's independence is at risk and speakers explained they have triggered a SIRAM case (Supreme audit institution Independence Rapid Advocacy Mechanism) with the independent international team from the INTOSAI IDI (International

Organisation of Supreme Audit Institutions development initiative). The SIRAM is a four-stage process by which immediate or potential threats to Supreme Audit Institutions independence are reviewed and addressed. It is intended to provide a clear, streamlined fast-track process for addressing such threats.

It was explained that NIK has triggered this procedure following a breach of the NIK President's immunity when CBA officers entered the building illegally and searched the President's office and took his notebooks and phones. Other difficulties as described above are also part of the SIRAM case.

In the **Q&A session** that followed, Members expressed their stupefaction at the pressure exerted on the NIK and suggested that EUROPOL be requested to investigate, given the seriousness of the facts reported.

10:30 - 12:00 MEETING WITH GENERAL PIOTR PYTEL

General Piotr Pytel gave an overview of his career in the area of security: he has worked for many years in the State Protection Office, the General Customs Inspectorate and the Internal Security Agency. From 2014 to 2015, he was head of the Military Counterintelligence Service.

He stated that the use of Pegasus or other similar systems by the Polish services had no legal basis and was *de facto* a violation of the law. The use of Pegasus or similar spyware violates the rules of confidentiality, privacy and proportionality.

He explained that Pegasus cannot be used by the services for operational control because it does not meet the requirements of operational control instruments, i.e. it cannot be fully controlled. At the same time, he assessed the use of Pegasus as illegal because the system cannot be certified. This, in turn, results in a very high probability of disclosure of the information gathered to unauthorised persons.

According to general Pytel, the idea of buying Pegasus was unlikely to have originated in the CBA, but at a higher level. Indeed, if such a system was to be purchased, the CBA "should be at the end of the queue before other services but the truth is CBA is actually functioning as a political police force in our country at the moment" he noted. He added that the known cases of Pegasus use show that it was a decision of the authorities, of high-ranking politicians who wanted to have such a tool for political purposes.

In his opinion, Pegasus would be much more useful in, for example, the police, who have to deal with life-threatening situations. In this case, the use of Pegasus, as all indications suggest, was a manifestation of the services' activities in the political field, incompatible with their ethos.

He also mentioned the surveillance of Senator Krzysztof Brejza and stated that this was a typical "information-psychological" operation that started precisely with a political decision. It was intended not only to discredit him, but also to create a deterrent effect in wider circles of society and influence the results of the elections. He stated that the first stage was that the top itself agreed to subject Senator Brejza to this type of surveillance. The next stage was the planning, the gathering of materials. Then, the analysis of these materials.

In these materials, there was probably no information enabling to confirm any criminal activity

by Senator Brejza or bring charges against him. What happened next was a mystification/manipulation of his messages, which were widely broadcasted on television.

He stressed that "under a state of law, this system cannot be applied and used for operational control". Evidence obtained through Pegasus should not be admissible in court because the program can alter the content of the phone and can be used to create false evidence. There should also be oversight of these systems by a body independent of the services, and all regulations relating to the use of operational control should be amended.

During the **Q&A session with Members**, the general pointed out that the data collected with Pegasus were probably be located outside Poland and could be accessed not only by the NSO Group company from which it was purchased, but also by the secret services of another country.

When asked if he believed Poland was one of the two countries whose Pegasus' licence had been terminated, he stated that, according to his information, special services were most likely still using advanced surveillance systems, either Pegasus or similar or both. He said the use of invasive tools such as Pegasus was confirmed by the exponential increase in the number of cases of operational surveillance.

13:30 - 15:00 MEETING WITH PEGASUS VICTIMS

*Meeting with **Krzysztof Brejza** (Senator and chief of staff in the election campaign in 2019)**; Dorota Brejza (**attorney-at-law)**; Andrzej Malinowski** (economist, former head of Employers organisation)**; Michał Kołodziejczak** (political activist)*; ***Ewa Wrzosek** (Prosecutor)*

During the meeting, the delegation heard the testimonies of various victims of Pegasus surveillance.

Krzysztof Brejza explained that his phone had been monitored 33 times during a six months period during the 2019 election campaign (when he was chief of the opposition campaign). Manipulated material from his phone was used on TV in that period and this is how he found out he was being spied on.
The surveillance activities on phone were confirmed by Citizens Lab in 2021. The phones of his father and assistant have also been targeted by Pegasus. He and his attorney stressed that they had filed several cases in Polish courts related to the illegal use of Pegasus against him but that all cases were either pending or dismissed. They stressed that Senator Brejza's case was an illustration of the democratic decay in Poland and that the reason for his surveillance could only be politically motivated.

Andrzej Malinowski stated that the information about the surveillance was a surprise to him and he never expected to be spied on. In his opinion, there could be several reasons for the surveillance. First of all, from the beginning of 2015 he was a columnist for "Rzeczpospolita", where he wrote short texts on economic issues.

His columns were not about a specific political group, but about the introduced solutions related to the economy, hence not favourable to the ruling party. Another reason for his surveillance could be his work in the Council for Social Dialogue. Malinowski assessed that Law and Justice was not keen on conducting social dialogue within the Social Council. He also reminded that

the Legislative Monitoring Center was established within the Employers of the Republic of Poland, which assessed legislative activity in Poland on an ongoing basis. Unfortunately, for the majority of the government, the assessments were very poor he said.

Michał Kołodziejczak informed the delegation that his phone was spied on several times in May 2019, a few months before the parliamentary elections, when he announced the registration of a political party. He added his phone hack had been confirmed by both Citizen Lab and Amnesty International. The reports show that, in addition to the hacking into the phone, there was an extraction of data. He pointed out that he did not know what data had been extracted, nor the reason why he was put under surveillance.

Ewa Wrzosek, who had already testified to the PEGA Committee during a dedicated hearing, did not present her case again but stressed the political motivations behind the surveillance. She pointed out that none of the known victims had been accused of any crime but were outspoken critics or opponents to the ruling party whose activism /activities were inconvenient to the state. "Law should regulate the use of surveillance tool such as Pegasus" she stressed.

During the **Q&A session**, there was a discussion on the possible legal recourses for the victims of illegal surveillance. The conclusion was that there is currently none given that most democratic institutions have been dismantled.

15:15-16:45 MEETING WITH OMBUDSMAN OFFICE

*Meeting with **Valeri Vachev** (Deputy Commissioner for Human Rights)**; Mirosław Wróblewski** (Director of Constitutional, International and European Law Department)*

The representatives of the Polish Ombudsman Office/Office of the Commissioner for Human Rights recalled that the Commissioner has been taking steps for years to create better supervision over special services. They recalled that the Ombudsman has for many years been involved in activities and initiatives concerning the incompatibility of surveillance laws with the constitutional standard set by the Polish Constitutional Tribunal, international standards set by the European Court for Human Right jurisprudence and standards set by the jurisprudence of the Court of Justice of the European Union.

The problems repeatedly signalled by the Ombudsman in relation to the activities of the special services relate primarily to the lack of effective control over their activities, underlining the illusory nature of judicial control over the activities of the services.

They also pointed out that Polish law does not provide for a person to be informed that he or she has been under surveillance - even when the surveillance has already ended and the person has not been charged. In turn, the judicial control over surveillance is illusory. As a result, citizens have no way to protect their rights.

The need for changes as to the rules of surveillance was pointed out by the Constitutional Court in July 2014. The inadequacies were also highlighted by the Venice Commission in June 2016.

However, these rulings have not been followed up on and various legislative changes adopted in 2016 (amendment to the Police Act, law on Anti-Terrorist Activities, amendment to the Code

of Criminal Procedure) have exacerbated the deficit in the protection of citizens' rights.

They recalled that when the Pegasus scandal became public, the former Ombudsman invited a group of experts to work on a report/proposal ("How to saddle Pegasus") to develop comprehensive regulations for supervising the secret services and all the abuses they might perpetrate that result in violations of the right to privacy. The document proposes two key elements:

- the creation of an independent body to oversee the special services 'activities;
- to grant the individuals the right to be informed that they have been put under surveillance and the right to access their personal data processed in the context of such surveillance.

The speakers indicated that the Ombudsman's Office (both under the former and the current Ombudsman) regularly uses its mandate to participate in legal proceedings, courts cases and hearings in Poland as well as in the Court of Justice of the European Union and the European Court of Human Rights. They also indicated that the issue of infringement of the right to privacy and legal secrecy would be discussed in a case lodged by two alleged Pegasus victims before the European Court for Human Right in the upcoming days with the participation of representatives of the Ombudsman's Office.

17:00 - 18:30 **MEETING WITH JUDGES ON THE JUDICIAL OVERSIGHT OF THE USE OF PEGASUS AND SIMILAR SPYWARE BY STATE AUTHORITIES**

*Meeting with **Piotr Gąciarek** (association of Polish Judges Iustitia); **Dariusz Mazur** (association of Judges Themis); **Katarzyna Kwiatkowska** (Lex Super Omnia Association of Prosecutors)*

The speakers started by expressing great concerns about **the independence of the judiciary in Poland**. They pointed out that the independence of the judiciary in Poland has been systematically dismantled since the 'Law and Justice' party won the elections in 2015.

Previously independent bodies, such as the Constitutional Tribunal and the National Council of the Judiciary have been brought under firm political control, so did the secret services and the Prosecutor's office.

The process of appointing judges has been changed so that the political authorities can nominate "their" judges without scrutiny, especially to the Polish Supreme Court.

As regards the Prosecutor's office, political control was taken by the ruling party through the combination of the functions of the Minister of Justice and Prosecutor General, together with a significant increase of his investigative powers.

These changes have resulted in a Public Prosecutor's Office that is fully subordinate to the ruling party and now empowered to initiate unjustified criminal proceedings against persons who criticise the ruling coalition and to drop proceedings against persons linked to the ruling camp.

At the same time, all specialised central services and investigative bodies, such as the Central Anti-Corruption Bureau, the Internal Security Agency, the Central Bureau of Investigation and

Military Counterintelligence service have been staffed with people closely related to the coalition of the government camp. Moreover, the appointment of Mariusz Kaminski as Minister-coordinator of secret services (after he was sentenced to 3 years' imprisonment for abuses in the use of operational techniques when he was the head of the CBA and then granted presidential pardon) was also pointed out as an illustration of the arbitrary control taken over secret services by individuals closely associated with the ruling camp.

The speakers also pointed out that the headquarters of all secret services being located in Warsaw, the Warsaw criminal courts are territorially competent to deal with applications for operational techniques. In this context, the accelerated process of replacing experienced judges with poorly qualified so called "neo-judges" is of great concern. It is very likely that the replacement of independent judges in these courts by judges who have reasons to be loyal to the current Minister of Justice, to whom they owe a fast and often undeserved career, is aimed at political control of court decisions, including in cases related to operational control.

On the legality of the Pegasus spyware, they stressed that in the current situation (i.e.: political control over the Prosecutor's Office and secret services and limitation of judicial control over operational techniques), the use of any operational techniques in Poland may raise doubts as to compliance with standards on the protection of civil rights and freedoms. All the more the use of a tool such as Pegasus, which allows not only the interception of telephone and Internet connections, but also the review of the entire content of the memory of the controlled device (even in the distant past, i.e. before the operational control was ordered), as well as the tapping or recording of the images, not to mention the possibility of interfering with the content of the recorded material.

They underlined that, in essence, Pegasus is not so much a surveillance system as an espionage system, which makes its use impossible under the current Polish legislation (such as the Code of Criminal Procedure or the Police Act).

With regard to legal consent to the use of operational techniques, the speakers pointed out that the automatic random case allocation system is not used. It is therefore possible that politically sensitive cases are assigned to judges who guarantee their loyalty to the ruling party. In addition, the court's decision to approve operational control must specify the purpose of the control (control of the content of correspondence, telephone conversations etc.), indicate the type of technical measure to be applied and the period of application.

In practice, the supervision of operational control by prosecutors and courts is in practice limited to a formal and legal assessment of applications for consent to control, rather than a thorough control based on the analysis of the files of specific cases submitted for approval. Polish courts are not even informed when operational control will be carried out using the "Pegasus" system. Speakers pointed out that there is in reality no effective control and supervision over how this software is used which is contradictory with the 2016 Venice Commission’s opinion, which pointed to the need to ensure institutional and procedural control over surveillance activities.

Speakers also underlined that the general problems related to surveillance overlap with the problems arising from the crisis of the rule of law in Poland.

Legislative changes adopted in 2016 deepened the deficit in the protection of civil rights:

- the amendment to the Police Act allowed the special services to monitor internet data in an almost unlimited way;
- the law on anti-terrorist activities granted the services a number of additional powers, but also essentially excluded foreigners from constitutional protection as regards possible surveillance;
- the amendment to the Code of Criminal Procedure granted the possibility of using the so-called "Fruit of the poisoned tree", i.e. evidence obtained illegally in criminal proceedings (e.g. as a result of illegal wiretaps, searches, provocations, but also the use of torture, inhuman and degrading treatment if it did not lead to damage to health). This type of procedural principle opens the door to various types of abuses by police officers, prosecutors and secret service officers since breaking the law allows for later trial use of evidence. The materials obtained as a result of covert operational control may be used not only for the prosecution of serious crimes, described precisely in the law, but also for the prosecution of each crime.

In their opinion, Polish law should first be amended so as to, on the one hand, ensure the protection of the citizens' rights to privacy, freedom and confidentiality of correspondence and, on the other hand, meet international standards regarding the observance of civil rights in the context of the secret services operations. The starting point for the debate on the observance of civil rights in the activities of secret services should be, in particular, the opinion of the Venice Commission of 2016 on the Police Act and other legal acts, which made a comprehensive assessment of Polish legislation and formulated recommendations to the Polish authorities.

Speakers finally stressed that an independent authority for the oversight of secret services should be created, which would enjoy the attributes of independence and impartiality.

The control body should:
- be independent of the organs of executive power;
- cover all services authorised to perform operational activities and all areas of their activities;
- have the possibilities and instruments for controlling the financial activities of the services;
- have powers to analyse specific operational cases;
- cover control over all persons, irrespective of nationality;
- cover activities performed in the country and abroad;
- give citizens the right to submit individual complaints regarding the functioning, action or omission of services, in particular cases of violation of the rule of law;
- assess the compliance of services with the Constitution and other legal provisions.

During the **Q&A session**, there was a discussion on the deterioration of the independence of the Polish judicial system. It was stressed that Poland does not obey the verdicts of the European courts, appoints "new" judges that do not meet European standards, and in addition intimidates its judges implementing European standards. It was concluded that the prospects for the independence of courts are rather poor.

III. MEETINGS ON WEDNESDAY 21 SEPTEMBER

08:00 - 9:30 **MEETING WITH EXPERTS ON SECURITY SERVICES**

*Meeting with **Piotr Niemczyk** (former director in Office of State Protection)**; Mr Jacek Mąka** (former colonel and former deputy Chief of Counterintelligence Service)*

Security expert Piotr Niemczyk stated he had no doubt that the Polish services had acquired Pegasus as it was a known fact that they had been using similar tools in the past. He recalled that, already in 2014, a Citizen Lab report revealed evidence that Hacking Team's RCS (Remote Control System) used in the so-called "Galileo" spyware was being used by the Polish government/law enforcement authorities. RCS was able to infect most operating systems (Windows, Android, OSX, iOS...), whether on a computer or a mobile phone. It could record Skype conversations, steal emails, SMS or even encryption keys used to exchange confidential information.

He explained that Pegasus features several new functionalities. IT specialists search for vulnerabilities in the software of newly created telecommunications devices - smartphone, tablet, laptop, computer - in order to take over the device in an imperceptible way. Zero-day vulnerabilities (vulnerabilities that the hardware manufacturer itself does not know about) are used to get full access to, for example, a specific smartphone, without a trace, and without the need for any activity from its owner (clicking, for example, on a suspicious link, opening the uploaded photo, etc.).

In addition, Pegasus has numerous additional functions: recording, saving calls and SMS, the ability to reach the phone's memory, search and respond to keywords. Entering the device's software also allows to bypass the encryption systems of messages during their transmission, e.g. via Signal, WhatsApp, Telegram. Pegasus "sees" this content before it is encrypted. It therefore works in real time and can collect all the data from such a device, save it and store it "for some time, for later, forever".

The detailed specifications of other surveillance and interception systems of this type are not known but this non-invasive, traceless ability of Pegasus clearly distinguishes it from similar solutions of the previous generation. As regards the current generation, there are similar surveillance systems on the black market but Pegasus is currently the more advanced.

He stated that the potential of these types of surveillance tools, experienced by Polish services through the use of Galileo, had probably motivated the government to gradually amend laws as regards operational surveillance and wiretapping so as to enable police and security services to lawfully use this kind of tools.

According to him, the suspension of the Pegasus license for Poland does not mean that Polish services will not continue to use similar tools. In fact, he pointed out that services were clearly abusing the use of surveillance tools, even to prevent the organisation and holding of peaceful demonstrations. He mentioned there were strong presumptions that Polish services were already using the almost identical Predator surveillance system produced by Cytrox.

He concluded saying that there is a real need to implement limits to avoid abuse and unlawful use of surveillance tools, including through the setting up of an independent oversight body as

recommended by the report “how to saddle Pegasus”.

Mr Jacek Mąka, former deputy Chief of Counterintelligence Service, pointed out that the use of Pegasus was made possible by the progressive dismantling of the Polish legal system, which previously prevented the abuse and illegal use of surveillance tools.

He recalled the changes introduced to the legal system in 2016 when a new method of operational control was introduced into all laws on wiretapping services, consisting in the possibility of 'obtaining and recording data contained in computer data carriers, telecommunication terminal devices, information and data communication systems'.

This new provision granted service previously unused possibilities. Among other things, it enabled them to gain access to data contained in phones, tablets, computers, memory sticks, memory cards and even smart TV sets.

Was the purpose of this amendment to provide services with access to data contained, for example, in encrypted messengers such as WhatsApp, Signal, Telegram, etc.? If so, and the Pegasus system in particular was to be used for the technical implementation of this intention, it was an irrational and dangerous measure he stated.

Through the legal amendments introduced in 2016, significant changes were introduced whose effects were manifold, including:

- the services have gained access to internet data via a fixed connection (no requests to operators needed);
- the collection of data does not have to be linked to any pending proceedings;
- the data can be collected not only when it is actually necessary;
- services can collect data on various aspects of a citizen's private life, lifestyle, views, likes or inclinations;
- there is no real control over the collection of citizens' data. The district court does have the right to control, but only on the basis of the services' biannual summary reports
- the invigilated person knows nothing about the services' interest in him or her unless the case goes to court. What happens to this data is unknown;
- it is now possible to use wiretap data in the scope of any criminal or fiscal offence regardless of the legal compliance of the application for wiretapping. As a result, under the current regulations, law enforcement authorities may, in connection with eavesdropping, e.g. in a corruption case, in the absence of evidence indicating corruption of the eavesdropped person, charge him/her with bicycle theft if evidence of such a crime is obtained during the eavesdropping;
- previously, the services and the public prosecutor could address the relevant application to the court no later than one month from the date of receipt of the materials collected in the course of eavesdropping. Currently, the prosecutor decides on the use of this evidence in criminal proceedings without any time limitation.

These amendments resulted in the total disappearance of any system of checks and balances with regards to the use of surveillance tools. He pointed out that, based on the opinions of experts in the fields of technology, IT and telecommunications, Pegasus is not a classic eavesdropping system. Its features go way beyond the operational control known to the Polish law.

He concluded by saying that his long professional experience in combating crime had showed him how important it is for the services and other relevant bodies to be able to effectively care for the security of both state and citizens. However, the performance of this duty can only take place within the framework and limits of the law. The ambiguities and doubts in connection with the use of the Pegasus system by the Polish services underline the need to redefine the role of the security and secret services and the scope of their powers.

9:45 - 11:15 **MEETING WITH POLISH EXPERTS: AUTHORS OF THE STUDY "HOW TO SADDLE PEGASUS":**

*Meeting with **Jacek Cichocki** (former Special Services Coordinator)**; Adam Rapacki** (retired Police General)**; Wojciech Klicki** (the Panoptykon Foundation)*

The authors explained that, thanks to the Ombudsman's initiative, they were given the opportunity to sit for several months with representatives of various professional groups and environments in order to prepare a proposal for comprehensive regulations for supervising the secret services. The cooperation between experts from operational security services with lawyers, judges and activists enabled the group to come up with realistic recommendations.

They stressed that the starting point was not to question the possibility of various forms of surveillance by the secret services nor to limit their effectiveness but to find a right balance between the protection of civil rights and freedoms and counteracting threats to state security and public order.

They underlined in this regard that the threats to state security and public order that can justify measures of surveillance are related to terrorist activities, foreign services and criminal activities. Indeed, the use of tools such as Pegasus should be regulated in a transparent way and limited to anti-terrorism and high criminality. However, none of the known victims were criminal offenders.

The authors noted that, unlike other democratic countries, Poland had never completed the process of building modern special services. The missing element is oversight and independent supervision.

They presented **their main recommendations**:

- the establishment of a special independent body to supervise the activities of the special services and to deal with individual complaints about the service operations;
- granting the individuals the right to be informed of the surveillance by the special services and the right to access the personal data they process.

On the system of authorisations for operational surveillance/wiretapping, they also stressed that the current system was pure fiction. They stated an independent prosecutor office/court should be given full independent power to vet and scrutinise surveillance requests with the necessary time and capacity to take informed decisions.

During the **Q&A session**, there was a discussion on the difficulty of envisaging, under the current conditions, the establishment of an oversight body that would really enjoy the independence necessary to carry out its mission.

11:30 - 13:00 **MEETING WITH CIVIL SOCIETY/HUMAN RIGHTS DEFENDERS/JOURNALISTS**

*Meeting with **Ewa Siedlecka** (journalist at Polityka); **Marcin Wolny** (Helsinki Foundation for Human Rights); **Sylwia Czubkowska** (Spidersweb)*

Marcin Wolny pointed out that, in his opinion, "the Pegasus scandal in Poland is only the tip of the iceberg". This scandal alone illustrates a number of observations denounced by the Helsinki Foundation in the course of its work monitoring the human rights dimension of actions taken by Polish public authorities, amongst others:

- the gradual disappearance of any system of checks and balances
- the total lack of oversight over the secret services activities and their extended powers
- the political and legal culture illustrated by the presidential pardon granted to Mariusz Kaminski followed by his appointment as Minister-coordinator of secret services
- the lack of clarity in the Courts' consents regarding operational surveillance and the almost unlimited range of offences justifying operational control

Ewa Siedlecka worked 27 years for Gazeta Wyborcza before joining Polityka. For over twenty years, she has been taking up the subject of human rights, minorities, exclusion and surveillance in her texts.

She explained that when information began to surface about the eavesdropping and collection of journalists' phone records, she felt that her preferred subjects made her a probable target for surveillance.
Worried whether the identity of her journalistic sources was under threat, she tried to find out if she had been subjected to surveillance. She asked her telecoms operator whether they shared information about her. And also asked the police, CBA and the internal security agency what they had collected on her. It was an arduous process, requiring for instance formal confirmation that her business phone was in fact a business phone. The services rejected her requests, claiming that there were no legal basis for providing such information. The GIODO (the predecessor of the current Office for the Protection of Personal Data) answered the same. She challenged these decisions in Warsaw court but she lost.

All that remained was the civil route, she therefore filed a civil lawsuit in 2020 against the CBA, the internal security agency and the police for violation of her personal rights - her right to practise her profession as a journalist without fear that the data of her interviewees will end up in the hands of the services.

She concluded explaining that she asked the court to refer the question to the European Court of Human Rights with the support of the Ombudsman, the Helsinki Foundation for Human Rights and Panoptykon. A hearing of her case combined with another one (Pietrzak v. Poland) will be held end of September. She also addressed a preliminary question to the Court of Justice of the European Union on whether Polish legislation, which provides neither an obligation to inform about surveillance, nor the right to find out whether someone has been subjected to surveillance, is compatible with EU law

Sylwia Czubkowska explained she had no reason to believe she has been monitored. She however pointed out that the steady increase of surveillance due to the broadened secret

service's capabilities, the almost unlimited range of offences justifying operational control and the use of more sophisticated surveillance methods, such as Pegasus spyware, was putting a pressure on every journalists, especially as regards the protection of journalistic sources.

Press Conference

The PEGA mission was concluded with a press conference by the PEGA Chair, Jeroen LENAERS, and by Sophia in 'T VELD, rapporteur. The link to the press conference is here below.

https://multimedia.europarl.europa.eu/en/webstreaming/press-conference-by-jeroen-lenaers-head-of-delegation-and-pega-chair-and-by-sophia-in-t-veld-rapport_20220921-1300-SPECIAL-PRESSER

Conclusion

The fact-finding mission allowed the PEGA Committee Members to take stock of the situation in Poland and to discuss reports of illicit surveillance through a series of fruitful meetings.

The PEGA Delegation had the opportunity to engage with several relevant Polish stakeholders, including Members of the Sejm and the Senate, representatives of the Polish Supreme Audit Office, experts, judges, prosecutor, journalists, civil society representatives and persons targeted by Pegasus spyware.

None of the competent Ministers wished to participate in the meetings with the PEGA Committee, although they were invited to do so.