GREEN
EUROPEAN
JOURNAL

The End of Privacy?

Article by Bartlomiej Kozek, Wojciech Klicki
June 21, 2022

In Poland, as in other countries, the Pegasus case exposed wiretapping carried out by the government against targeted individuals through the use of spying software. The revelations highlighted the unethical and disproportionate practices within the country's secret service. Wojciech Klicki of the Panoptykon Foundation argues that there is an urgent need for greater social control over the ways in which such services operate. Steps taken at the European level may bring us closer to this reality.

Bartlomiej Kozek: Can you explain what Pegasus is and why it is such a controversial tool?

Wojciech Klicki: Pegasus is a software and service sold by an Israeli company – NSO Group. It allows the user to completely takeover the mobile phones of targeted individuals. National intelligence agencies buy this tool and train their agents in its usage. They can then attack a designated phone in several ways. Sometimes the user must click on a link, sometimes no action is even required. After such an attack, our smartphone becomes a spying tool which we actively carry everywhere with us.

The phone can now be used in three ways. The first is typical wiretapping, allowing others to listen in to our conversations. The second use allows access to all of the data registered on our phone, such as photos or messages – including encrypted information such as Signal messages or bank account activity. Lastly, and most shockingly, there is the possibility of modifying data. Pegasus allows the representative of an agency to delete data from our phone, but also to put compromising materials in its memory. It is the surveillance equivalent of a nuclear bomb.

The temptation to use such a powerful tool was too strong for many countries: Catalan activists as well as journalists and politicians in Hungary were under surveillance in this way. Didier Reynders, the European Commissioner for Justice, was also attacked by Pegasus. Traces of the software were also found on the phones of at least 5 French cabinet ministers last year. This shows that the latest surveillance technologies are quickly becoming a pan-European problem.

What is the Polish context of the Pegasus scandal? What parts of the affair do

you consider most concerning?

In November 2021, Prosecutor Ewa Wrzosek received news from Apple that her phone was an object of interest to the Polish intelligence services. Not long afterwards, researchers from the Canadian CitizenLab confirmed that it was attacked by Pegasus software. Wrzosek was known for her political independence at the time of a governmental reform of the judiciary.

From that moment on the case gathered pace as several other attacks were confirmed. Among those affected was Krzysztof Brejza – a senator from the main opposition party, Civic Platform (PO). He was under surveillance while leading the campaign team of the Civic Coalition, of which PO was a member, ahead of the 2019 parliamentary elections. Another hacking victim was Michał Kołodziejczak, leader of a newly established political initiative, Argo-Unia, that is seen as potentially taking rural voters away from the ruling Law and Justice (PiS) party.

All of this was possibly because of a lack of strong social and political control over the intelligence services in Poland. Even if they – in accordance with the law – requested permission for wiretapping in the courts (which remains uncertain) the judges did not know that they were using Pegasus, which was not permitted under Polish law.

We are not talking about suspected terrorists, but people and politicians who are a thorn in the side of the government. The Pegasus case clearly shows that surveillance is out of control. It is not only the right to privacy that is at stake, but also the rules of free and equal elections. At the height of the electoral campaign – an important politician from the opposition bloc was under observation by the politicians of the ruling party via his phone! You don’t need to have tonnes of sympathy for a particular party to see that this is an unhealthy situation.

Do you think that surveillance levels have spiked since PiS came to power in 2015? Or is this a steady trend that had already begun under the previous PO and PSL (Polish People’s Party) government between 2007 and 2015, as many PiS politicians claim?

The message of our organisation, Panoptykon, has remained the same regardless of who is leading the government: Poland lacks serious civilian oversight over its intelligence services. That was the case both before and after 2015. In the 1990s, we worked to decommunise the security apparatus, but we forgot to take the next step and create institutions of independent, apolitical oversight over them. As time goes on, this misstep leads to more and more negative outcomes, for example as technological progress provides intelligence services with increasingly efficient surveillance tools.

In recent years we have seen the broadening of privileges of the Polish intelligence services. Legislative changes passed after 2015 gave them more opportunities and incentives to gather evidence of crimes at all costs – even if that meant breaking the law. Such changes were made with no regard for the rights to safety and security, nor the right to privacy. Such a situation has led to the wiretapping of around 10,000 people a year in Poland. Only a fraction of these cases results in gathering material useful for criminal proceedings, the rest end without any meaningful results.

Poland lacks serious civilian oversight over its intelligence services.

Can such a level of surveillance ever be justified?

In my opinion? No, no matter the character of the case in which Pegasus is being used. And this is not just my opinion – Amnesty International called for a moratorium on Pegasus, arguing that the Polish law was not suited to control the scale of its usage. Such use should be permitted only after a reform of the Polish intelligence services.

Is there a connection between the Pegasus case and the rule of law infringements the current government is accused of?

Up to this point, we largely connected discussions regarding rule of law with reforms of the judiciary. We now see there is a much broader context. Wiretapping the head of the opposition's campaign staff not only means breaking the law, it is also a threat to democracy, freedom, and equality before the law. That would be the case even if the courts worked perfectly and independently.

What steps were taken after the Pegasus case broke in Poland – and what next steps should we expect? There is talk of creating a select committee in the lower chamber of the Polish Parliament (Sejm).

We should briefly explain the Polish parliamentary system, which is a bicameral one. The upper chamber (Senate) is less crucial in crafting legislation but is currently in the hands of the opposition. A special committee has been created there with the purpose of determining the scale and scope of the surveillance. It collects the testimonies of those who were under surveillance and seeks to establish whether there are connections between the wiretapping of senator Brejza and the election results. In my view, this seems far-fetched, as it is difficult to prove a direct connection between intelligence gathered from the opposition coalition's campaign leader and PiS activities. The situation is further complicated by the fact that only people connected to the opposition, as well as some not connected with the government, have accepted the invitation to stand before this committee. Government officials and those leading the intelligence services declined to take part.

The committee set itself a goal of creating draft legislation that would put in place some independent control mechanisms over the intelligence services, as well as requiring that those subject to wiretapping receive relevant information on the matter. Although the chance of passing such laws is currently slim, they will be ready for a potential change of government. This is important in case the new ruling majority were reluctant to implement changes that would not be in their interests. In the Sejm, we are currently in a deadlock due to a lack of a stable majority. Each vote hangs in the balance and is dependent on a small set of MPs, including members of the Kukiz'15 parliamentary grouping led by a musician, Paweł Kukiz.

Right now, the Senate's committee work has slowed down due to the war in Ukraine. The war itself creates a difficult context: talking about limiting the prerogatives of intelligence

services at such a time may seem at odds with the Polish national interest. I think the opposite is true. Intelligence services activities up to this point have led to a decline in trust within society, non-governmental organisations, and their foreign partners. Restoring the necessary levels of oversight would contribute to regaining this trust – something that is necessary for coordinated work on national security in which the society needs to be involved as well.

Wiretapping the head of the opposition's campaign staff not only means breaking the law, it is also a threat to democracy, freedom, and equality before the law.

This case has an important European dimension. Should EU institutions focus more on the Polish case specifically, or on the wider angle of democratic oversight over intelligence services in all member states?

The European Union has a lot of work to do here. A special committee has been launched in the European Parliament. Its work should lead to crafting minimum joint standards for the intelligence services of all member states.

Security issues have long been the sole competence of member states. Things started to change due to the Lisbon Treaty and the jurisprudence of the Court of Justice of the EU. At the European level, there are rules limiting the exports of dual-use technologies, such as those with potential spy applications. It is time to ask whether we should also regulate imports more tightly.

The EU has no magic wand that will solve Polish problems with uncontrolled surveillance, but the European level influences the Polish one. Pressure on the authorities should come from several directions, including the EU – as the steps taken there increase the awareness of the need for change, not only among the public, but of decision-makers as well.

Do you think levels of surveillance changed during the Covid-19 pandemic? Do events such as the war in Ukraine or cybersecurity threats influence surveillance levels? How should we proceed without compromising our democratic values?

When the pandemic started there was quite a strong anxiety that it would lead to more surveillance of individual members of society and that greater control being exerted on our bodies and our health. Initially, technologies were used mainly in such a manner, for example in the form of contact tracing apps. But this turned out to be much more complicated to enforce in practice, so with hindsight I do not think the pandemic has led to as many problems as first feared.

When talking about the war in Ukraine, we need to bear in mind that just last year it was the 20th anniversary of the attack on the World Trade Centre. We can see how such events generate acceptance of spikes in surveillance levels, as was documented by Edward Snowden. It is too early to say what will be the outcomes of current events and if we will fall into the "let's give up some freedom for more security" narrative.

We can observe some first steps in that direction in Poland. With the recently passed Law on the Defence of the Fatherland, the army was granted access to all public databases, such as those gathered by hospitals or the Social Insurance Institution (ZUS). Such regulations were passed in the name of national unity. The problem is that these tools, often seen as temporary, have a tendency to become permanent.

How then can we strike a balance between the right to privacy and the efficient work of intelligence services? It seems particularly relevant in a context in which we need strong regulations that protects us both from corporate misuse of our data as well as from abuses carried out by public authorities.

Sometimes, when we search for such a balance, we fall into a trap of single-choice thinking, in which intelligence services are either weak or strong. We need to keep in mind other points of reference, such as levels of oversight. Today in Poland we are in a situation in which we have strong secret services and weak oversight. “Privacy versus security” is a false dichotomy – we need to distinguish these concepts.

What tools does the European Union have to respond to such challenges – and what tools does it lack? Will the Digital Services Act boost its capacity to act in this area?

The EU continues to fall into the trap of further restrictions on the right to privacy under the guise of the need to protect other values; recently the European Commission proposed a regulation that filters all messages (e-mails, chats, etc.) with the aim of protecting children from sexual abuse. In practice, this could mean the end of encrypted communication such as Signal or Whatsapp. The EU Court of Justice’s ruling have cooled these aspirations however, ruling provisions that allow excessive surveillance as invalid.

In the context of surveillance by digital corporations, the EU noticed the threats stemming from the fact that data collected from its citizens empowers those who have it. There is now a fight over control of this power, in which both corporations and intelligence services are involved. We already have proof that digital platforms know they have such power and know how to use it. The recent Facebook Files leak, that lead to a hearing in the European Parliament, showcased the scale of the influence platforms have over public opinion.

While the problem has been noticed, the solutions remain a point of contention. The work on the Digital Services Act (DSA) has just finished. It does not directly address the issue of mass data collection by the state. Unfortunately, the provisions that could have been relevant in this area (for example, the prohibition on states obliging intermediaries to retain data or use online behaviour monitoring tools, prohibition to obstruct encryption, and the prohibition to impose restrictions on anonymity) were removed from the DSA draft in the trilogue stage.

The DSA mainly addresses the problem of corporate surveillance. The strongest regulations are those that respond to the problem of tracking in advertising and recommendation systems. Their shape is far from ideal, but in practice a lot depends on how these solutions will be implemented by companies and on the determination of the supervisory authorities to oversee them. It is no secret that the corridors of Brussels are filled with representatives of GAFA (Google, Amazon, Facebook, Apple) who have easier access to decision-makers

than typical citizens and their organisations. We need to be aware of the situation in order to fight more effectively for our right to privacy, for the right to control our data – and, in the end, for our freedom to make our own conscious de

---

Bartlomiej Kozek is a journalist of Zielone Wiadomości (Green News), a Polish bi-montly magazine and web portal presenting current affair commentary from a green point of view. He has been a secretary general of the Polish Green Party – Zieloni 2004 and one of the authors of the party's policy on social issues.

Wojciech Klicki has been working with Panoptykon since January 2012 and is currently the head and heart of the legal team. Before coming to Panoptykon he worked with the Helsinki Foundation for Human Rights. He is responsible for the monitoring of legislative works in the Polish parliament and the preparation of legal analyses. He engages in advocacy activities, talks with political decision-makers and the media. Wojciech's main interest is surveillance exercised by the police and intelligence services.

Published June 21, 2022
Article in English
Published in the *Green European Journal*