Case number: NAIH-423-2/2022.
Antecedent: NAIH-6583/2021.

Findings of the investigation of the Nemzeti Adatvédelmi és Információszabadság Hatóság (Hungarian National Authority for Data Protection and Freedom of Information) launched ex officio concerning the application of the "Pegasus" spyware in Hungary

(The detailed summary concerning the investigation of the Nemzeti Adatvédelmi és Információszabadság Hatóság constituting the basis of these findings must not be disclosed as it contains classified data with "Top Secret" classification according to Section 7 of Act CLV of 2009 on the Protection of Classified Data.
The classification is valid until: 31.12.2050.)

I. Antecedents:

Based on Section 51/A (1) of Act CXII of 2011 on the Right to Informational Self-Determination and the Freedom of Information (hereinafter: Privacy Act), the Nemzeti Adatvédelmi és Információszabadság Hatóság (hereinafter: Authority) launched an investigation ex officio concerning the application of the "Pegasus" spyware in Hungary on 9 August 2021, in view of the fact that according to the news published by the media, personal data may have been unlawfully processed by using the spyware.

I.1.
The news published in the media

On 19 July 2021, an article by Szabolcs Panyi and András Pethő entitled ***"A tough Israeli spyware was exposed as used to target critics of the Orbán government and Hungarian journalists"***, which included the following:

As part of an international investigative project, Direct36 discovered that "the spyware of an Israeli cyber company called NSO suitable for jailbreaking smart phones, "Pegasus" began to be used against targeted Hungarian persons years ago; investigative journalists and wealthy businessmen owning also media companies and their close milieu were among the persons targeted. In the course of the research, we found a number of indirect proofs indicating that Hungarian state bodies may be behind the secret surveillance.

The international investigation taking place with the participation of altogether 17 editorial boards, including those of The Washington Post, The Guardian, the Süddeutsche Zeitung, the Die Zeit and the Le Monde, was led by the network of investigative journalists called Forbidden Stories, which gained access to a database related to the activities of NSO clients together

with Amnesty International (AI), a human rights organisation. The database included over 50 thousand phone numbers which according to the findings of the investigative project NSO clients selected as targets of observation in over 50 countries of the world from 2016.

The fact that the phone number is included in the database does not necessarily mean that Pegasus was certainly deployed against the targeted persons and their phones were jailbroken, but in many cases the subsequent examination of the phones proved that the devices were truly jailbroken by the NSO spyware.

Pegasus exploits faults of the phones' software remotely to penetrate them unnoticeably, of which not even the developers and manufacturers were aware. Penetrating the phones through these gaps it was possible not only to listen in on the conversations of the targets, but access their most confidential information, such as their e-mails and other messages, photos and videos.

Pegasus is considered to be such a serious cyber weapon that NSO may sell it to other countries only with the permission of the Israeli Ministry of Defence. Officially, it could only be deployed against persons suspected of terrorism and organised crime, but the investigative project revealed that NSO clients used it against journalists, human rights activists, opposition politicians, lawyers and businessmen in at least 10 countries."

"For the time being, the following people were identified of over 300 Hungarian targets:

- *Four journalists, including two members of the Direkt36 staff, Szabolcs Panyi and András Szabó, in whose case the subsequent examination of the phones demonstrated that their devices had been jailbroken using the NSO software. In addition to them, we also identified Dávid Dercsényi, former journalist of Hvg.hu and a fourth journalist, who requested that his name should not be disclosed.*
- *A Hungarian photographer who worked with an American journalist, who wrote about the affairs of the International Investment Bank – a bank under Russian management that was just moving to Budapest.*
- *Zoltán Varga, the owner of Central Médiacsoport (Central Media Group) – who had been the target of attacks from government circles for quite some time – and several other businessmen who participated in a dinner discussing public affairs in Varga's house in 2018. Subsequent investigations confirmed that the phone of at least one guest was hacked using the NSO program. Attila Chikán, professor of economics, a former minister for economic affairs in the first Orbán government, also participated in the meeting hosted by Varga, and his phone number was also among the leaked data.*
- *The son of Lajos Simicska, a former oligarch, and one of his closest confidants. Both became targets prior to the elections in 2018 when Simicska was the owner of an entire media empire and openly attacked the government. (Simicska did not use a smart phone, hence there was no point in targeting him with this software.)*
- *Adrien Beauduin, a foreign student of CEU, , who was arrested by the Hungarian authorities at an anti-government demonstration in 2018.*
- *In addition, several other Hungarian public figures are also among those targeted, including a prominent lawyer and an opposition city leader – their stories will be reported in the coming days.*

The data made available to the international fact-finding team did not clearly reveal who exactly deployed the spyware. However, several circumstances strongly suggest that the Hungarian authorities used the programme against targets in Hungary.

NSO firmly states that they sell the services only to governments and public organisations and information is available on the fact that the spyware appeared in Hungary after high-level meetings between the Israeli and the Hungarian governments in 2017 and 2018.

The former officer of the Hungarian secret service told Direkt36 that according to information he holds the national security agencies began using Pegasus with Hungarian-Israeli relations becoming closer from 2018. A former NSO employee also confirmed to the German Die Zeit, one of the partners of the international investigative team, that Hungary became an NSO client. In addition, a Canadian research group called Citizen Lab also found signs of the use of the spyware in Hungary in the course of an international analysis in 2018.

The Hungarian targets themselves indicated that the Hungarian authorities may be behind the designation of the targets in several cases. Based on the phone numbers, we also identified targets – for instance condemned criminals – who were investigated and prosecuted by the Hungarian authorities based on information accessible to the public. The international fact-finding project arrived at the conclusion in the cases of several other countries as well that the local authorities used the cyberweapon regularly and abused it at the same time.

The team of journalists sent a series of detailed questions to NSO which, however, did not react to the questions related to Hungary. The company disputes whether the phone numbers obtained by Forbidden Stories would really be Pegasus targets. In their view, it is possible that these numbers are parts of a larger list, "which the clients of the NSO Group used for other purposes". According to the company, it is possible that the numbers in the database stem from a so-called HLR database, which is accessible to the public. HLR (Home Location Register) is a system which assists the operation of mobile phone networks by keeping records of the geographical location and other identifiers of the individual devices, thus enabling call and text message forwarding.

However, precisely for this reason, this register may be a useful step for launching the surveillance. Through HLR, NSO clients may check whether the device associated with the phone number of interest to them is truly operational (it is switched on) and where it is located physically (this is important because there are restrictions on the countries in which clients may use Pegasus). A source knowledgeable about the NSO systems told a member of the fact-finding project that the company's clients do use HLR because of this.

The international security staff of Amnesty International checked 67 devices which based on the leaked database could be targets of spyware attacks. Of these they established in 23 cases that the phones were really hacked using Pegasus, in 14 cases they found traces indicative of attempted intrusion. No such results were found in the case of the remaining 30 checks, but in many cases the underlying reason was that the data subjects have already replaced their phones since the time of the alleged surveillance and, because of this, the data were lost. In addition, the phones examined included 15 Android devices which in contrast to iPhones do not store information on the basis of which the Amnesty International staff could unambiguously establish whether the device was hacked. Still, even among Android phones, there were three showing signs of surveillance attempts because text messages were found on them, bearing traces of Pegasus.

Amnesty International also shared the underlying data of its examinations from several devices with the researchers at Citizen Lab, who confirmed that those phones were hacked using Pegasus. Citizen Lab reviewed AI's examination methods and found them to be technically sound.

The Hungarian government also received a series of detailed questions, including all the material statements in this article, and they did not deny any of them, or rather they did not

react to them in merit. All they said was that "they were not aware of the alleged data collection that the questions referred to" and added that Hungary "is a state under the rule of law and as such, action is always taken in accordance with the legal regulations in force in the case of every individual".

[…]

"The NSO Group was founded by a former officer of the Israeli Army, Shalev Hulio, with a business partner during the ascending phase of smart phone penetration. The company developed technologies with which they were able to hack the new types of mobile phones and access the data stored on them and forwarded by them, including information run through encrypted channels.

Although NSO now has foreign investors, the company continues to operate from its headquarters in Israel and it is closely linked to the government of the Jewish state. If, for instance, NSO wishes to sell its services to a foreign country, they can do so only if permitted by the Israeli Ministry of Defence.

NSO claims that this does not mean that the company would be "an instrument of Israeli diplomacy". Yet, there are examples where the appearance of Pegasus in some countries has coincided with a high-level Israeli meeting. This happened in the case of India, where according to leaked data, the selection of targets was speeded up after the visit by Indian Prime Minister Narendra Modi to Israel in July 2017.

Some overlap can be seen also in the case of Hungary between the relationship with Israel becoming closer and the appearance of Pegasus."

[…]

"A former officer of the Hungarian secret service also told Direkt36 that as far as he knew, the Hungarian state began using Pegasus from early 2018" and that "the procurement had a great deal to do with our relations with Israel becoming closer". According to the source requesting anonymity, the Hungarian government has long been troubled by the fact that they could not have access to communications through encrypted applications (such as Signal or WhatsApp) using the traditional means of interception, so they snatched the opportunity of using the NSO product. This is due to the fact that by hacking a smart phone, Pegasus users can see everything that appears on the display of the device, including conversations and messages running through encrypted apps.

Advanced technology commands a high price. According to a Mexican contract made public earlier, the tariff amounted to USD 64,000 (HUF 19 million) per target, while in the case of a contract with Panama, it was USD 89,000 (HUF 27 million). The members of the team of journalists of the Pegasus project spoke with several sources knowledgeable about NSO's internal affairs and according to them, the spyware is presumably cheaper than this today. It is difficult to quote a specific amount because pricing depends on a number of factors (for instance which region the client is in, how many targets it would like to monitor at the same time, or how risky it is to contract the client from the viewpoint of respecting human rights).

Hungarian law does not separately regulate spyware similar to Pegasus. Legal regulations address the so-called secret gathering of information only in general, which includes for instance traditional wire-tapping or putting up mikes in a residence. These rules provide a very broad leeway for the authorities to use various tools, such as Pegasus.

Fundamentally, there are two categories of secret operations for gathering information depending on which authority carries them out. On the one hand, law enforcement authorities (the police, tax inspectors, etc.) may carry out such operations, if they are conducting investigations on the suspicion of a specific criminal act. They may do so only if they obtain permission from a judge and carry out such activities only for a restricted time afterwards. If they cannot obtain sufficient information for bringing an indictment during this period, then in principle they have to eradicate the data. If somebody is indicted, then the data collected secretly must be "brought into the open", that is, they must be included in the official documents of the investigation, which the suspect may also have access to later on.

If the covert collection of information is carried out by the National Security Services, the rules are more elastic. They do not need permission by a judge, approval by the minister of justice will suffice (in some cases, they may begin the secret collection of intelligence even prior to obtaining the authorisation.

The over 300 Hungarian phone numbers obtained by Forbidden Stories and AI only show who the Hungarian clients of NSO selected specifically as targets of surveillance in Hungary. The number of surveillance operations carried out by the Hungarian authorities is much higher.

Recently, 168 Óra reported that the covert operations of information gathering approved by the minister of justice increased substantially over the past five years. Whereas in 2015, 1,038 such authorisations were issued, in recent years the number of cases was at around 1,200-1,300. This means that the minister issued more than three authorisations for monitoring a day on average. Relative to this, close to 500 ministerial authorisations were issued during the first 3.5 months of this year, that is, five approvals were issued every day.

Legal regulations are quite elastic about the cases in which such operations can be carried out by the various services – including, for instance, the Office for the Protection of the Constitution functioning as a civil secret service supervised by Minister of the Interior Sándor Pintér, the Information Office in charge of foreign intelligence under Minister of Foreign Affairs Péter Szijjártó and the Terrorism Prevention Centre headed by János Hajdu, former personal bodyguard of Viktor Orbán. The technical management of the specific monitoring his carried out by a fourth agency, the Specialised National Security Service as a kind of service organisation, which is also supervised by Pintér. A typical example of the broad framework in which the services carry out their work is the description of the responsibilities of the Information Office provided by the law: "it obtains, analyses, assesses and forwards information needed for government decision-making".

Early in July, a journalist of the French Le Monde participating in the investigative project asked Minister of Justice Judit Varga in an interview whether she would authorise the monitoring of a journalist or a member of the opposition; she indignantly answered: "What a question? This is a provocation in itself!" Varga said that only surveillance requests in compliance with legal regulations may be authorised, adding that "there are so many threats to the state all over".

Later Varga also received a detailed set of questions about the Hungarian journalists and media owners selected as targets and specifically subjected to surveillance, but no answer was received."[1]

II. Legal background

[1] https://www.direkt36.hu/leleplezodott-egy-durva-izraeli-kemfegyver-az-orban-kormany-kritikusait-es-magyar-ujsagirokat-is-celba-vettek-vele/

II.1.
Constitutional and international legal framework

Hungary's Fundamental Law sets forth the following requirements concerning the protection of fundamental rights and ensuring their enforcement:

"Article I(1) The enviable and inalienable fundamental rights of man must be respected. It shall be the primary obligation of the state to protect these rights.
(2) Hungary shall recognise the fundamental individual and collective rights of man.
(3) The rules for fundamental rights and obligations shall be laid down in an Act. A fundamental right may only be restricted to allow the effective use of another fundamental right or to protect a constitutional value, to the extent absolutely necessary, proportionate to the objective pursued and with full respect for the central content of the fundamental right." [Hungary's Fundamental Law Article I (1)-(3)]

Pursuant to Article VI(1) of the Fundamental Law, everyone shall have the right to have his or her privacy, family life, home, contacts and reputation respected and according to paragraphs (3)-(4) everyone shall have the right to the protection of his/her personal data, as well as to access and disseminate data of public interest. Paragraph (4) of this Article lays down that the enforcement of the right to the protection of personal data and access to data in the public interest shall be supervised by an independent authority established by a cardinal act.

In terms of international legal obligations, it is necessary to take into account the Convention for the Protection of Human Rights and Fundamental Freedoms (hereinafter the Convention)[2], Article 8 of which states that "*Everyone has the right to respect his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interest of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".*

According to the relevant practice of the Constitutional Court as pointed out also by Constitutional Court Decision 32/2013 (XI.22.) AB, the use of the means and methods of covert information gathering is closely related to the right to privacy, the right to informational self-determination and the right to human dignity.

With regard to the constitutionality of covert information gathering, the justification to Decision 2/2007. (I. 24.) AB of the Constitutional Court provides important guidance: "*In a democratic constitutional state, the circumstance that traditional means do not prove to be sufficient for successfully combating certain criminal acts severely violating or jeopardizing the order of society lays the foundation for making use of covert information gathering and secret collection of data as an instrument of criminal law. To protect society, methods and means are needing, which may allow law enforcement agencies to make up for the eventual disadvantage they have against crime. Hence the restriction of the fundamental rights under study by the methods*

[2] It was promulgated by Act XXXI of 1993 in Hungary.

applied in covert procedures is not a constitutionally unnecessary instrument. The protection of the constitutional state and of the fundamental rights, however, also requires the law to regulate the order of using such instruments in detail and in a differentiated manner. As the use of covert instruments and methods constitutes a severe intervention in the life of an individual, they may be applied only exceptionally as a transitory and ultimate solution."

Decision 32/2013. (XI.22.) AB of the Constitutional Court also takes into account the judicial practice of the European Court of Human Rights call to supervise the implementation of the Convention, on the basis of which it states the following: *"As covert information gathering by necessity excludes the possibility of efficient legal remedy, it is indispensably important that the procedural order enabling its application provide sufficient guarantees to protect the individual's rights. In view of all this, its application has to be subjected to control consisting of three stages: when the intervention is ordered, during the implementation of the intervention and after the completion of the intervention. Control will have to be carried out by bodies independent of the executive power. Primarily, permanent, continuous and compulsory monitoring is a guarantee that proportionality is not breached in specific cases. In its decisions, the Court pointed out the requirements, which the regulation concerning the use of covert instruments must at least comply with. It underlined that precisely because the intervention in fundamental rights is covert and the use of such instrument provides imponderable opportunities to the executive power, it is indispensable that the procedures themselves provide sufficient guarantee for the enforcement of the rights of the individual. This requires that states give priority to the enactment of precise and detailed rules that are easy to follow and accessible to the citizens. The legal regulation must make clear the powers of the authority using such instruments, the essence of the measures and how they are exercised. As part of the requirements of a clear requirement, the Court also pointed out that the laws must cover the cases warranting intervention, the circumstances, as well as the conditions of intervention. As a minimal guarantee they must include the conditions suitable for specifying the range of persons concerned, as well as the provisions for the rules concerning the documentation of the intervention, the safekeeping of the documentation and its annihilation. The authorities may not be given too broad right of consideration in terms of bringing the decision on the intervention. The guarantees of use include furthermore that access to the information must be restricted (for external persons)."*

II.2.
Covert information gathering and the regulation concerning the protection of personal data

In terms of the processing of personal data, Act CXII of 2011 on the Right to Informational Self-Determination and the Freedom of Information (Privacy Act) specifies the legal framework of general data protection for covert information gathering.

From the perspective of the Privacy Act, information may be gathered for the purpose of *law enforcement* (prevention, investigation and interdiction of criminal acts) or for purposes of *national security*. Pursuant to Section 2(3) of the Privacy Act, the substantive and procedural rules of the Privacy Act shall apply in both cases to these data processing operations and their supervision. It is however important to note that whereas data processing for the purposes of

law enforcement is subject to EU law, in the Law Enforcement Directive[3]transposed into Hungarian law by the provisions of the Privacy Act, data processing for national security (and defence) purposes is outside the scope of EU law and it is within the regulatory and administrative competence of the Member States. Both Article 2(2)(a) and Recital (16) of the General Data Protection Regulation[4] (GDPR) and Recital (14) and Article 2(3)(a) of the Law Enforcement Directive are unambiguous concerning the fact that the processing of personal data carried out in the course of activities related to national security are outside the scope of EU law. This means that national security as the subject matter of legislation and the application of the law is exclusively within the scope of authority of the Member States according to EU law.

Pursuant to Section 4 of the Privacy Act, which specifies the principles of data processing, personal data shall be processed only for clearly specified and legitimate purposes in order to exercise certain rights and fulfil obligations. The purpose of processing shall be met in all stages of processing; data shall be collected and processed fairly and lawfully. Only personal data that are essential and suitable for achieving the purpose of processing may be processed. Personal data may be processed only to the extent and for the period of time necessary to achieve its purpose. In addition, based on Section 7 of the Privacy Act, the controller shall design and implement data processing operations so as to ensure the protection of the privacy of data subjects applying the Privacy Act and other rules pertaining to the processing of data. The controller and, within its sphere of activities, the processor shall ensure the security of the data and take the technical and organisational measures and develop the rules of procedure, which are necessary for the enforcement of the Privacy Act and other rules for the protection of data and secrets. Data shall be protected with the appropriate measures, particularly against unauthorized access, changing, forwarding, disclosure, erasure or destruction and accidental annihilation and corruption, and becoming inaccessible as a result of changes in the applied technology.

II.3.
The types and fundamental conditions of covert infromation gathering

Covert information gathering by the National Security Services impact fundamental rights, thus the right to respect privacy and the protection of personal data, hence in accordance with Article I (3) of the Fundamental Law, they are to be regulated at the level of a law. The duties and the principles of operation of the National Security Services, data processing carried out by them and the means and methods that they may use in the course of their covert information gathering activities, as well as the conditions and the order of using tools are specified in Act CXXV of 1995 on the National Security Services (hereinafter: National Security Services Act).

The rules pertaining to the application of the means and methods used in the course of covert information gathering activities are laid down in the sectoral acts of the bodies authorised to carry out such activities – the controllers from the viewpoint of data protection: the National

[3] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and on the free movement of such data and repealing Council Framework Decision 2008/977/JHA
[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation - GDPR)

Security Services Act, Act XXXIV of 1994 on the Police (hereinafter: Police Act), Act XC of 2017 on Criminal Procedures (hereinafter: Criminal Procedures Act), Act CLXIII of 2011 on the Prosecution and Act CXXII of 2010 on the National Tax and Customs Administration.

Covert information gathering may be carried out for the purposes of law enforcement and for purposes other than this. Covert information gathering for the purposes of law enforcement may be carried out in some cases subject to permission by a judge [Police Act Section 70], while in other cases not subject to permission by a judge [Police Act Section 66]. Section 75/B(1) of the Police Act allows covert information gathering subject to permission by a judge for a period of ninety days, which may be extended at most by another ninety days provided that a new request is submitted.

The police may apply concealed means in order to detect and interrupt criminal acts, apprehend and arrest perpetrators, obtain evidence and recover assets derived from criminal acts exclusively in accordance with the provisions of the Criminal Procedures Act. The body established to carry out the general duties of the police and the body performing internal crime prevention and detection may carry out covert information gathering for the purposes set forth in Section 64 exclusively in accordance with the rules laid down in the Police Act. The terrorism prevention body may carry out covert information gathering with a view to the performance of its task related to the prevention of crime as set forth in Section 7/E(1)(a)(aa) and its tasks laid down in Section 7/E(b)(ba) and (c) of the Police Act exclusively in accordance with the rules laid down in the Police Act. With a view to performing its task according to Section 7/E(1)(a)(ad) and (e), the terrorism prevention body may pursue covert information gathering by appropriately applying Sections 53-60 of the National Security Services Act, in the course of which it is authorised to request and process data according to Sections 38-52 of the National Security Services Act. Covert information gathering laid down in Section 56(a)-(e) of the National Security Services Act is authorised by the minister in charge of justice.

For the purposes of preventing criminal acts, covert information gathering may be carried out if there are grounds to suppose that the intervention will lead to obtaining information concerning crime through the analysis and assessment of which endeavours to commit criminal acts may be detected and the prevention of criminal acts may become possible. The terrorism prevention body of the police may pursue covert information gathering for the purpose of performing its tasks according to Section 7/E(1)(b)(ba), if it is expected to lead to the disruption of a criminal act within its scope of authority or the collection of information needed for the arrest of the perpetrator. [Police Act Section 65(1)-(2)]

Covert information gathering pursued for purposes other than law enforcement, i.e., for national security purposes, may also be, by its nature, not subject to external permission [National Security Services Act Sections 54 and 55] and subject to external permission [National Security Services Act 56-60]. In the cases specified by the act, the external permission may be an authorisation granted by a judge or by the minister in charge of justice.

As mentioned by Constitutional Court Decision 32/2013 (XI. 22.) AB already referred to, there are many examples in international practice of states distinguishing between information gathering for law enforcement (and the closely related crime prevention and detection purposes) and for other national security purposes.

With reference to the judicial practice of the European Human Rights Court, the Constitutional Court stipulates the application of *detailed rules that are easy to follow and accessible to the citizens, which will* "*make clear the powers of the authority using such instruments, the essence of the measures and how they are exercised" as a requirement.*

Accordingly, the National Security Services Act designates the National Security Services that may pursue covert information gathering in order to fulfil their tasks, and it lists the duties of the individual national security services and it also contains the detailed rules applicable to covert information gathering. These can be summarised as follows:

Pursuant to National Security Services Act Article 53(2), the National Security Services may use special means and methods of covert information gathering only if the data needed for the fulfilment of the functions defined in this Act cannot be obtained in any other manner. The National Security Service authorised to secretly gather information may carry out covert information gathering independently or in collaboration with another National Security Service or rely on the Specialised National Security Service.

In the latter case, the basis for the procedure of the Specialised National Security Service is that pursuant to Section 8(1)-(2) of the National Security Services Act, the Specialised National Security Service provides services, upon written request, within the limits of the relevant legal regulations, with the special means and methods therein provided, for the bodies authorised for covert information gathering and the use of concealed means under the Criminal Procedures Act to carry out covert information gathering and the use of covert means. The Specialised National Security Service provides the special technical equipment and materials required for for this activity on the basis of the needs of the bodies authorised for covert information gathering and the use concealed means.

Pursuant to the provisions of the National Security Services Act, the National Security Services may, based on external authorisation, search residences, other premises, fenced off places, vehicles other than vehicles of public transport and objects used by the data subject in secret, they may record their observations using technical means, survey and record whatever is happening in the residence or other premises using technical means in secret, secretly open mail or other sealed packages tied to an identifiable person and they may get to know, check and record its content. Based on external authorisation, they may secretly get to know and record the content of communications made in the context of an electronic communications service by means of system carried out using an electronic communications network or device, or an information system.
In addition, the National Security Services may also secretly learn about and record the data processed in the information system using technical devices, or they may place the electronic data needed for this into the information system and install the necessary technical devices in the residence, other premises, fenced off places or vehicles and in the objects used by the person concerned, and they may intervene in the information to counter a threat from cyberspace. [National Security Services Act Section 56(a)-(e).

So, in the regulatory system of the National Security Services Act, the use of means and methods of covert information gathering referred to above is subject to external authorisation because these devices and methods have a direct impact on privacy, family life, respect for home and relationships, as well as the fundamental right to the protection of personal data.

II.4.
Procedure to authorise covert information gathering

Pursuant to Section 57 of the National Security Services Act, the submission for the authorisation of covert information gathering subject to external authorisation authorised may be submitted by the director general of the Information Office, the Office for the Protection of the Constitution, the Military National Security Service and, with regard to specific tasks, the Specialised National Security Service. The submission shall include the place of the covert information gathering, the name(s) or the circle of the person or persons concerned, and the mode and the justification of the need for the covert information gathering , the initial and closing date of the activities specified in days. In the case of the so-called exceptional authorisation, the submission shall include the justification that in the given case it is imperative for the effective operation of the National Security Service.

With regard to the detection of specific criminal acts, covert information gathering is authorised by the judge designated for this task by the president of the Budapest Municipal Court . Other activities specified in Section 56 of the National Security Services Act, performed in the course of general information gathering is authorised by the minister in charge of justice. The authoriser (judge or the minister responsible for justice) brings a decision within 72 hours from submission of the request either authorising it or rejecting authorisation if unfounded. This means that bringing the decision on the external authorisation typically precedes the use of tools; the external authorisation is a precondition to the commencement of cover information gathering. Exceptional authorisation according to Section 59 of the National Security Services Act (see below) is an exception to this, but the continuation of using the tool and the subsequent use of the data is subject to granting the external authorisation also in this case as set forth in Section 60(2) of the National Security Services Act.

The authorisation procedure is launched with the submission of the request for authorisation. The authoriser decides whether the request for the external authorisation is well-grounded, whether the request substantiates the need for covert information gathering, whether it provides a sufficiently accurate description of the means and methods to be used, the place, start and end dates of the intervention and the persons affected by the intervention. The authoriser authorises the covert information gathering for ninety days at most, which may be extended in warranted cases by an additional ninety days based on the supplementary submission of the general directors.

Pursuant to Section 14 of the National Security Services Act, Parliament with the collaboration of the National Security Committee is entitled to exercise control over the authorisation procedure of the minister in charge of justice. The limits to covert information gathering should be specified in every case so as to restrict the right to privacy and the protection of personal data to the minimum extent necessary for the purpose for which the information is collected, in accordance with the requirements of purpose limitation. The requirement of necessity applies not only to whether covert information gathering is necessary or the data indispensable for the discharge of a task can be obtained by other means, but also to when, where, by what means and against whom the covert information gathering is necessary.

By way of derogation from the general rules, the directors general of the National Security Services may authorise the covert gathering of information as listed in Section 56 of the National Security Service Act until the decision of the authoriser (judge or minister in charge of justice) is obtained, if the external authorisation of the covert information gathering would involve a delay which in the given case would obviously violate the interests linked to the successful operation of the National Security Services (the so-called exceptional authorisation). The exceptional authorisation is valid at most until the decision of the authoriser is obtained and the directors general of the National Security Services have to make the submission for the external authorisation simultaneously with granting their authorisation. As a general rule, the director general empowered to order covert information gathering in a given case based on exceptional authorisation may do so only once. Section 60(2) of the National Security Services Act sets forth that in the case of exceptional authorisation the covert information gathering shall be immediately terminated if the authorising judge or minister in charge of justice does not grant the authorisation for the continuation of a covert information gathering. In this case, data obtained during the covert information gathering shall be destroyed immediately in accordance with the legal provisions applicable to the destruction of classified data. In all other cases, the covert information gathering subject to external authorisation shall be immediately termination, if it has achieved its purpose specified in the authorisation, if the continuation of the covert information gathering is not expected to be successful, if the period open for this expired without extension, or if the covert information gathering violates the law for any reason whatsoever.

II.5.
Implementation of the covert information gathering

If the implementation of the covert information gathering is carried out within the framework of the services of the Specialised National Security Service, the agency ordering the implementation shall be responsible for obtaining the authorisation needed for carrying out the covert information gathering. This means that the ordering agency is responsible for the lawfulness of the intervention, while the Specialised National Security Service is responsible for its implementation. Pursuant to Section 11(1)(h) of the National Security Services Act, the internal procedural and authorisation rules of covert information gathering are approved by the minister overseeing the individual national security services upon the submission of the directors general. As the Specialised National Security Service provides services according to Section 8(1) of the National Security Services Act, it has to delete all data from its records obtained in the course of covert information gathering, following the forwarding of the data to the agency ordering them.

The Specialised National Security Service keeps records in relation to its tasks as service provider, which contains the written request of the ordering agency together with the necessary authorisation, the personal data needed to identify the person indicated in the request, a description of the means and methods used in the course of the covert information gathering, as well as information having operational value that do not qualify as personal data, technical data, as well as a list of the data media forwarded to the ordering agency. The Specialised National Security Service may not store any personal data other than this in relation to discharging its tasks as service provider.

The body authorised to conduct covert information gathering, not subject to the National Security Services Act, may use the tool of secret surveillance of an information system exclusively by relying on the services provided by the Specialised National Security Service [National Security Services Act Section 62/A].

This is explained in detail by the ministerial justification of the National Security Services Act: "*The Specialised National Security Service shall have exclusive responsibility for covert information gathering and the segment of using disguised tools subject to external authorisation where it is necessary to build up systems that are unique and complex from a technical point of view and hence require substantial expenditure or special expertise and experience, or human resources with special expertise. It is warranted to refer the implementation of the secret surveillance of information systems to the exclusive responsibility of the Specialised National Security Service because similarly to wiretapping, the use of this instrument also requires technical systems with substantial expenditure and human resources with special expertise. The concentration of these capabilities within the Specialised National Security Service ensures the efficient and economical use of budgetary funds, and unwarranted parallel capacities may not be set up as a result of centralisation. With regard to the secret surveillance of information system, there is no similar act or sectoral regulation at the level of a government decree, such as in the case of the secret opening of mail, or wiretapping, so the relevant provision may only be included in the National Security Services Act, which as a special rule lays down that in the case of the secret surveillance of an information system, such an intervention may be carried out exclusively through the Specialised National Security Service.*"

Based on the legal regulations currently in force, nine organisations may gather information in secret, or are authorised to use disguised tools in Hungary. The responsibilities of the Specialised National Security Service specified by law include supporting the work of organisations authorised to use the means and methods of covert information gathering and the use of disguised tools by way of providing special services.

The government determines the order of cooperation between the organisations authorised to gather information in secret and the Specialised National Security Service by decree. The Specialised National Security Service also uses software qualified as a secret service tool listed in Chapter XXVI of Annex 1 to Government Decree 156/2017 (VI. 16) on the detailed rules of the authorisation of military technical activities and the certification of business undertakings that are capable of covertly obtaining, forwarding and recording stored information from computers storing and/or processing data, IT or other tools and the data media used with them, and of the real time covert surveillance and recording of the activities carried out on IT devices and obtaining the communication carried out on electronic communications networks. Such tools and software are capable of controlling IT devices, as well as controlling communications carried out through electronic communications networks (and the network substituting for it).

II.6.
Supervision of the lawfulness of covert information gathering

The National Security Committee of Parliament is called to supervise the lawfulness of the operation of the National Security Services. The National Security Services Act lays down the

rules of the supervision of the services by Parliament. Accordingly, within the framework of its supervisory activity, the National Security Committee may request information from the minister and from the directors general of the services about their operation, it may request information from the competent ministers and the directors general about the authorisation procedure related to covert information gathering subject to external authorisation, it may investigate the complaints indicative of unlawful activities by the National Security Services and call upon the minister to conduct investigations, if it supposes any unlawful activity of a service. If the committee detects unlawful operation on the part of a National Security Service, it may conduct a fact-finding investigation, in the course of which it may inspect the documents concerning the given case held by the services, hear the staff members of the services and call upon the minister to take the necessary measures [National Security Services Act Sections 14-16].

As the Constitutional Court explained in its Decision 23/2013 (XI.22) AB referred to above, covert information gathering excludes the possibility of an effective legal remedy by necessity, therefore, in order to evaluate whether the regulations provide sufficient guarantees for the protection of the rights of individuals, the intervention must be subject to a three-stage control: when the intervention is ordered, during the implementation of the intervention and after the completion of the intervention. Such control has to be carried out by a “body” independent from the executive power. First and foremost, the permanent, ongoing and mandatory control guarantees that the requirement of proportionality is not violated in specific cases. In other words, external control is a fundamental guarantee element for ordering and implementing covert information gathering. In its decision adopted in 2013, the Constitutional Court established that the National Security Services Act enables the control of the authorisation procedure by the minister in charge of justice by bodies independent of the executive power through the fact that control is carried out by the National Security Committee of Parliament (which may request a report from the minister on general and specific affairs) and the Ombudsman. According to the position of the European Human Rights Court stated in 2016, the reporting obligation of the minister to the National Security Committee of Parliament and the limited investigative powers of the Ombudsman could not be regarded as sufficient guarantees.

II.7.
The responsibilities and powers of the Authority with regard to covert information gathering

With the amendment of the Privacy Act in 2018, the Authority’s responsibilities and powers were expanded relative to the possibilities provided by the earlier Ombudsman-like investigative procedures. The Authority may carry out investigations both on the basis of notification and ex officio, and according to the Privacy Act, it may conduct its data protection procedure both upon the request of the data subject and ex officio. It should, however, be noted that the Authority’s responsibilities and powers with regard to the control of data processing for national security purposes are not new, already the data protection commissioner had such powers based on the Data Protection Act [5] in force at that time.

As a supervisory body independent of the executive power, the Authority meets the criterion

[5] Act LXIII of 1992 on the Protection of Personal Data and the Accessibility of Data in the Public Interest

detailed in the decision of the Constitutional Court as its powers extend to control both during the implementation of the intervention and during the stage following its completion. The fact that the powers of the Authority do not extend to preliminary control does not constitute an impediment from the viewpoint of lawfulness because as indicated by the decision of the Constitutional Court, control has to be adequate and efficient not in the individual phases, but altogether over the three phases.

The Authority's responsibilities and powers for the supervision of data processing by the National Security Services and, within that, the control of the lawfulness of the covert information gathering is rather wide also in an international comparison. In the course of its investigation, the Authority contacted the data protection authorities of the Member States and requested information concerning their responsibilities and powers to take action to control data processing for national security purposes. It transpires from the responses of the data protection authorities of the EU Member States that the supervisory authorities of numerous Member States do not have supervisory or controlling powers with regard to data processing by the National Security Services, in particular, their covert information gathering, and the majority of the Member States authorities, which according to their national law are authorised to supervise data processing for national security purposes have never yet carried out an investigation of this kind.

To substantiate the above, it should be noted that – as far as it is aware – the Authority examined the compliance of data processing by the Specialised National Security Service through a comprehensive audit in 2017, which was unique in an international comparison.

The Privacy Act shall apply for the processing of personal data for law enforcement, national security and defence purposes. According to Section 51/A(1) of the Privacy Act, the Authority may launch an investigation ex officio in relation to the processing of personal data subject to the material scope of the Privacy Act.

The legislator established the material scope of the Privacy Act based on the purpose of processing, distinguishing data processing for law enforcement purposes, national security purposes and defence purposes. The Privacy Act lays down the range of interpretation for such data processing as follows:

processing for law enforcement purposes *means processing by an organ or person (hereinafter jointly "organ carrying out processing for law enforcement purposes") which is, within its or his functions and powers laid down by law, engaged in an activity aimed at preventing or eliminating threats to public order or public safety, preventing and detecting criminal offences, carrying out, or contributing to, criminal proceedings and preventing and detecting infractions, as well as carrying out, or contributing to, infraction proceedings, and implementing the legal consequences imposed in criminal proceedings or infraction proceedings, within the limits and for the purpose of this activity, including the processing of personal data connected to this activity for archival, scientific, statistical or historical purposes (hereinafter jointly "law enforcement purpose";* [Privacy Act Section 3(10)(a)]

processing for national security purposes *means processing by the National Security Services, within their functions and powers laid down by law, as well as processing under the Act on*

national security services by the counter-terrorism organ of the police, within its functions and powers laid down by law; [Privacy Act Section 3(10)(b)]

processing for national defence purposes *means processing under the Act on data processing by the defence forces and the Act on national defence and the Hungarian Defence Forces, as well as the measures that can be introduced during a special legal order, and the Act on the registration of foreign armed forces staying in the territory of the Republic of Hungary for service purposes and of the international headquarters and their staff established in the territory of the Republic of Hungary, as well as on certain provisions concerning their status* [Privacy Act Section 3(10)(c)]

This means that for launching the Authority's investigation, a notification or specific complaint by the data subject is not necessary to initiate the procedure. Considering the facts of the case within its own powers – i.e. the circumstances of whether an infringement has taken place, or the direct threat thereof in relation to the processing of personal data and the exercise of the right to have access to data in the public interest or data accessible on the grounds of public interest – the Authority may launch an investigation ex officio.

Pursuant to Section 54(1) of the Privacy Act, in the course of its investigation, the Authority shall be given access to and may make copies of all data processed by the controller subject to the inquiry that are presumed to relate to the case at hand and it shall have the right of access to and may request copies of such documents, including documents stored in an electronic data medium.

The Authority may learn about the data processing associated with the case under investigation, it may enter the premises serving as the venue of processing, it may have access to the tools used for performing the processing operation and it shall have the right to request written or oral information from the controller subject to the inquiry and from any employee of the controller. These investigative powers, however, are not limited to the controller as the Authority may request written information and copies of any data associated with the case under study including data stored in an electronic data medium not only from the controller, but also from any organisation or person associated with the case subject to the inquiry. The controller subject to the inquiry and any other organisation or person associated with the case under investigation shall comply with the call of the Authority within the period specified by the Authority.

The powers of the Authority extend only to the control of the lawfulness of external authorisation by the minister in charge of justice in relation to data processing operations by the courts, the control of the enforcement of the right to the protection of personal data takes place by way of data protection objections within the judicial system.

In the course of controlling the lawfulness of external authorisation by the minister in charge of justice, the Authority examines the submission in every single case to see whether it complies with the formal and procedural requirements set forth in legal regulation.

Within this, the Authority examines whether the submission for covert information gathering comes from the director general of the National Security Service authorised to secretly gather information and whether it contains all the data set forth in Section 57(2) of the National

Security Services Act. The submission must include the location of the covert information gathering, the name(s) or the circle of the person(s) concerned, and the available data suitable for identification. In addition, the submission must include the description of the covert information gathering (i.e. the means and methods to be applied) and the justification of its necessity, the start and end dates of the activity and in the case of a submission related to an exceptional authorisation according to Section 59 of the National Security Services Act, justification of the fact that it was indispensably necessary in the given case for the successful operation of the National Security Service.

When investigating the lawfulness of external authorisation, the Authority examines whether there is adequate verification of the fact that the covert information gathering was necessary in the interest of national security. The Authority's investigation therefore extends to the existence and the nature of the *interest of national security*. Section 74(a) of the National Security Services Act defines the interpretation of "interest of *national security*"; by comparison with the given facts of the case, it can be established or excluded whether interest of national security obtains. As the Authority may examine with regard to every data processing operation whether it restricts the right of the data subjects to informational self-determination to the necessary and proportionate extent, therefore, even where the interest of national security is invoked, it must be examined whether the enforcement of the interest of national security in the given case restricts the right of the data subjects concerned to informational self-determination and the right to privacy to a necessary and proportionate extent by the covert information gathering.

The Authority also examines whether there is sufficient verification in the submission concerning the external authorisation of the covert information gathering that the purpose of data processing cannot be achieved without it and whether the requested use of the means and methods is necessary. The submission is also to verify whether the covert information gathering is indispensably necessary for the requested period, and the Authority examines whether the authorisation was requested for a maximum of ninety days, or if that period was extended by another ninety days via a new submission and justification as required by law.

The Authority is also responsible for examining whether the decision of the minister in charge of justice causally follows from the facts set forth in the submission. The minister brings the decision on whether to approve the submission or to reject it if it is unfounded within 72 hours from its receipt. This means that the Authority examines not only the formal and procedural requirements of the submission, but also the decisions made by the minister in charge of justice on the individual submissions.

It is important to examine in the case of every decision whether the minister in charge of justice justifies the granting of the external authorisation in view of the facts and circumstances detailed in the given submission. Point 1 of Constitutional Court Decision 32/2013 (XI.22.) AB referred to the obligation to provide justification for the external authorisation as a precondition to the enforcement of ex post external control by specifying a constitutional requirement. Consequently, the justification must be sufficiently detailed and individualised so that it should enable the control of the facts and circumstances taken into account in making the decision and the adequacy of the content of the decision made on the basis of these facts and circumstances in the course of ex post external control.

Pursuant to Section 71(1) of the Privacy Act, in the course of its procedure and to the extent and for the period necessary for conducting it, the Authority may process all the personal data, as well as data qualified as secrets protected by law or secrets linked to the exercise of a vocation, which are related to the procedure and whose processing is necessary for the successful conduct of the procedure. According to Section 71(3) of the Privacy Act, the Authority shall have access to the data specified in Section 23(2) of Act CXI of 2011 on the Commissioner for Fundamental Rights (hereinafter: Ombudsman Act) in accordance with the provisions of its Section 23(7)[6]. Pursuant to this restriction, the investigation could not extend to the technical data of the operation of the means and methods used for the covert information gathering, the data enabling the identification of the person using them and the data related to cryptographic activities and encoding.

Irrespective of Section 71(3) of the Privacy Act, the Authority may have access to the data specified in Ombudsman Act 23(3)(e), (4)(f) and (5)(d), if it is necessary in the investigative procedure, the Authority's data protection procedure or the Authority's secret supervisory procedure launched in relation to the protection of the personal data of the collaborating person. The Authority may also have access to the data enabling the identification of the persons using the means and methods used to conduct the covert information gathering, or the use of disguised devices as set forth in the Ombudsman Act 23(3)(f) and (4)(g), if it is necessary in the investigative procedure, the Authority's data protection procedure or the Authority's secret supervisory procedure launched in relation to the protection of the personal data of the collaborating person. If the document that the Authority wishes to examine also includes data, which the Authority may have access to only according to paragraph (3), the document has to be made accessible to the Authority by blocking the data that are not to be accessed [Privacy Act Section 71(3a), (3b) and (3c)].

The Privacy Act therefore introduces a differentiated regulation with regard to the Authority's possibilities to access data, according to a threat of infringing other fundamental rights concomitant with the direct access to the data concerned by the Authority and the extent of the demand for the protection of rights linked to the direct access to the data.

III. The course of the Authority's investigation

III.1.
Launching the investigation

Pursuant to Section 51/A(1) of the Privacy Act, the Authority launched an investigation ex officio on 9 August 2021 to establish whether the Hungarian law enforcement agencies and National Security Services use the spyware called "Pegasus" as reported by the press and if so, whether these activities are compliant with the legal regulations applicable to the processing and protection of personal data.

[6] Ombudsman Act Section 23(7): *If, in order to ensure the complete clarification of a case, the Commissioner for Fundamental Rights considered it necessary that the documents specified in Fundamental Rights Commissioner Act Section 23(1)-(6) also be inspected, he may request the competent minister to have those documents inspected. The competent minister shall make the inquiry or shall have it made and inform the Commissioner for Fundamental Rights on the outcome of the inquiry within the time limit set by the Commissioner.*

The Authority was responsible for investigating whether in the course of applying the means and methods according to Section 56 of the National Security Services Act, data processing by the bodies authorised to gather information in secret by the minister in charge of justice operated in compliance with legal regulations and whether information was secretly gathered in the case of the persons made public and if so, whether it was done lawfully. To perform a general investigation of data processing related to the covert information gathering using the application constituting the subject matter of the investigation at the bodies concerned, the Authority used the investigative method of sampling.

The list with the names and phone numbers of 300 Hungarian citizens referred to in the articles published in the press[7] was not available to the Authority at the time of launching the investigation. To obtain this alleged list, the Authority, exercising its investigative powers described above, carried out procedural acts as follows.

In its letter of 11 August 2021, the Authority requested the director of Amnesty International Magyarország Egyesület to send the list containing the identification data and phone numbers of allegedly Hungarian citizens available to Amnesty International to the Authority within 15 days in view of Section 54(1)(d) of the Privacy Act. As Amnesty International Magyarország Egyesület did not respond to the Authority's letter, the Authority again requested the director on 13 September 2021 to forward the list in view of Section 54(1)(d) of the Privacy Act.

In its answer of 16 September 2021 Amnesty International Magyarország Egyesület informed the Authority that "*in relation to the phone numbers concerned, including the phone numbers potentially linked to Hungarian citizens, in the cases where Amnesty International Security Lab did not carry out its own tests of the 50,000 phone numbers concerned, we are unable to assist the investigation of the Authority by transferring data, because neither Amnesty International Magyarország Egyesület, nor Amnesty International International Secretariat has access to this list. In the cases, where Amnesty International carried out forensic tests and was able to demonstrate that the device was infected or involved, it notified the owners of the devices of the results and published the methodology of the forensic test as stated above."*

In a new request of 6 October 2021, the Authority requested the director of Amnesty International Magyarország Egyesület to forward the names and phone numbers of the persons referred to in their response in whose case forensic tests were performed and they were able to demonstrate their involvement.

In his answer of 18 October 2021, the director of Amnesty International Magyarország Egyesület informed the Authority as follows: "*the Egyesület is a legal entity registered in Hungary and as controller is separate from the International Secretariat or other Amnesty International entities";* the director also emphasised that *"our Association does not have the data requested in the letter, we have not processed the data and we do not qualify as controllers with regard to these data. In order to carry out your investigation as successfully as possible, please contact the International Secretariat of Amnesty International".*

---

7 https://www.direkt36.hu/leleplezodott-egy-durva-izraeli-kemfegyver-az-orban-kormany-kritikusait-es-magyar-ujsagirokat-is-celba-vettek-vele/

In its letter of 19 November 2021, the Authority informed the director of Amnesty International Magyarország Egyesület that in the course of its investigation, the Authority may request written information from any organisation or person that may be associated with the case under investigation and request copies of any data or documents including those stored in electronic data media that may be associated with the case under investigation. Pursuant to Section 54(1)(d) of the Privacy Act, Amnesty International Magyarország Egyesület as an entity that may be associated with the case under investigation, has to comply with the call of the Authority, even if it does not regard itself as controller or processor with regard to the data requested.

In a letter of 29 November 2021, the Authority contacted the International Secretariat of Amnesty International located in London requesting them to send the list containing the identification data and phone numbers of Hungarian persons available to Amnesty International to enable the successful conduct of the Authority's investigation.

In view of the fact that the International Secretariat of Amnesty International did not respond to the Authority's letter, the Authority re-sent its letter to the organisation located in London on 10 December 2021.[8]

In addition to the above, there was also another issue how the phone numbers associated with Hungarian persons – which Amnesty International's Security Lab unit found to be infected by the spy software, could have been disclosed during the so-called Pegasus Project fact-finding investigation into the software of the Israeli-based NSO group, in which 80 journalists from 17 media companies in 10 countries took part.

III.2.
Method for the clarification of the facts of the case

With a view to clarifying the facts of the case, the Authority developed an investigation plan as a first step, in which the planned course of the investigative acts needed to conduct the investigation, the possible range of controllers to be investigated and the methodology of the investigation were laid down. The methodology for selecting individual file and authorisation numbers for sampling constitutes an annex to the memo drafted on the investigation plan.

Accordingly, once the statistical reports requested from the Specialised National Security Service were forwarded, the Authority requested the file and authorisation numbers of all the cases related to the use of devices from the ordering bodies and in the course of the on-site investigations, it checked all the files and documentation included in the list of files generated from the file and authorisation numbers in the course of sampling.

To clarify the facts of the case, the Authority carried out the following investigative acts:

- The Authority contacted the director general of the Specialised National Security Service requesting the information necessary for clarifying the facts of the case, and

[8] At the closing date of this manuscript, the International Secretariat of Amnesty International did not send an answer of merit to the Authority, but it indicated in an e-mail on 7 January 2022 that it received the Authority's request.

statistical reports concerning the use of the tool.

- The Authority held an on-site investigation at the Specialised National Security Service, requested oral information, as well as copies of documents, and inspected the relevant documentation.
- The Authority carried out on-site investigations also at the individual ordering bodies, in the course of which it examined the lawfulness of the external authorisation by inspecting the relevant documents.
- The president of the Authority participated in the closed session of the National Security Committee of Parliament, where information was provided concerning the subject matter of the investigation.
- The president of the Authority also requested the minutes of the additional closed sessions from the National Security Committee of Parliament, whose agenda included the “Pegasus” spyware constituting the subject matter of the investigation.
- With reference to the news appearing in the press, the Authority contacted Amnesty International Magyarország Egyesület and in view of Section 54(1)(d) of the Privacy Act requested them to send a list containing the personal data and phone numbers of the data subjects of allegedly Hungarian citizenship available to them according to the information published in the press in relation to the investigation to the Authority.
- The Authority also contacted the International Secretariat of Amnesty International requesting them to send to the Authority the list containing the personal data and phone numbers of data subjects of allegedly Hungarian citizenship available to them, according to the information published in the press in relation to the investigation.
- The Authority also engaged an IT expert with a view to be able to check all the accessible information related to the software in the course of the investigation.

It is important to note that the documentation constituting the subject matter of the investigation may include data under Section 71(3)-(3c) of the Privacy Act, which the Authority may not have access to. Accordingly, the Authority may not have access to the documents containing the technical data of the operation of the means and methods used for covert information gathering, all the documents enabling the identification of the persons applying them, documents related to cryptographic activity and encrypting, and the documents, which would enable identification of the source of information, as well as documents access to which would violate the obligations of the National Security Services undertaken vis-a-vis foreign partner services. In the event that such data ae found, the Authority may request copies of the documents, subject to their being rendered unidentifiable, or may request the competent minister to examine the documents.

In view of the fact that the documents constituting the subject matter of the investigation include classified data, when documenting the results of the investigation the classification marking was repeated in accordance with Section 7(1) of Act CLV of 2009 on the Protection of Classified Data (Classified Data Act).

III.3.
Examination of the legal conditions for covert information gathering

The precondition to the enforcement of ex post external control of covert information gathering

is the justification of the authorisation. The authorisation by the minister in charge of justice must include the detailed justification enabling the Authority to examine the facts and circumstance taken into account in the course of decision-making, as well as compliance of the content of the decision on the occasion of the Authority's subsequent control. In the course of the on-site investigations carried out at the individual controllers, the Authority examined submissions requesting authorisation for covert information gathering subject to external authorisation, as well as the decisions of the minister of justice containing the decision on external authorisation.

Using the investigation methods detailed above (list of specific persons and list according to case numbers selected by sampling), the Authority examined close to a hundred submissions, as well as the compliance of the decisions of the minister of justice associated with them, along with the following questions concerning the lawfulness of the external authorisation.

- Were the submissions compliant in terms of formal and procedural rules?
- Was the submission received from the director general?
- Did the submission include all the data specified in Section 57(2) of the National Security Services Act?
- Was the authorisation granted within the time limit?
- Did the validity of the authorisation exceed 90 days?
- Was justification attached to the authorisation?
- If there was exceptional authorisation, were the rules thereof complied with?
- Did the submission verify that the covert information gathering was needed in the interest of national security?
- Did the submission verify that the purpose of data processing could not be achieved without the covert gathering of information?
- Did the submission verify that the use of all the means and methods requested were necessary?
- Did the submission verify the necessity for the duration of covert information gathering requested?
- Did the decision of the minister in charge of justice causally follow from what was said in the submission?
- Did the minister in charge of justice justify the granting of the external authorisation with sufficient detail reflecting on the facts and circumstances presented in the submission?

In relation to the above, it is important to consider the notion of "*interest of national security*" whose interpretation is defined in Section 74(a) of the National Security Services Act:

"To secure the sovereignty and protect the constitutional order of the Republic of Hungary and, within that framework,
aa) to detect aggressive efforts against the independence and territorial integrity of the country,
ab) to detect and prevent covert efforts which violate or threaten the political, economic, defence interests of the country,
ac) to obtain information of foreign relevance/origin necessary for government decisions,
ad) to detect and prevent covert efforts to alter/disturb by unlawful means the constitutional order of the country ensuring the observance of fundamental human rights, representational democracy based on pluralism and the constitutional institutions, and
ae) to detect and prevent acts of terrorism, illegal weapons dealing and trafficking in drugs,

and illegal trafficking in internationally controlled products and technologies;".

In the course of controlling the authorisation for covert information gathering by the minister in charge of justice, the Authority also considered the earlier statement of the minister in charge of justice made to the press, according to which "*authorisations are outsourced, they are signed by secretary of state Pál Völner; the secretary of state is the person who grants or refuses authorisations and in this regard the Ministry of Justice is responsible only for compliance with the legal regulations and the existing content of the legal accessories in the constitutional order of the covert information gathering and not for the professional content sent to our desk".*[9]

Section 58(2) of the National Security Services Act expressly refers the powers of authorisation to the minister in charge of justice and does not authorise the delegation of the authorisation powers. Section 5(3) of Act XLIII of 2010 on Central State Administrative Organs and on the Legal Status of Government Members and Secretaries of State allows that the Rules of Organisation and Operation of the central state administrative organ provide for the delegation of the right of issue documents in certain cases within the powers of the head of the organ to a person filling in posts listed in the Act, who would take action on behalf of the organ's head when making a decision. Section 5(1) and (2) of the Ministry of Justice Instruction 9/2019 (VIII.1) IM on the rules of organisation and operation of the Ministry of Justice (hereinafter: IM SZMSZ) determine the order of substitution in the event that the minister is incapacitated. The Rules of Issue can be found under Title 31 of Section V of the IM SZMSZ. This does not mention the delegation of powers concerning the authorisation of covert information gathering.

In relation to this, it is necessary to set forth that the Constitutional Court in its Decision 23/2018 (XII.28) AB pointed out that "*the person acting within issuing powers has only the right to sign, which does not include the right to make decisions, but certifies that the decision issued is authentic and its content is identical with that, which was originally brought and signed by the addressee of the powers. The person exercising the powers has therefore the power to both issuing and to delegating the right to issue, however, the person to whom the powers to issue were delegated does not have a right to exercise those powers, he is not entitled to make decisions in an administrative legal relationship."*

Because of this above, the Authority contacted dr. Pál Völner, secretary of state to the Ministry of Justice, in relation to the decisions of the minister of justice under investigation, who stated in his response of 8 November 2021 that "*in the case of the authorisation of the file numbers listed [in the letter of the Authority] the authorisations were signed within the powers of substitution because the minister was incapacitated".*

In its procedure, the Authority checked only the decisions of the minister of justice concerned in the investigation and did not examine in general how the order of issuing evolves in the authorisation procedure. The National Security Committee of Parliament is entitled to do so according to the legal regulations in force. As mentioned by Constitutional Court Decision 32/2013 (XI.22) AB "*pursuant to Section 14(4) of the National Security Services Act, the National Security Committee of Parliament exercises control over the authorisation procedure*

[9] Source: https://telex.hu/video/2021/07/21/pegasus-kemszoftver-lehallgatasi-botrany-nso

of the minister of justice". According to Section 14(4)(b) of the National Security Services Act referred to by the Constitutional Court, the National Security Committee of Parliament may request information about the authorisation procedures defined in Sections 56 and 59 from the minister in charge of justice, the minister in charge of the civil national security services, the minister in charge of civil intelligence activities, the minister in charge of defence and the directors general.

IV. The software subject to the investigation

The Authority invited Alverad Technology Focus Kft. to analyse the news and information related to the "Pegasus" spyware. The expert in information security compiled the following summary analysis on the "Pegasus" software.

IV.1. Summary analysis

*B**ackground and actors of the events***

The corporate and personal background of the NSO Group

The Pegasus spyware was created by the NSO Group operating in Israel. The NSO Group is an organisation operating in the field of cyber intelligence, commonly referred to as "Surveillance-For-Hire"[10], which develops surveillance technologies and builds and leases surveillance infrastructure to its clients, characteristically nation states and governments. "
NSO obtained its name from the initials of the names of its founders as the company was founded by Niv Karmi, Shalev Hulio and Omri Lavie in 2010. Whereas in the case of Hulio and Lavie, it is a known fact that they had served earlier at decyiphering and cyber intelligence unit of the Israeli Army (Unit 8200), all that is known about Karmi is that he served as a major of the special forces and one of the "most outstanding" organisations of the intelligence community[11] (the name of Unit 8200 also arise in his case, but he did not confirm this even in an interview made with him).

According to the official history of NSO, the company developed a tool for civilian use, with which service providers were able to maintain and adjust the users' mobile phones remotely. The user clicked on the link sent in a text message, and then the service provider had access to the device and made the adjustments. Later, secret services contacted Hulio and Lavie to modify the solution in accordance with their demands and purposes. The Pegasus spyware was born after this transformation.

---

[10] Surveillance-For-Hire includes observation, wire-tapping and tracking services. Such organisations do not carry out observation or wire-tapping, they only develop and rent the technologies and services needed for such activities. It is the clients that carry out the observation or wire-tapping using the technology or service; currently, however, it is not at all certain that the activities of NSO are limited to the delivery and commissioning of the system and the licences. There are also indications that NSO also provides central services that play a substantial part in infecting the devices which may constitute operative activity.
[11] Source: https://www.zeit.de/digital/datenschutz/2021-10/nso-group-technologies-gruender-niv-karmi-pegasus-ueberwachungssoftware

According to Karmi's statement, however, the other two founders saw new business opportunities in transforming the tool for civilian use into spyware and they contacted Karmi and requested his collaboration. A few months later Karmi left NSO as he disagreed with the business decisions of his co-founders and established his own venture under the name Polus Tech[12], which develops and instals portable mobile cell tower systems.

In 2014, Francisco Partners, a technological investment company, acquired the company for USD 130 million, but in 2019 Lavie and Hulio re-acquired majority holding through Novalpina Capital, an investment group, in the company then estimated to have a net worth of USD one billion.

A substantial increase in value is also attributable to the fact that Circles, athe cyber intelligence company, also acquired by Francisco Partners, and the NSO Group was merged in 2014 [13]. Circles is an Israeli company specialised in mobile surveillance and tracking. Currently, the value of the NSO Group, which today employs close to 500[14] employees, can be estimated at USD 1.5 billion.

The NSO Group is one of the companies having the most powerful capabilities providing surveillance services for rent and satisfying demand for cyber intelligence. The surveillance infrastructure service for hire and the private cyber spying sector constitute a market of many billions of dollars, the NSO Group has several substantial competitors, for instance, in December 2021, Meta owning Facebook and Citizen Lab working together identified four additional private cyber intelligence companies with Israeli backing (Cobwebs, Cognyte, Black Cube and Blue Hawk) and three other organisations that used the Facebook platform for their operations[15].

After examining Pegasus, Ian Beer and Samuel Groß, cyber security researchers at Google's Project Zero, called Pegasus one of the most technologically advanced attack codes they have ever seen and in their view the ability to create Pegasus would be available only to a few nation states at most.

Organisations participating in the investigations and their role

Pegasus Project

The Pegasus Project[16] umbrella organisation embraces 17 international media organisations, which participated in the investigative work related to Pegasus' activities; an international organisation of journalists called Organized Crime and Corruption Reporting Project[17] (OCCRP) is also one of its members. Under *the umbrella organisation, 80 journalists from 10 countries[18] participated in the investigation.*

---

[12] https://polustech.com/
[13] The NSO Group (which was by then held by Francisco Partners) acquired the company owning Circles through OSY Technologies, its Luxembourg subsidiary. Source: https://forensicnews.net/the-covert-reach-of-nso-group/
[14] During the 2014 acquisition period, the NSO Group had 50 employees.
[15] Meta banned the companies concerned from using the platform and deleted the 1,500 profiles used for these operations.
[16] https://forbiddenstories.org/about-the-pegasus-project/
[17] Project to uncover organised crime and corruption
[18] United Kingdom, France, Germany, United States, Israel, Mexico, Belgium, India, Syria, Hungary

Forbidden Stories

The goal of the non-profit organisation established by Reporters Without Borders and the Freedom Voice Network in 2017 is to ensure the operation of a free press through international and local consortia. The organisation built up an international network[19] and platform through which the work of journalists threatened, silenced or murdered can be continued, published and propagated[20].
The Forbidden Stories and Amnesty International obtained the list containing 50,000 phone numbers, which served as the basis of the investigations and the identification of the potential data subjects. The source of the list is unknown, Forbidden Stories and Amnesty International did not disclose where the list came from and how they obtained it for reasons of protecting the source. Not even the media organisations and journalists collaborating in the Pegasus Project know the source.

Amnesty International (AI)

Amnesty International is one of the largest and best-known human rights organisations founded in 1960, which has some seven million members, supporters and activists in close to 150 countries. The organisation operates local offices in the regions, thus there is a local office also in Hungary.

Amnesty Tech[21] is the technical division of Amnesty International, which researches and controls the impact of using technologies on human and personality rights; another important task of it is the detection and investigation of cyber-attacks against civil society (including spyware or other surveillance or wire-tapping systems). The Security Lab group established in 2019 under the auspices of Amnesty Tech provided the necessary technical competence and support within the Pegasus Project[22].

Amnesty International published the investigative report[23] on 18 July 2021 which documented the investigative methodology used by them and the results of their investigations.
Amnesty International noticed the activities of Pegasus developed by the NSO Group as early as in 2018 when they identified the Pegasus spyware in the mobile device of one of their staff[24].

Citizen Lab

Citizen Lab operating at the University of Toronto is an independent research laboratory, which largely carries out research and investigations related to digital spying against civil society and other cyber security issues. Citizen Lab typically uses mixed methods overlapping several areas in its research and they apply political, legal and IT analyses. Citizen Lab follows upon the operation of several other organisations similar to the NSO Group. They have been working

---

[19] *https://web.archive.org/web/20210719090134/https://forbiddenstories.org/our-network/*
[20] *https://rsf.org/en/news/launch-forbidden-stories-project*
[21] *https://www.amnesty.org/en/tech/*
[22] *As to the size of Amnesty Tech, it can be estimated from the LinkedIn profile of an earlier manager and co-founder Tanya O'Carroll, whose work experience includes having directed 20 people in 6 countries as a director of Amnesty Tech.*
[23] *https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/*
[24] *https://www.amnesty.org/en/latest/research/2018/08/amnesty-international-among-targets-of-nso-powered-campaign/*

on the investigation of the activities of the NSO Group since 2016; they published their first report[25] in August 2016 when the Pegasus infection was found in the mobile phone of Ahmed Mansoor, a human rights activist.
As Citizen Lab had earlier examined the activities of the NSO Group, as well as the traces of the Pegasus tool, Amnesty International invited Citizen Lab to examine and validate the methodology of Amnesty International and to check the results of its investigation. Citizen Lab confirmed the results of Amnesty International's research, they found Amnesty International's methodology well-founded on the basis of the published documents[26], the results of the investigation as correct, or rather the two groups arrived at the same results independently of one another.

Amnesty Tech Security Lab shared the security copies of four iPhone devices with the experts of Citizen Lab, which had also been examined by Security Lab. Citizen Lab's own examinations verify the results of Security Lab in all four cases, and the two groups found the traces of Pegasus in these devices independently from one another.

The leaked list containing the phone numbers

A "leaked" list containing some 50,000 phone numbers is a key element of the Pegasus Project. According to the Pegasus Project, the phone numbers in the list have been involved in the activities of the Pegasus spyware in one way or another since 2016. The data included the time and date of the selection of the numbers and their entry in the system.

The source of the list is unknown and there is no information available about the circumstances of the leakage. It is not known who compiled the list on what basis and how the list was obtained by the Pegasus Project umbrella organisation or Amnesty International, nor is it known what data are included in the list in addition to the phone numbers and dates.

Based on the data in the list, the media partners of the Pegasus Project identified ten governments, which are believed responsible for selecting the targets[27].
There is a great deal of uncertainty around the list. The statements related to the list can be misinterpreted and do not necessarily match their direct or underlying meaning:

- *"leak 50,000 phone numbers of potential surveillance targets" – Amnesty International*
- *"more than 50,000 phone numbers selected for surveillance by the customers of the NSO Group, an Israeli company" – Forbidden Stories*

The NSO Group firmly denies[28] that the list could be connected to their activities or the activities of their clients; according to their position, the list is not a list of the targets or potential targets of NSO clients.

NSO's response included an allusion to the fact that the phone numbers in the list may come

---

[25] https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/
[26] https://citizenlab.ca/2021/07/amnesty-peer-review/
[27] Azerbaijan, Bahrein, Kazakhstan, Mexico, Morocco, Rwanda, Saudi-Arabia, Hungary, India and the United Arab Emirates
[28] https://www.theguardian.com/news/2021/jul/18/response-from-nso-and-governments

from public services, including among others HLR search service, which is not connected to NSO or the services of the company.

The Home Location Register (HLR) is one of the "databases" of mobile service providers, which contains data pertaining to the subscriber in relation to the given service provider, entitlements to the service, current place of stay, the status of the device (switched on or off) or other subscriber data. Incidentally, using public HLR search services, anybody can make enquiries, but stringent rules apply to the data returned from such services[29], at most the data returned from such public services include whether the phone number exists or not, which operator the device belongs to and whether it is switched on or off. Typically, publicly accessible HLR search services are used to prevent fraud or for commercial purposes, for instance in the case of a text message campaign, HLR searches can be used to ensure that the messages are only sent to existing and operational phones.

The use of the HLR search service as the source unrelated to NSO or its presence in the processes does not arise in the original investigative report of Amnesty International, it crops up directly in relation to NSO's response; it does not exclude however that there is a connection between the list (even as a set of data from an HLR search service provider) and the NSO service, because the use of the HLR search can be envisaged in the process of propagating Pegasus, or even in additional related operations.

For instance, the collaborating operator (the person or organisation launching and managing the attack process) may find out using an HLR search, whether the targeted device exists, whether it is registered and switched on, whether the attack against the device can be launched. Another aspect is that a HLR search can be found also in the delivery process of text messages and in earlier periods Pegasus got to the targets through the links placed in text messages. It can also possible that Pegasus' background infrastructure (for instance an interface) uses HLR searches, or even NSO may use an external HLR search service provider with appropriate authorisation for the handling of such queries and reporting.

Reacting to NSO's response, the Pegasus Project mentioned that according to a source, directly knowledgeable about the NSO system, who wishes to remain anonymous, HLR searches were integrated into the system after the merger of NSO and Circles. According to another source[30], this integration was not truly successful and NSO closed the Cyprus office of Circles in 2020 and dismissed the employees working there[31].
Amnesty International responded to the NSO Group's denial and the information published in the media in a statement[32]. The organisation advocates for the validity of the data and the results of the investigation, and puts on record that the list includes potential targets [33].

One of the sources of the "misunderstandings" surrounding the list could be that one Israeli media organisation[34] applied presumably false terminology in their report, on the basis of which other media organisations were also willing to handle the statement as a fact that the list

---

[29] Earlier this was not always the case, the area was rather underregulated; by now however stringent rules apply to such services and data that the person making the query can get are strongly filtered.
[30] https://zetter.substack.com/p/the-nso-surveillance-list-what-it
[31] https://www.vice.com/en/article/ep48kp/nso-group-cyprus-circles-bulgaria-ss7
[32] https://www.amnesty.org/en/latest/news/2021/07/amnesty-categorically-pegasus-project-data-linked-to-nso/
[33] „and that the data are irrefutably linked to potential targets of the NSO Group's Pegasus spyware"
[34] No longer accessible (Source: https://www.calcalist.co.il/home/0,7340,L-8,00.html)

contains phone numbers, which Pegasus had already infected, i.e. NSO clients wire-tapped or subjected to surveillance all the phone numbers included in the list. According to Amnesty International's statement, the list includes phone numbers which they think would be of interest to NSO's customers[35], but they were not necessarily spied upon (although based on technical examination, some of the persons in the list were presumably spied upon as traces of Pegasus were identified in their devices).

According to The Guardian's summary,[36] the phone numbers in the list are indicative of the potential targets NSO's government clients identified and marked in advance for possible surveillance attempts. According to the article, this is an indication of intent, but the list does not reveal whether attempts were made to infect and wire-tap the devices with Pegasus or whether the devices were actually infected and wire-tapped.
The Guardian's summary suggests that the forensic examination by Amnesty Tech Security Lab not only demonstrated the traces of the Pegasus spyware in the physically examined devices (of a small number relative to the list), but also uncovered some correlation between the times and dates when the traces were created and the times on the list, in some cases with only a few seconds of difference between the start of Pegasus' activity on the device and the time shown in the list. This can be interpreted that in such cases the device was targeted virtually immediately after its selection (when the phone number was put on the list, for instance, by an HLR search) and it was successfully hacked.

Thus, it can be concluded that inclusion in the list means specific surveillance activity only if coupled with a positive result of the examination and digital trace analysis of the device (this however was established only in the case of 37 phone numbers according to the investigative report). In such a case it may become apparent that there is a connection between the time and date of the inclusion in the list and the specific infection.

It was stated in several analyses that it seems unimaginable that secret services or ***other government agencies of several nations would upload data related to eventual targets into a common (even jointly used cloud) system because such data are*** *processed in house by all such organisations because of classification and confidentiality.*

This opinion was confirmed by a leaked document presenting the infrastructure necessary for the operation of Pegasus. The document is a product presentation[37], presumably from 2013 produced by the person in charge of products at NSO[38]. Based on the document, clients operate on their own side of the system, i.e. "targeting" is done on the client's side[39].

In relation to the leakage of the list containing the phone numbers, it was raised on several occasions that the data were leaked from a Cyprus server. Shalev Hulio, NSO's founder and

---

[35] https://www.opindia.com/2021/07/pegasus-spyware-controversy-amnesty-backs-out-says-they-never-claimed-list-was-of-nso-targets-media-misrepresented/
[36] https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus
[37] The document was also shared by Claudio Guarnieri, the head of Amnesty Tech Security Lab (Source: https://www.documentcloud.org/documents/4599753-NSO-Pegasus.html#document/p12/a437979)
[38] According to the metadata of the document, it was prepared in 2013, which is supported by the version numbers of the targeted operating systems supported at the time. The document was prepared by Guy Molho, who was director of product management at NSO between 2013 and 2018.
[39] This, of course, does not technically exclude the possibility that the numbers entered into the system on the client's side can be transferred later to some external source in some way.

CEO mentioned in an interview[40] that the company was contacted by data brokers concerning the data package and stated that they were leaked from NSO's Cyprus servers. NSO claims that it has no servers in Cyprus[41], and they checked several data in the list and none of them are connected to any of their clients. In relation to this, Hulio mentioned that NSO has 45 clients globally and they checked the phone numbers in the list jointly with every one of their clients and the numbers do not belong to any of their clients.

The journalists of the Pegasus Project identified about a 1,000 phone numbers, they were able to associate the person of the owners with these phone numbers. Amnesty Tech Security Lab examined 67 devices, whose number was included in the list.

Their examinations found the traces of a successful Pegasus infection in 23 cases and in another 14 cases they identified the traces of attempted intrusion. In the case of the remaining 30 devices, the tests were unsuccessful and in many cases the devices have already been replaced. The phones included 15 Android devices, none of which showed signs of successful infection[42], but 3 Android phones were found to have signs of targeted attacks, such as text messages related to Pegasus.

The list included 300 Hungarian phone numbers. The appendix to the digital trace analysis report issued by Amnesty International[43] shows only two Hungarian data subjects, but investigative portal Direk36, the Hungarian partner of Pegasus Project identified several phone numbers and continues to publish material related to the Hungarian persons concerned.

Direkt36 published materials in relation to several persons concerned, whose devices could not be examined, but whose phone number was included in the original list. According to the terminology used by Direkt36, the persons in the list were "targeted"; this, however, did not mean that the device of the person concerned was actually infected and/or wiretapped: "The leaked data do not necessarily mean that Pegasus was certainly deployed against the targets and the devices were actually penetrated, but in many cases – including several Hungarian targets – the subsequent examination of the phones proved that the devices were truly penetrated using the NSO program[44]."

Direkt36 published some material also about a person, whose phone number was not included in the leaked list[45], but he had earlier initiated an examination by the staff of Citizen Lab and Amnesty International, who did find the traces of Pegasus generated in 2021 on the device handed over for examination.

Internationally, there were several validations carried out by the government of the given country or an independent organisation entrusted by the government. One such examination was the official examination carried out by ANSSI[46], the cyber protection organisation of the

---

[40] https://www.calcalistech.com/ctech/articles/0,7340,L-3912882,00.html
[41] They also stated that NSO and Circles operate fully independently and separately from one another.
[42] In contrast to iPhones, Android phones do not log the information needed for Amnesty's trace analysis.
[43] https://www.amnesty.org/en/latest/research/2021/08/appendix-e-pegasus-forensic-traces-per-target-identified-in-the-aftermath-of-the-revelations-of-pegasus-project/
[44] https://www.direkt36.hu/az-orban-kormany-allamtitkarat-is-megceloztak-a-pegasusszal-mikozben-belharcokat-vivott-paks-ii-miatt/
[45] https://www.direkt36.hu/iden-is-bevetettek-meg-a-pegasust-tavasszal-megfigyeltek-egy-ellenzeki-mediatulajdonost/
[46] Agence nationale de la sécurité des systèmes d'information (ANSSI)

French state, initiated by the French government[47], which validated Pegasus infection in the cases of two French journalists via technical examination and in the course of their investigation they reached the same result as Amnesty International's analysis. In Belgium, the military intelligence service examined[48] two devices of a Belgian journalist and his wife included in the list and they assumed that both devices were infected by Pegasus.

The operation and detection of Pegasus and the infrastructure

In earlier periods, Pegasus and the operation of the infrastructure built up by NSO underwent an evolution. Basically, there are five information sets, from which deduction can be drawn concerning the operation of the system and any eventual difference between versions:

- *The "spyware" application running on the infected mobile devices, which has already been analysed by several expert companies,*
- *The Product Description earlier leaked from NSO, presumably around 2013, which presents the operation of the Pegasus infrastructure at the time[49],*
- *The relevant materials of the Pegasus Project,*
- *The investigative report of 2018 by Citizen Lab[50],*
- *WhatsApp submission in a litigation, which includes a leaked contract between NSO and its Ghana client signed in 2015[51].*

Naturally, many other sources also published information concerning the operation of Pegasus, but they characteristically analysed the vulnerabilities through which this malicious application could infect devices. If Pegasus is examined as a complex system, it is worthwhile to do more than merely analyse the application exploiting the vulnerabilities of the devices which then infects the devices and carries out spying activities.

Pegasus Agent (the "spyware" application)

Following successful infection, a "spyware" application is installed on the device. Installation does not require the users' authorisation, it takes place without the user noticing it. The application running on the infected device provides full authorisation for the attacker with regard to the device and the data stored in it.

The Pegasus agent is integrated into the kernel of the device's operating system and the legitimate applications running on the device. This ensures that the agent can access the system functions and legitimate applications, as well as the data stored in them. The agent "sees into" the operation of the applications (for instance phone calls, text messages, chat, etc.), which means that even though a chat application may use encryption from endpoint to

---

[47] https://blogs.mediapart.fr/la-redaction-de-mediapart/blog/300721/pegasus-french-judicial-probe-confirms-technical-proof-espionage-against-mediapart-jo

[48] https://thewire.in/tech/pegasus-journalist-wife-targetted-by-nso-spyware-finds-belgiums-military-intelligence

[49] Information from hacking the Hacking Team, which operates in a similar field, includes letters, which the clients shared with the staff members of Hacking Team about information on NSO products. The government of Mexico forwarded this document to Hacking Team.

[50] https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

[51] NSO and Infraloks Development Limited, presumably a covert company for the government of Ghana, signed an 8 million dollar contract on the simultaneous surveillance of 25 phones on 17 December 2015.

endpoint, the attacker is able to access the data, which are as yet unencrypted. Integration between the applications and the kernel enables the agent to receive the system calls of the applications launched towards the kernel, as well as the data sent by the applications through the system functions towards the kernel. Operation close to the kernel creates the possibility for passive and active surveillance and the collection of data.

For the installation of the application, Pegasus uses the vulnerabilities of the devices or the applications running on the devices. In the course of the evolution of Pegasus, the researchers identified several vulnerabilities, through which the malicious code was able to install itself without the knowledge and intervention of the user.

Evolution

In the cases of the earlier versions of Pegasus, the user had to click on the link sent by the attacker in order to have the malicious code downloaded and installed without the user's knowledge and intervention. Because of this, in the period before 2019, in most cases the attacker sent misleading content to the victim, for instance by e-mail or text message or other chat-like application(for instance WhatsApp). In the earliest case of 2016 examined by Citizen Lab, Ahmed Mansoor[52], a human rights activist, received a text message, which promised new information concerning prisoners tortured in a prison. The text message contained a link, which Mansoor sent to the analysts of Citizen Lab, who in the course of their examination identified NSO's attacking infrastructure[53].

The website accessible through the link contained an attack code, which would have infected the device exploiting vulnerabilities that had not been known before. Citizen Lab and a company engaged in the security of mobile devices called Lookout examined the code and then they identified three till then unknown "zeroday" vulnerabilities, which were later called Trident[54].

This means that NSO already in 2016 exploited vulnerabilities, which had been unknown before and enabled the installation of the malicious application with one click of the user and to compromise the device in its full depth.

From 2019, however, users no longer had to click for the Pegasus agent to be downloaded and installed on their device. The next step of the evolution was the "zeroday - zeroclick" penetration when the user did not even have to click for the Pegasus agent be installed on his device.

According to WhatsApp, the mobile phones of over 1,400 users were targeted in 2019 by the technology sold by NSO in twenty countries in the course of a 14-day attack campaign. For this attack, they exploited a till then unknown WhatsApp vulnerability[55], which enabled the installation of the malicious code on the targeted device without the knowledge and interaction

---

[52] This was not the first occasion when attempts were made to compromise Mansoor's device remotely using spyware. In 2011, an attempt was made to hack his device using FinFisher/FinSpy, and in 2012 using the solution of Hacking Team. https://index.hu/tech/2015/07/07/600_milliot_fizettunk_a_vilag_legostobabb_hekkereinek/)
[53] https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/
[54] The Trident vulnerability chain: https://support.apple.com/hu-hu/HT207107
[55] https://nvd.nist.gov/vuln/detail/CVE-2019-3568

by the user through a WhatsApp call. The malicious code could install itself even if the user did not take the call. WhatsApp worked with the researchers of Citizen Lab in the investigation of the event. In the course of its investigation Citizen Lab identified more than a hundred cases when human rights activists and journalists were targeted with Pegasus. WhatsApp notified the persons presumably concerned and in 2021 it launched a lawsuit against NSO in front of a court in California[56]. Although the exploitation of the WhatsApp vulnerability did not require any interaction on the part of the user, but the call, or the call not taken may have triggered suspicions in the user. In the next phase of the evolution, Pegasus no longer leaves such traces, the attack goes totally undetected.

In 2020, Citizen Lab identified an attack against 36 devices aimed at staff members of the Al Jazira TV channel, exploiting a vulnerability unknown until then in iMessage available on every Apple phones. Based on subsequent examination, the vulnerability named KISMET was exploited as early as between October and December 2019, for instance against staff members of Al Araby TV [57]. The exact operation of the KISMET vulnerability is not known. Citizen Lab notified Apple of this case, who indicated their intention to investigate the phenomenon; however, no specific publication was made about this. According to the assumptions of Citizen Lab and other researchers such as Samuel Groß of Google Project Zero, Apple improved the iMessage vulnerabilities in iOS14, for instance, when the BlastDoor protection feature appeared in Apple's operating system, which acts as a sandbox and is responsible[58] for opening and scanning untrusted attachments that come via messaging[59].

Although the BlastDoor introduced in the iOS 14 operating system made the exploitation of the KISMET vulnerability impossible, NSO began to use a new attack code from February 2021 also targeting the iMessage application. Citizen Lab identified the mode of attack on the infected device of a Saudi activist in March, then notified Apple of the vulnerability in early September. There is plenty of information available concerning the vulnerability called FORCEDENTRY[60], because Apple validated the vulnerability in just a week[61], and then it published the patch[62]. Similarly to WhatsApp, Apple also launched a lawsuit[63] against NSO in front of a California court, and announced that it was going to support similar organisations carrying out security research with 10 million dollars and the amount of compensation recovered from the litigation.

Numerous security researchers and security companies analysed the FORCEDENTRY vulnerability and Google Project Zero also published the highly detailed analysis[64]. Through

---

[56] https://law.justia.com/cases/federal/appellate-courts/ca9/20-16408/20-16408-2021-11-08.html
[57] https://threatpost.com/zero-click-apple-zero-day-pegasus-spy-attack/162515/
[58] "sandbox" functionality. Every application runs in a closed space, they cannot exit it and other applications can have no access to its processes.
[59] https://appleinsider.com/articles/21/01/29/apples-ios-14-integrates-new-messages-security-sandbox-called-blastdoor
[60] Although this vulnerability is widely known as FORCEDENTRY, it is the same as the MEGALODON vulnerability presented in Chapter 5 of Amnesty International's investigation report, just not under that name.
[61] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30860
[62] For instance, the security updates of iOS/iPadOS 12.5.5 and iOS/iPadOS 15 versions patched up close to 25 vulnerabilities (Source: https://blog.qualys.com/vulnerabilities-threat-research/2021/09/29/apple-fixed-nso-pegasus-iphone-spyware-vulnerabilities-in-ios-ipados-12-5-5-for-old-iphones-and-fixed-more-vulnerabilities-in-ios-ipados-15-0-detect-prioritize-using-vmdr-for-mobile-devices), although iOS 14.8 already patched the FORCEDENTRY vulnerability.
[63] https://index.hu/techtud/2021/11/24/apple-nso-per-pegasus-botrany/
[64] https://googleprojectzero.blogspot.com/2021/12/a-deep-dive-into-nso-zero-click.html

this vulnerability Pegasus is able to dodge the BlastDoor security feature, because GIF images are not processed within BlastDoor in the iMessage application. In the course of the attack, a code embedded in PDF in a forged GIF image file is introduced to the iMessage application, which is then processed by the CoreGraphics module instead of the image processor, which has a vulnerability that enables the hacker to run the code with the highest authorisation.

vulnerabilities not only in iMessage, but also in Apple Music[65] or Apple Photo[66], for instance, may enable entry. Amnesty International's investigation report presents evidence, on the basis of which, the vulnerabilities of these applications also enabled "zeroday-zeroclick"-based attacks.
For the Pegasus agent to be able to operate with such high authorisation and to be integrated between the kernel of the operating system and the applications, it had to bypass both the Android and iPhone defence systems and security functions. Such steps may be taken by the users themselves (rooting or jailbreaking[67]), but Pegasus is able to do this remotely and imperceptibly.

Although the Pegasus agent may be installed on the device of the victim in several ways, the "zeroday-zeroclick" method, i.e. the exploitation of unknown vulnerabilities without interaction, total compromising carried out remotely and imperceptibly (rooting or jailbreaking) best demonstrates the true capabilities and value of the NSO technology and the underlying human resources available to them[68], as well as the risk, which it may cause to devices and users.

The devices affected

According to our current knowledge, the Pegasus agent is able to compromise the iPhone iOS operating system and the device up to iOS 14.8 i through the vulnerabilities of the given system or the applications. So, it is not the type of the device, but the version of the operating system and the applications and the vulnerabilities that can be found and exploited in them that determine which devices can be hacked using the remove "zeroday-zeroclick" methods.

The NSO product presentation document dated around 2013 details the capabilities of the agent providing the list of supported devices and operating systems. The 2013 NSO document includes iPhone 4, 4S and iPhone 5 devices up to iOS 4 and iOS 6.1.4 operating systems. The reports by Amnesty International and Citizen Lab reveal that Pegasus is able to infect modern devices with more advanced operating systems, for instance iPhone 11, iPhone 12, iPhone 12 Pro Max, iPhone 6S and iPhone SE 2 devices through the vulnerabilities found in their operating systems or applications. The FORCEDENTRY vulnerability concerned every iOS version below iOS 14.8[69], i.e. practically every more modern iPhone device became affected.

The 2013 NSO document mentions Android (2.1-4.2), BlackBerry (5.0-7.1), Symbian (S60

---

[65] „5. Apple Music leveraged to deliver Pegasus in 2020"
[66] „3. Pegasus processes following potential Apple Photos exploitation"
[67] There are well-known procedures for the implementation of rooting or jailbreaking in both the Android and the iOS worlds. It is not a simple solution even for the owner of the device which is usually applied to enable the user to access the non-accessible functions of the device, or to install applications outside the ecosystem of the given manufacturer, or to be able to use functions or applications, the security functions of the device would not allow.
[68] In terms of value, it is worth considering that Zerodium, one of the leading actors in the vulnerability brokerage market, pays as much as 1.5-2 million dollars "to researchers" for a vulnerability enabling remote jailbreaking.
[69] It also affected certain OSX and watchOS versions.

OS9, Symbian 3 and other versions) devices and operating systems as supported ones. The technical annex to the leaked 2015 NSO contract includes the 7.x-9.1 iOS, 4.x-5 Android, and 5.x-7.1 BlackBerry devices among those supported. Amnesty International's investigation report discusses the 15 Android-based devices examined by them, in whose case it was established that the Android operating system does not store the information needed for the examination, hence in the case of the Android devices they were unable to find unambiguous evidence of successful infection. However, in three devices they found text messages, which were associated with the text message-based propagation vector of Pegasus, i.e. in these devices the attempt at hacking was identifiable.

During the period of the Trident vulnerability chain affecting iOS, news related to Android devices being affected appeared in a broader range (although it was known based on the NSO document that Pegasus had had a capability to infect Android devices too). During this period, Pegasus' Android-based version was known under the name Chrysaor, which was first analysed by Lookout, a company dealing with the security of mobile devices[70]. It was a similar application in terms of capabilities, but in the case of Android, installation did not necessarily require unknown vulnerabilities and "zeroday-zeroclick", because rooting could be achieved more easily on Android devices[71]. It was easier for Pegasus in the case of Android because there was a possibility to request the user's permission during installation as it is done by other malware and APK packages, so it was going to work even if rooting was unsuccessful on the device. In 2017, Lookout and Google found a few dozen data subjects[72], whose Android devices were infected by Pegasus (or Chrysaor).

Capabilities

Although IOS and Android are substantially different operating systems, Pegasus obtains full authorisation for both operating systems, i.e. the confidentiality and integrity of all data and processes is degraded to zero. If the Pegasus agent is successfully installed on the device, text message records, contact lists, call logs, calendar entries, e-mails, traffic from messaging applications, browsing history, favourites, ie. all the important data stored, are retrieved[73] and the Pegasus agent sends the data to the control server[74].

The passive monitoring function of the agent ensures that following the initial data download all new data records be sent to the control server. This function can be used in real time mode, i.e. whenever new data appear on the device, they can be forwarded immediately, but it is possible to specify special scheduling conditions, so that data be forwarded only at certain intervals, or upon meeting other conditions. This function enables, for instance, cell information-based tracking of the location of the device.
The agent has an active data collection function, which provides data from the devices upon the manually launched queries of the operator running Pegasus . In such a case, therefore, the operator requests data from the infected device, which can be, for instance, location data based on GPS information, or files stored on the device; this function, however, is responsible

[70] *https://www.lookout.com/blog/pegasus-android*
[71] In 2017, this was, for instance, the Farmaroot method and application.
[72] *https://www.techtarget.com/searchsecurity/news/450416359/Pegasus-malware-expands-from-iOS-to-Android*
[73] The 2013 NSO document calls this the "*Initial Data Extraction*" function.
[74] The data are not sent directly, but to an anonymisation network, which then forwards them to the infrastructure of the Pegasus operator. The purpose of the interim network is to cover up the operator's servers and network.

also for switching on a microphone and recording sound, for wiretapping calls, making photographs, video recordings and recording screenshots. According to the 2013NSO document, call interception was supported only in the case of Android devices, but this function appeared also for iOS and BlackBerry devices in the technical annex of the leaked 2015 contract.
The developers paid great attention also to small matters. For instance, when the operator takes a photo using the front or back camera of the device through active data collection, the camera does not use a flashlight, thus the user has no idea that the device made a photo.
The leaked 2013 NSO document shows how the microphone was switched on and the sound recording was made at the time. An Asterisk PBX IP phone exchange was also included in the infrastructure of those days (a background system operating on the side of the Pegasus operator and the NSO client). When the microphone is switched on, the IP phone exchange functioning at the operator called the phone number of the victim, but the user was unable to perceive this call and the automatic recording of the call. If the device was active, because the user was just using it and the screen was on, this function could not be used because the moment that the user began to use the device, for instance by switching on the screen, the call was immediately broken and the data captured till then were erased. In the newer Pegasus versions, presumably this function no longer requires the IP phone exchange; the Lookout 2017 analysis shows code parts, on the basis of which it can be presumed that a much simpler and much more effective microphone-based wire-tapping was implemented.

Through the agent, the Pegasus operator has access to all the files stored in the internal memory of the phone, and eventually on the SD card. The operator may request the list of libraries and files, and on that basis, it may request any file from the device, which then the agent forwards to the control server.

When analysing the Android version of Pegasus in 2017, Lookout called attention to the keylogger function. This function was not included either for the Android or the iOS-based devices in the 2013 NSO document; it is possible that this is a new function. Lookout's analysis of 2016 did not document keylogger function in relation to Pegasus run on iOS and the leaked contract of 2015 refers to this function only for Android.

The Pegasus agent is able to retrieve the passwords of the users, as well as send a list of the WiFi networks seen by the device and the keys to the WiFi networks saved to the control server.
In terms of the various chat applications (Skype, WhatsApp, Viber, BlackBerry Messenger) the 2013 NSO document speaks only about the text of conversations and file transfers (even the Ghana contract of 2015 refers to several chat applications and not to recording calls), however, Lookout1s analysis of 2017 also called attention to the possibility of recording calls in the case of Skype, WhatsApp and Viber.

Installation vectors, propagation

Based on Amnesty International's report and Citizen Lab's earlier examinations, the attacks starting with text messages containing a link to the malicious page in the period 2016-2018 began to be replaced by attacks exploiting the vulnerabilities of iMessage and other applications by 2019.

After compromising devices through the Trident vulnerability in 2017, NSO invested substantial resources into the development of "zeroday-zeroclick" methods that the investigation reports basically deal only with remote penetration, and even the examination methodology of Amnesty International focuses on this.

Possibilities of remote penetration:

- *The phone automatically downloads the necessary link through WAP/Push messages without any interaction by the user. In the 2013 NSO document, this is referred to as "Over-the-Air", however, with the termination of WAP this form of hacking went out of fashion.*
- *Text message, e-mail or other message with misleading content and the link to the malicious site, where the device is hacked[75] and the Pegasus agent is installed. Earlier, several Amnesty International and Citizen Lab reports documented the text message-based propagation vector, for instance, in 2016 Ahmed Mansoor received the link to the malicious site in a text message[76], but text message-based delivery was used successfully in 2017 and in 2018[77]. There are several examples of text message-based delivery in Annex "D" to Amnesty International's investigation reports, one of the data subjects (INHRD1 – SAR Geelani) received 3 text messages on close consecutive days in February 2018, then 8 messages in April and 5 messages in May.*
- *Through the vulnerability of an application or service, such as WhatsApp, iMessage, Apple Music, etc. using the "zeroday-zeroclick" methods. As from 2019, clearly this form of attack is the most characteristic. According to the Amnesty International report, most of the examined iPhone devices were compromised through the vulnerability of the iMessage application.*

The product presentation of 2013 leaked from NSO presents two additional possibilities for installing the Pegasus agent:

- *Devices can be compromised also using tactical and network elements. 2013 The NSO documents also mentions the method under the name "Tactical Network Element", whereby the phone number of the target can be obtained using the portable base station developed by NSO and the Pegasus agent may be entered remotely. At the Paris international conference of Milipol in 2019[78], NSO presented a portable base station (BTS) developed by them and installed in the back of a van. The device emulates a legitimate mobile cell tower and forces mobile devices to connect to it within a given area. The hacker may manipulate the GSM traffic of the connected devices, which enables it to install the Pegasus agent on the device remotely. This method was mentioned already in the 2013NSO document , however, with the integration of Circles, which developed similar mobile device wire-tapping technologies from 2008, this technology may have advanced substantially.*
- *The possibility of physical installation was also raised by the 2013NSO document. If the hacker has access to the mobile device, he can install the Pegasus agent in less than 5 minutes according to the document. Following manual installation, the agent*

[75] *The malicious site contains an exploit code, which when run is capable of rooting/jailbreaking the device, then it can install the Pegasus agent on the device using high privilege code running.*
[76] *https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/*
[77] *https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-appendix-d/*
[78] *https://www.milipol.com/Invisiblegoogle/Catalogue-2019/Liste-des-exposants/NSO-GROUP*

functions just the same way and provides just the same services as the remote installation described earlier. Other information is not available in relation to the manual procedure, for instance, about how to bypass the screen lock, presumably however this is the method least frequently applied.

Hiding, ability to survive and self-destruction

Once installed, the Pegasus agent hides its operation as it functions at the kernel level of the operating system, its activity is virtually imperceptible for the user, at most the increased data traffic may betray that a fairly substantial exfiltration is taking place in the background.
Although the Pegasus agent endeavours to operate invisibly, yet this may precisely lead to its exposure. In the course of the attacks against WhatsApp users, what made users suspicious was that they saw an incoming call with the signal for a not received call being shown, and then later, the signal for the not received call disappeared, because it was deleted by the Pegasus agent.

The technical annex to the leaked 2015 contract details the ability of the installed Pegasus agent to survive. As an installed application, the agent remains operational after restarting the device, and blocks the automatic updating of the operating system, although it was noted that users could still update the OS manually. The agent was able to tolerate the resetting of the device to its default settings in the case of Android operating systems and it still remained operational.

In the case of the later Pegasus versions, Amnesty International's examinations established that in the case of iOS, the malware was no longer persistent after restarting the device, the hacker had to infect the device again. Citizen Lab identified the spyware application Predator by Cytrox, a North Macedonian company, with activities similar to NSO, in December 2021[79]. Predator exploits unknown application vulnerabilities, but is not able to infect using the "zero-click" method; similarly to earlier versions of Pegasus, it needs user interaction, the user's click on the malicious link. Predator's functionalities are similar to those of Pegasus, but it is able to survive the restarting of the iPhone.

The Pegasus agent contains self-destructive mechanisms in the event the agent is unable to communicate with its control server. In such cases, it automatically removes itself after the default 60 days, this time interval, however, can be set freely.

There may be several reasons for the agent not being able to communicate with its control server, for instance, it may be off-line or the control servers are not accessible (switched off infrastructure), or perhaps mobile Internet is switched off and the control server cannot be accessed because of the filtering through the WiFi connection, , etc.

The leaked 2013 NSO product presentation refers to the fact that the agent may self-destruct also if it sees that its operation will be exposed, but it does not detail what conditions trigger this mechanism.

---

[79] *https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/*

The compromising process and the underlying infrastructure

One of the figures of the leaked 2013 NSO document shows how the compromising process takes place in the course of a text message-based delivery. The processes is initiated by the operator, i.e. the staff member of NSO's client by entering the phone number of the target. The operator sends the phone number, i. e. the request for installation. From this point, the system works automatically without any intervention by the operator. The GSM modems or text message gateways functioning within the client's own infrastructure send the message to the phone number of the target; the message contains the link to the malicious site and when it is visited, the Pegasus agent is installed on the device of the client.

This is the point where the question arises that it may well be unlikely that the 50,000 phone numbers obtained by the Pegasus Project originate directly from some central Pegasus infrastructure. The leaked 2013 NSO document contains the blueprint for high-level architecture and a set of requirements concerning the infrastructure to be operated by the client. The figure shows the infrastructure elements on the "Customer side", which the client (or operator) has to operate. It can be seen quite well that the initiation of both targeting and the request for installation starts off on the part of the client in its own system.

Neither this document, nor other analyses contain specific information on, for instance, who, when and where drafts the text of the message in the case of text message-based delivery or who, when and where compiles the malicious site installing the agent. Presumably, this activity also takes place on the client's side as in the case of "Social Engineering" attacks based on misleading, the misleading content (localised and specific to the target) is of outstanding importance, because this content will entice the victim to the malicious site. If the content is not sufficiently attractive, the user will not click on the link and the hacking will be unsuccessful.

In the case of delivery through vulnerable applications (such as iMessage), there is no need for misleading content; however, the infrastructure performing the installation (Pegasus Installation Server) is needed there too. In such cases it can be assumed that what we have here is not servers centrally provided by NSO, but infrastructure operated by the client; the code delivered through the iMessage ecosystem has to be able to download and instal Pegasus agents without any user interaction and imperceptibly to the user; for this, however, it has to connect to the server containing the installer. It does not seem to be lifelike that a secret service or other government agency[80] performing similar activities would share even the least of information with a third party.

NSO firmly stated on several occasions that they only sell the technology, its use and operation are the responsibility of the client; however, according to WhatsApp, NSO operated the infrastructure through which the earlier "zeroday-zeroclick" attack took place affecting 1,400 users. The accessible court material reflects the wording that according to WhatsApp, the attacking activity was carried out by NSO[81], thus it cannot be clearly determined, based on the contradictory and somewhat vague information what the role of NSO and of the client was in

[80] *According to the statements of NSO Group, it sells the solutions under controlled circumstances and only to governments.*
[81] *https://cases.justia.com/federal/appellate-courts/ca9/20-16408/20-16408-2021-11-08.pdf?ts=1636394536*

the hacking process. This issue is of outstanding importance, because if devices centrally operated by NSO also participate in the hacking processes, NSO can have access to information about the activities carried out by the operator, such as the persons under surveillance or even the data collected by them.

What seems to be certain at this moment is that the leaked 2013 NSO document and the signed Ghana contract of 2015 document infrastructure operating at the client; this, however, may have been modified substantially with the development of the technology and changes in the installation vectors in the meantime.

For the client-side infrastructure, the leaked contract and NSO's earlier product demonstration set out detailed requirements.
According to the 2013NSO document, 5 servers, 10TB storage capacity are required and the necessary GSM modems, UPS, PBX devices and other network equipment are needed for the operation of the system. The figure showing the hardware environment shows the image of 42U rack cabinet, of which the required hardware environment takes up only 23U space.

The contract of 2015 specifies the required equipment in much more detail and also includes an offer for the commissioning of the equipment. The technical annex to the contract includes 5 Dell servers in various configurations (altogether with a storage capacity of close to 10TB), 3 CISCO firewalls, 4 CISCO switches, 9 Cinterion GSM modems, 15 Dell workstations (presumably operator's workstations), 30 Dell monitors, 2 APC UPS-s, etc. The contract also covers the software environment, including 6 socket licensing Veeam virtual backup systems, 2 Windows 2012R2 licenses, 2 MS SQL 2014 licenses and the Nagios Enterprise licence for system supervision. The contract also mentions that the contracting party is able to deliver these or equivalent equipment.

Based on these two documents, the servers responsible for the installation of the agents operate on the client's side and the direction, configuration and updating of the agents is also implemented from these servers. The servers, which receive the data obtained from the infected devices, the GSM communications modules or text message gateways that store the collected data and the operator work stations enabling the operation of the system, operate at the client's side.

Although the 2013 NSO product presentation does not include it, the Ghana contract of 2015 expands the information related to the Pegasus background system, adding an additional infrastructure element, which presumably justifies the earlier analyst opinions, according to which currently Pegasus is the most advanced spyware and cyber espionage application.

The technical annex to the NSO Ghana contract mentions that one or more SS7 gateway devices can be placed with one or more local mobile telecommunications service providers in the course of installation. This means that Pegasus' background system and the operator can connect to the interconnect network of the mobile service provider or providers, which ensures for instance roaming between service providers and enables service providers to query information from one another's HLR.

Through this connection, Pegasus' operator acts on behalf of the service provider with whom the SS7 gateway was placed, so all the HLR queries initiated by it, or any other

telecommunications request or transfer (for instance, sending text messages, request for redirecting calls, etc.) will take place on behalf of the mobile service provider concerned. Through the SS7 gateway, Pegasus' operator can search the HLR of every service provider, with which the mobile service provider concerned has a roaming agreement, or authorise HLR searches in one another's systems.

The connection can also be used by the roaming partner to request a valid device (session) authentication key from another service provider with reference to the fact that the given device is in its region and the authentication key is needed because of domestic roaming. The session authentication key may be set up in NSO's mobile or other base station hacking purposes; thus the victim's radio traffic may be unencrypted at the base station, the GSM data traffic (or the 2G, 3G[82] data traffic) can be wire-trapped and manipulated[83].
Under special circumstances, advanced secret services use such technology; here, however, this function appears as the operating capability of a private company which integrated with the Pegasus system lends NSO's clients signal-based wire-tapping and manipulation capabilities. In the contract, NSO reminds the client to use this capability only in particularly important cases, not to send too many requests, because once this activity exceeds the various service providers' limits, it may generate alerts.

Indeed, mobile service providers pay increasing attention to the traffic in the interconnect network, they began for instance to apply SS7 protocol firewalls and anomaly sensors, however, the advanced defence functions appear at the service providers only slowly and cumbersomely as the priories of the availability and continuity of operation are much higher than that of introducing such security solutions. Limit values are of a different order of magnitude than the volume of traffic administered through the SS7 implant, thus the rare and minor volume traffic has a good chance of slipping through the defence.

It is rather difficult to place and develop the SS7 implant or other signal-based hacking or intercepting devices and/or other grey zone connections within the European Union or in the systems of mobile service providers operating in democratic countries. This is possible only if the government of the given country has a substantial say in the operation of the service provider (for instance owns the mobile service provider, or has a majority holding in it), or is able to exert great pressure on the given service provider using other methods[84].

The NSO contract also contains a reference to this, if there is no possibility for deploying SS7 gateways with the local service providers, it is possible to use cloud SS7 gateways (as another external service), but in such cases loss of functionality may occur. The NSO product presentation and the leaked Ghana contract reveal that NSO is responsible for the installation of the hardware and software for the Pegasus background system, and the development of an

---

[82] 4G does not use SS7, but the Diameter protocol. There are units of equipment similar to the SS7 gateway or implant devices with which the functions can be implemented.
[83] If the target device belongs to a US or Israeli citizen, the system may not, and does not, request 3G keys.
[84] In 2004, for instance, in the course of events that have become infamous as the Greek "Watergate", the United States, exerting pressure on the Greek government, achieved that the Greek government got Vodafone of Greece to authorise access for the Ericson centre for legal and lawful interception during the Olympics. The purpose was to protect the Olympic Games and combat terrorism, however, the USA "forgot" to remove the hardware and the installed software after the end of the Olympic Games, and even secretly installed malicious code into the system and began wire-tapping the leaders of the Greek government, for instance, the prime minister. Source: https://theintercept.com/2015/09/28/death-athens-rogue-nsa-operation/

operational environment ready to be used, but in the Ghana contract of 2015, NSO also offered an option for the delivery of hardware.

The 2013 NSO product presentation breaks down the installation of the system into various phases of 10-15 weeks commissioning, where the transfer of the operational system and testing by the client where to take place on the 15th week. The service includes two weeks of training[85], where operators can get to know the architecture, operation and operating tasks of the system and its use, and they can participate in practical simulations. Training may take place at the premises of the client or any place designated by it, but NSO's central office may also administer the training. The Ghana contract of 2015 also includes training as part of the service, also for a period of two weeks, and the duration of the handover process of the system was also specified as requiring one-week on-site activity on the part of NSO.
The documents reveal that NSO provides integration services similar to commercially available corporate solutions in, from this point of view the delivery of the Pegasus system is just like any other complex corporate IT infrastructure delivery and implementation[86]. As part of the service, the NSO provides ongoing product follow-up and updating, Service Desk/Help Desk services and support and specifies its warranty conditions, as well as SLA-based availability. The fee for product follow-up and support is 22% of the entire project fee, payable annually[87], which also corresponds to pricing characteristic in the case of corporate solutions.

Based on the details of the various support levels and debugging activities, it may be assumed that NSO's support engineers get remote access to the systems operating at the client or already have such access in order to carry out these activities. In relation to this, the question may arise whether NSO may have access to the data stored in the system through the deep-level technical support and the necessary access (whether temporary or periodic). This is so in the case of traditional external corporate IT support, and that is why such access is controlled by the more security-minded organisations that are more mature from the viewpoint of IT security, for instance, by monitoring support activities even by recording the activities on video[88].

The Transparency Report issued by NSO[89] contains a statement[90], which according to the Darknet Diaries professional podcast [91] raises the possibility that NSO can have insights into the data of the clients under certain circumstances. The host of the podcast and John Scott-Railton, the head of Citizen Lab's NSO research, discussed that clients are under an obligation to provide data to NSO in relation to the use of the product.

The transparency report indeed includes such a statement but in the context that NSO may launch an investigation against the given client, if suspicion of the unlawful use of the product arises. In such cases, the client must provide information, for instance, the data of the system log files, or even data related to targeting specific targets. Refusal to provide this information

---

[85] According to the plan, from the 12th week to the 14th week.
[86] Naturally, there may be deviations, for instance, the preconditions of installation include a bank card with a credit of USD 4,000, which cannot be associated with the client, and the scanned passport of the holder of the bank card, which can also not be associated with the client.
[87] Altogether, the total value of the contract is USD 9.7 million.
[88] Handling special privilege users (PIM), session / recording.
[89] https://www.nsogroup.com/wp-content/uploads/2021/06/ReportBooklet.pdf
[90] "The customer is contractually required to provide this information which is maintained in the customer's systems logs in a tamper proof manner."
[91] https://darknetdiaries.com/episode/100/

leads to the immediate suspension of the right to use the system. Shalev Hulio, NSO's CEO, mentioned in several interviews[92] that in the event of the suspicion of abuse, they carry out investigations with the clients, hence he was quite certain that the list containing the 50,000 phone numbers cannot come from the clients and that the 37 examined devices mentioned in Amnesty International's report were not among the targets.

Anonymizer and proxy network

The installation of the Pegasus agent is the task of the Pegasus Installation Server, which according to the 2018 analysis by Citizen Lab[93] takes place from the infrastructure of the client or operator. However, the Pegasus agents on the infected devices do not communicate directly with the control servers and the infrastructure of the client or operator. The reason for this is that NSO and the client endeavour to hide the underlying systems, so as to prevent the possibility of direct association between the infected device and the client conducting the surveillance. To this end, an interim communication and data transfer stratum was developed, termed the Pegasus Anonymizing Transmission Network (PATN).

For instance, a click to the link in the misleading content received by text message directs the browser of the device to websites with external VPS service providers (such as Amazon, DigitalOcean, etc.). The servers direct the browser through a chain of additional proxy servers to the Pegasus installation Server at the operators. The use of several intermediary servers excludes the possibility of associating the activity with the given client.

The server installing the Pegasus agent examines various characteristics of the request and the device to determine whether it is at all supported for the infection. If the device is supported, the installing server sends the appropriate exploit code to the device through the anonymizing network and makes an attempt at infecting. If this is unsuccessful for some reason, it redirects the browser of the device to fake or legitimate website specified by the client, so that the user should not meet error messages or other suspicious phenomena on the basis of which he could perhaps recognise being subject to hacking.

Once the Pegasus agent has been successfully installed (or launched) on the target, i. e. the device has been infected, the Pegasus agent starts communicating with the control server and starts monitoring and intercepting, transmitting and processing data. The control server works separately from the infrastructure implementing the infection, presumably in the infrastructure of the client. In the course of the early examinations by Citizen Lab, they covered the anonymizer infrastructure and, through it, they got to the systems of the operators or clients. Amnesty International collected the addresses and other indicators characterising the evolutionary stages of Pegasus and PATN[94]. Until 2021, they identified a total of 1,406 domain addresses, 17 e-mail addresses and 75 malicious device processes.

In the case of PATN, it can be assumed that NSO operates these web and domain addresses as the 2013 NSO product presentation laid down that anonymization addresses serve only a

---

[92] For instance: https://www.forbes.com/sites/thomasbrewster/2021/07/22/nso-group-ceo-defends-1-billion-spyware-company-against-pegasus-project-hacking-allegations/?sh=3a8e0be6472d
[93] https://citizenlab.ca/2018/07/nso-spyware-targeting-amnesty-international/
[94] https://github.com/AmnestyTech/investigations

single client (at any one time?) and this clause would not be necessity in the document, if the client were to operate these addresses, because obviously the web and domain addresses operated by the client serve only its own targets. Presumably, the anonymization addresses to be used for a given infection and communication process can be selected and reserved addresses cannot be chosen by other clients. An earlier report by Amnesty International may indicate operation by NSO[95], when it mentions that they examined the registration dates of domain addresses and found that the vast majority of domains were registered between Sunday and Thursday, which corresponds to the Israeli working week (adding that naturally there may be similar working weeks also in other countries). So, there are signs that indicate that NSO is responsible for the operation of PATN; it cannot be excluded however that clients can also create such addresses used for anonymization purposes as referred to by the 2018 report of Citizen Lab[96].

The possibility to intercept and detect Pegasus

If already installed (or launched), the activity of the Pegasus agent is virtually imperceptible for users, however, iOS devices carry out system logging, in which signs of Pegasus activity can be detected by digital trace analysis and, it is possible to detect some of the signs indicative of infection in the case of Android devices as well[97].

Digital trace analysis is a complex technical and administrative process based on documented and attested examination methodology, which consists of recording the digital traces, exploring the digital traces (activity, event data, logged data, process information, file characteristics, data content, transaction data, traffic data, dates, etc.), searching the connections between the information collected, their analysis and evaluation and the preparation of the report on digital trace analysis.

In other words, digital trace analysis is the reconstruction and technical/scientific examination of past digital events that have already taken place, providing answers and evidence of whether or not an event or activity has taken place, why, when and how it took place, what was its extent, what processes were affected, etc. It is an important criterion that the examination can be reproduced, thus it can provide attested evidence whether the activity or event under study has taken place.

Citizen Lab confirmed the results of the research by Amnesty International; based on the document they published,[98] they found Amnesty International's methodology to be sound and the results of their examination correct, and both organisations found the same results in the course of their examinations independently of one another.

Although neither the Pegasus Project, nor Amnesty International disclosed the source through

---

[95] https://www.amnesty.org/en/latest/research/2018/08/amnesty-international-among-targets-of-nso-powered-campaign/

[96] "The domain names often resolve to cloud-based virtual private servers (we call these front-end servers) rented either by NSO Group or the operator" Source: https://tspace.library.utoronto.ca/bitstream/1807/95391/1/Report%23113--hide%20and%20seek.pdf

[97] According to Amnesty International, Android devices do not log and stored the information on the basis of which the presence of Pegasus can be credibly established.

[98] https://citizenlab.ca/2021/07/amnesty-peer-review/

which they had access to the list containing 50,000 phone numbers, or the list itself, the independent investigations of the French and the Belgian governments confirmed the results of Amnesty International's investigation in relation to Belgian[99] and French[100] data subjects.

Amnesty International issued a free Mobile Verification Toolkit (MVT[101]), which can be used to verify whether the device was in contact with the Pegasus spyware.

Amnesty International made an IoC[102] database available to the MVT application, whose elements[103] are searched by the MVT tool on the device and a match or hit shows whether the device was in contact with Pegasus. The database contains the domain and e-mail addresses discovered in the course of the investigations related to the operation of Pegasus in the period 2018-2021, as well as the process and file names identified in the infected devices.

The use of MVT requires fairly substantial expertise, however, iMazing[104] implemented the functionality of the MVT tool in its own application, with which practically anyone is able to check his or her own phone by some simple clicks. Both applications use Amnesty International's IoC database for the searches.

Protection against Pegasus?

In Pegasus' earlier evolutionary stage between 2016-2018, user interaction was necessary for infection. It was necessary to click on the links in the text messages, e-mails or other messaging applications for the user to be connected to the server installing the Pegasus agent. In such a case, users' security awareness meant protection, if the user did not click on the link in the message received from an unknown source, and the attack may have been thwarted. However, a well-structured Social Engineering attack based on misleading is able to manipulate the victim to finally voluntarily breach the norms of security awareness and click on the malicious link. In the case of devices where Amnesty International was able to demonstrate the traces of successful "one-click" attack, the Social Engineering manipulation proved to be stronger than the users' awareness of security.

Keeping the operating systems of the devices up-to-date did not protect the user, because even if the device's operating system was up-to-date, it was in vain, if its vulnerability ccould be exploited. Apple, however, very quickly published the necessary patches, having examined the case and produced the patch, the installation of the update now provides protection against Pegasus infection.

If a citizen walks around the street carrying millions of forints in cash in a see-through bag, sooner or later there will be someone who will attempt to grab the bag. The more spectacular

---

[99] Forensic traces for FRJRN1&FRJRN3 – Lenaig Bredoux, Edwy Plenel – Source: https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-appendix-d/
[100] Forensic traces for BEJRN1 – Peter Verlinden, Journalist - Source: https://www.amnesty.org/en/latest/research/2021/08/appendix-e-pegasus-forensic-traces-per-target-identified-in-the-aftermath-of-the-revelations-of-pegasus-project/
[101] Mobile Verification Toolkit - https://github.com/mvt-project/mvt
[102] Indicator of Compromise
[103] https://github.com/AmnestyTech/investigations/tree/master/2021-07-18_nso
[104] https://imazing.com/guides/detect-pegasus-and-other-spyware-on-iphone

the bag and the more money there is in it, the greater the probability that an attack will take place. The basis of defence against cyber-attacks is that the user or the organisation concerned reduces its exposure to attacks and attempts to mitigate the extent of possible damage to an acceptable level, i. e. it introduces and applies defence measures proportionate to risks.

In addition to keeping the device up-to-date, such a protective measure to reduce the risk is the protection of mobile devices against malicious codes in the case of Android mobile devices. The anti-virus or anti-malware applications run on Android devices may be capable of intercepting the signature of the Pegasus agent (as a file), so they may be capable of preventing the installer from starting and running. However, they do not necessarily intercept the concrete attack itself, the exploitation of the vulnerability and the remote running of the code; the code of the Pegasus agent must be downloaded and started in order that, at the level of files, the signature could be recognised using the database. Several anti-virus manufacturers published that their mobile security applications protect against the Pegasus infection.

The protection of the Android mobile devices against malicious codes is significantly different from the traditional virus protection tools running on computers. The virus protection functionality of a computer is much broader, but the available resources of mobile devices do not make it possible to carry out resource- intensive and sophisticated tests, thus they largely rely on signature-based recognition. A disadvantage of signature-based recognition is that the security application will recognise the malicious file only if the manufacturer has already met the file and made a signature of it, which means that only the already known Pegasus variants can be recognised in this way. If the file changes even just a little, its signature will not correspond to the signature known to the manufacturer and the virus protection will not recognise the file.
In the case of the iOS platform, classic virus protection cannot be implemented. The reason is Apple's closed ecosystem; applications can only be installed to iOS devices from the Apple Store, and only the applications that have been strictly examined by the manufacturer and therefore regarded as secure by Apple can be placed there[105]. Another problem is that in the case of iOS, applications work in sandboxes, fully closed off from one another, i. e. no application is able to exit its own environment, hence they are unable to check one another's operation or to intervene in processes running in another separate sandbox. If, however, an application is still able to get out of the sandbox, there is no protection or control over its activity. That is what Pegasus utilised.

Based on Pegasus' capabilities, it can be said that users can do very little against "zeroday-zeroclick" attacks. It is worth dividing the defence options into two groups.
The first group includes general cyber hygiene skills, which should be utilised by an average everyday mobile device user to protect his own personal and other important data, and to reduce the exposure arising from presence in the Internet or the use of the mobile device, quite irrespective of Pegasus.

Such measures reducing exposure may be, for instance:

---

[105] That is why remote jailbreak is needed for installing/launching the Pegasus agent, which enables bypassing this protection and operation close to the kernel.

- *Removal of the applications not used because fewer applications mean less vulnerability.*
- *Applications should be installed only from secure sources (Android, Google Play).*
- *Checking the content of messages and links. Disregarding messages coming from unknown sources.*
- *Checking abbreviated URLs (for instance copy them into the ExpandURL service, which reveals the address pointing to the actual website).*
- *In the case of strange messages coming from acquaintances that look like spam, it is worthwhile to ask through another channel of communication whether they were indeed sent by the acquaintance.*
- *Using a browser other than the default browser preferred by the operating system. In many cases, web attack codes are written for the default browser, in such cases the attack may be thwarted because the user uses a different browser[106].*
- *Keeping the operating system and the applications up-to-date, installing the patches.*
- *Regular checking of the installed applications, checking and withdrawing application authorisations.*
- *Restricting physical access to the device, screen lock, password protection, using PIN codes.*
- *Making backup copies, external checking of the backup copies using anti-virus solutions.*
- *Resetting the device to default settings from time to time, reloading data.*
- *Restarting the device from time to time because the operation of the non-persistent malware is terminated.*
- *Use of security solutions developed for mobile devices (web content screening, virus protection (Android), data annihilation (wipe), SPAM and SCAM protection, checking settings, protection against fraud and data phishing, etc.)*
- *Checking data traffic statistics and major outliers*
- *Avoiding unknown or free Wi-Fi networks.*
- *Use of encrypted communications (HTTPS).*
- *Password hygiene, use of secure passwords, use of two-factor authentication, use of unique password for each access, password manager applications.*

Pegasus and other similarly advanced spyware are not deployed against "average" everyday users. The cost of Pegasus and similar technologies and the cost of interceptions broken down to devices is exceedingly high, therefore a wide range of users may be exposed but not threatened by such advanced technologies.

The other group includes users or organisation in whose case not only their exposure is high, but they also feel threatened. In addition to the general cyber hygiene skills, the following could, for instance, be recommended to them:

- *Implementation of a Mobile Device Management (MDM) system responsible for the central management and secure operation of mobile devices. Containerised encryption. setting unique password protection for applications, device supervision, traffic analysis, etc.*

---

[106] This is also mentioned in the NSO product presentation stating that in such cases the infection does not take place and the user may see error messages.

- *Compartmentalisation, dedicated devices for various applications, storing confidential data or conducting confidential communication.*
- *Use of old type "feature phones" (for voice communication only) – although this will not provide protection against GSM-based interception.*
- *Daily restarting of devices.*
- *Resetting to default, for instance, weekly or monthly.*
- *Encrypting the stored data.*
- *Avoiding the storage of particularly confidential data.*
- *Encrypting data communications through a VPN network.*
- *Using phone cases capable of covering front-facing and back-facing cameras, or using separate camera covers.*
- *Using microphone blockers*[107]
- *Using charge-only USB adapters to charge devices*[108]*.*
- *Use of containers or cases to shield or block GSM and other radio communications of devices ("Faraday Bag")*
- *Frequent replacement of phone numbers and devices.*
- *Periodic examination of the devices with the help of an expert in digital trace analysis or a forensic expert.*

It is recommended to users who feel themselves threatened to use MVT or other tools intercepting Pegasus traces;, however, MVT contains the indicators needed for the establishment of being affected by Pegasus only up to the recent past. For example, following the report of Amnesty International, Amazon shut down the NSO servers associated with their platform, but it can be assumed that the "service" is going to be re-launched elsewhere and at other addresses and MVT (with the current database of indicators) will not be able to identify the new addresses on the devices. Pegasus had earlier been characterised by frequently changing the PATN addresses operating on the public internet, and because of this MVT will not be able to provide reliable information in the future, unless Amnesty International expands its indicator database on an ongoing basis.

V. Findings

V.1.
The application of covert information gathering

First and foremost, the Authority attaches importance to calling attention to the circumstances explored in the course of its investigation launched in the wake of the following statement published in the press and the Hungarian legal situation in force:

According to the Direkt36.hu article published on 19 July 2021:

"Pegasus is considered to be such a serious cyber weapon that NSO may sell it to other

[107] *https://en.wikipedia.org/wiki/Microphone_blocker*
[108] *https://www.usbcondom.org/*

countries only with the permission of the Israeli Ministry of Defence. Officially, it could only be deployed against persons suspected of terrorism and organised crime, but the fact-finding project revealed that the NSO clients in at least 10 countries use it against journalists, human rights activists, opposition politicians, lawyers and businessmen."[109]

The bodies authorised by legal regulation to covertly gather information subject to external authorisation may use special means and methods of covert information gathering to discharge their duties specified by the National Security Services Act. Pursuant to Section 53(2) of the National Security Services Act, they may do so only if the data necessary to discharge their duties specified in the National Security Services Act cannot be obtained in any other way. Sections 4-8 of the National Security Services Act details the duties of the bodies authorised by legal regulation to covertly gather information subject to external authorisation, while its Section 9(b) lays down that the National Security Services carry, inter alia, out the tasks linked to situations of threat of terrorism as specified by law.

Hungarian law in force does not differentiate between professions and professional activities with regard to the conditions for using covert information gathering subject to external authorisation, i. e. it does not restrict the authorisation of the National Security Services to carry out the activities under Section 56 of the National Security Services Act for any profession (e.g. "journalist, human rights activist, opposition politician, lawyer and businessman").

In the course of the Authority's investigation, no information was found that the bodies authorised to covertly gather information subject to external authorisation according to Section 56 of the National Security Services Act would have used the spyware for any purpose other than those specified by the manufacturer (prevention and detection of criminal acts and acts of terrorism), and the discharge of the duties specified by law.

V.2.
The data processing operations of the bodies investigated by the Authority

The technical tool constituting the subject matter of the Authority's investigation is a dedicated software capable of covertly observing the content on the infected device and to ensure remote access to the peripherals (camera, microphone). The tool is capable of covertly surveying the information system, as well as the premises under the covert gathering of information. Based on the data made available to the Authority, it can be established that in Hungary, the Specialised National Security Service used the tool subject to the investigation. The task of the Specialised National Security Service specified by law is to support the work of organisations authorised to use the means and methods of covert information gathering and disguised tools, by way of providing special services. As the central service provider organ of the national security and policing organs, The Specialised National Security Service, as the central service provider of national security and law enforcement bodies, not only has the right, but has the express obligation to ensure the availability of the tools necessary for the discharge of its service provider tasks.

---

109 https://www.direkt36.hu/leleplezodott-egy-durva-izraeli-kemfegyver-az-orban-kormany-kritikusait-es-magyar-ujsagirokat-is-celba-vettek-vele/

According to the information made available to the Authority in the course of its investigation, the Specialised National Security Service used the technical tool subject to its investigation in the course of the provision of its services in the field of the covert surveillance of information systems and premises.

The Authority established that the contractual conditions concerning the use of the technical tool stipulate that the contracting party is to take all the measures to prevent access by any unauthorised external party to the personal data affected by the use of the tool. According to the position of the Authority, the data protection provisions of the contract provide requisite guarantees for this purpose.

No data were found in the course of the Authority's investigation that would cast **doubt on whether the Specialised National Security Service has acted, and is** acting, when using the technical tool, in accordance with the relevant legal regulations, the provisions regulating the organisation of public administration and, in the case of contractual relationships, its obligations undertaken in the contract.
According to the circumstances explored in the course of the Authority's investigation and the information available, the Specialised National Security Service used the technical tool exclusively for the purpose of the prevention and detection of criminal acts and act of terrorism, and to discharge its tasks specified by the relevant Hungarian regulations and has ensured that it is not used for the unlawful restriction of fundamental rights. In contrast to the news published in the press, the Authority's investigation did not find information that the Israeli Ministry of Defence would have forbidden the use of the technical tool for Hungary.

In the cases under investigation, the Authority did not find any unlawfulness with regard to the processing of data by the controllers (ordering organs).
The authorisations of the minister in charge of justice examined by the Authority contained, in each case, the elements of content specified in the National Security Services Act, such as the place and date of covert information gathering, its subject and the description of the authorised tool.
The submissions examined by the Authority contained the legal basis for the order of covert information gathering and the statement of the facts and circumstances, which justify the use of the tool according to Section 56 of the National Security Services Act. The authoriser complied with its obligation to provide justification in accordance with the relevant legal provisions in each of the decisions by the minister of justice examined by the Authority.

The findings of the Authority concerning the investigation of specific individual cases – and the notes made on the individual cases – contain classified data according to Section 7(1) of Act CLV of 2009 on the Protection of Classified Data, thus they will not be detailed in the present summary.

In view of the fact that the International Secretariat of Amnesty International did not make the list, containing the 300 phone numbers referred to in the news as described above, available to the Authority in the course of its investigation, the Authority was not in a position to ascertain its existence or the range of persons mentioned in it.
It follows that in the course of its investigation, the Authority carried out procedural acts in relation to those data subjects whose involvement by the use of the software was made public in the press. It can be established on the basis of the data of the investigation that covert

information gathering subject to authorisation by the court or the minister in charge of justice according to Section 56 of the National Security Services Act was carried out with respect to several of the persons identified as being subjects of the use of the “Pegasus” spyware in the press.

V.3.
The possibilities of legal remedy by the data subjects

In order to enforce their rights in relation to the processing of their personal data, data subjects may submit a notification to the Authority for an investigation to inquire into the lawfulness of the controller's action if the controller restricts the exercise of their rights or rejects their request for the exercise of those rights, and may request the Authority to initiate data protection proceedings if they consider that the controller is processing their personal data in breach of the provisions on the processing of personal data laid down by law or by a legally binding act of the European Union. [Sections 22, 51/A(2), 60(1) of the Privacy Act]

Although the Authority has not received any complaint or request from any of the data subjects included in the press coverage to initiate the Authority's data protection procedure, the Authority is responsible for monitoring and promoting the right to the protection of personal data and has therefore decided to conduct an ex officio investigation.

The Authority's ex officio procedure has an important role to play in facilitating the exercise of data subjects' rights, in view of the fact that in the course of data processing for national security purposes, the data subject's ability to exercise his or her data subject rights under the Privacy Act is limited, as defined in the National Security Services Act. According to Section 48 of the National Security Services Act, the director general of the National Security Service may refuse to provide information on data processed by the national security services or to erase personal data at the request of the data subject, on grounds of national security or in order to protect the rights of others, and the director general may restrict the right of access of the data subject in connection with the classified data of the national security services, as provided for in Act CLV of 2009 on the protection of classified data, on grounds of national security. However, the national security services are obliged to keep records of the requests received from data subjects, how they have been dealt with and the reasons for their refusal, and to inform the Authority annually.

As regards processing for law enforcement purposes, Article 17 of the Criminal Justice Directive obliges Member States to adopt provisions where national law provides for the delay, restriction or suspension of the exercise of the rights of the data subject[110] whereby "the rights of the data subject may also be exercised through the competent supervisory authority”.

Since the rules on data processing for law enforcement purposes laid down in the Privacy Act [111] pursuant to the Criminal Justice Directive apply with regard to data processing for law enforcement purposes – with some exceptions expressly provided for in the Privacy Act –, the data subject may exercise his or her rights in accordance with the above provisions of the

[110] Cf. Criminal Justice Diective, Article 15(3), Article 25(3) and Article 15(4)
[111] Privacy Act Section 2(3)

Privacy Act[112], with the assistance of the Authority, in the event of refusal to provide information pursuant to Section 48 of the National Security Services Act.

Given that more and more names have appeared in the press since the start of the Authority's investigation under the above case number, there are several ex officio investigations in progress and the Authority will continue to carry out ex officio investigations in similar cases, even if the persons concerned do not avail themselves of the possibilities provided to them to enforce their rights.

V.4.
Disclosure of the circle of data subjects as a data protection accident

The Authority's investigation has failed to clarify how the phone numbers that may be linked to Hungarian individuals, which Amnesty International's Security Lab unit found to have been infected by the spyware, could have been disclosed during the so-called Pegasus Project fact-finding investigation.

Pursuant to the principles governing the processing of personal data set forth in Section 4(1)-(3) of the Privacy Act, personal data shall be processed only for clearly specified and legitimate purposes in order to exercise certain rights and fulfil obligations. Data processing must comply with the purpose of processing in all its stages; data shall be collected and processed fairly and lawfully. Only personal data that is essential and suitable for achieving the purpose of processing may be processed. Personal data may be processed only to the extent and for the period of time necessary to achieve its purpose. The personal data will retain this quality during processing as long as the relationship with the data subject can be re-established. The link with the data subject can be re-established if the controller has the technical conditions necessary for the re-establishment.

Pursuant to Section 4(4a) of the Privacy Act, the controller shall ensure adequate security of personal data by applying appropriate technical or organisational measures during processing, in particular measures to protect against unauthorised or unlawful processing, accidental loss, annihilation or damage to data. The controller shall ensure an adequate level of security of the personal data processed and the fundamental rights of the data subjects by implementing technical and organisational measures appropriate to the extent of the risks represented by the processing. In designing and implementing the technical and organisational measures, the controller shall take into account all the circumstances of the processing, in particular the state of science and technology at all times, the cost of implementing the measures, the nature, scope and purpose of processing and the risks of varying likelihood and severity to the rights of data subjects presented by the processing.

The use of the technical means under investigation requires respect for the principles of integrity and confidentiality, including protection against unauthorised or unlawful processing and accidental loss, annihilation or damage, by applying appropriate technical and organisational measures.

While EU law does not apply to processing for national security purposes, the European Data

[112] Privacy Act Section. 22, Section 51/A(2) and Section 60(1)

Protection Board's Guideline 4/2019 on data management principles[113] deserves attention, which sets out among the principles of data protection by design and by default that appropriate measures are necessary to ensure the security of personal data, to prevent and manage data breaches, to ensure the proper performance of processing tasks and compliance with other principles, and to facilitate the effective exercise of individuals' rights. The Guideline requires that information security measures for the protection of personal data and the procedures for handling data breaches are reviewed regularly.

Pursuant to Section 3(26) of the Privacy Act, "*personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised transfer or disclosure of, or unauthorised access to, personal data transferred, stored or otherwise processed"*.

In his opinion described above, the information security expert explained that the circumstances of the data leak are not known, but it can be assumed that data security was compromised in some way, as unauthorised access to personal data can be presumed, so it cannot be excluded that a personal data breach took place.

The Authority's investigation therefore also covered whether a personal data breach could have occurred in the context of the use of the technical tool by the data controllers investigated by the Authority. The Authority's investigation did not identify any information indicating that such a personal data breach had occurred.

The source and content of the "*leaked list of 50,000 telephone numbers*" is unknown to the Authority, but if the "list" has come in the possession of the Pegasus Project organisation or Amnesty International and it contains personal data relating to specific individuals, it follows from the legal provisions that the only way it could have happened was by unauthorised transfer of personal data.

The alleged "list of 300" containing the personal identification data and telephone numbers of Hungarian citizens – which, according to press reports, was made available to Direkt36 journalists by Amnesty International[114] – and which was created from the originally leaked list of 50,000 telephone numbers by some criteria unknown to the Authority – also raises the illegality of these data processing operations. According to the information at the Authority's disposal, it is not clear on the basis of what legal authorisation and for what purpose the organisations mentioned (data controllers) are processing the personal data of the data subjects on the leaked list, which in some cases are presumed to be personal data of a criminal nature, nor how and under what legal framework the personal data of Hungarian citizens came into the possession of a third-country data controller, the International Secretariat of Amnesty International, based in London.

If the third party has unauthorised access to the personal data processed, it is punishable according to Act C of 2012 on the Criminal Code (hereinafter: Criminal Code), several criminal offences may have been committed (e.g. Criminal Code Section 219: misuse of personal data,

[113] EDPB Guidance No 4/2019 on data protection by design and by default according to GDPR Article 25 (Date of adoption 20 October 2020)
[114] „A story fit for a spy movie"– report by the two Direkt36 journalists observed | Direkt36

Criminal Code Section 265: misuse of classified data, Criminal Code 261: spying, Criminal Code Section 423: information system or data breach, Criminal Code Section 424: circumvention of a technical measure to protect an information system).

In view of the above, it cannot be ruled out that a criminal offence has been committed, therefore the Authority will initiate criminal proceedings with the investigating authority pursuant to Section 70 (1) of the Privacy Act.

Although the Authority has not been able to prove or rule out beyond reasonable doubt during its investigation whether a data breach has occurred at the data controllers it has investigated, if the investigating authority's procedure proves that a data leak has occurred and that the cause of the leak was a data breach, the Authority will investigate it.

Budapest, 31 January 2022

Dr. Attila Péterfalvi
President
Honorary university professor

Legal regulations:

- Fundamental Law of Hungary
- Constitutional Court Decision 32/2013. (XI.22.)
- Constitutional Court Decision 2/2007. (I.24.)
- Constitutional Court Decision 23/2018. (XII. 28.)
- The Convention for the Protection of Human Rights and Fundamental Freedoms (Convention)
- Szabó and Vissy vs. Hungary, judgment/ruling, European Court of Human Rights, Strasbourg, 12 January 2016.
- Act CXXV of 1995 on National Security Services (National Security Services Act)
- Act CXII of 2011 on the Right of Informational Self-Determination and the Freedom of Information (Privacy Act)
- Act LXIII of 1992 on the Protection of Personal Data and the Accessibility of Data in the Public Interest
- Act CLV of 2009 on the Protection of Classified Data (Classified Data Act)
- Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016

on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and on the free movement of such data and repealing Council Framework Decision 2008/977/JHA

- Act XXXIV of 1994 on the Police (Police Act)
- Act XC of 2017 on Criminal Procedures (Criminal Procedures Act)
- Act CLXIII of 2011 on the Prosecution
- Act CXXII of 2010 on the National Tax and Customs Administration
- Act CXI of 2011 on the Commissioner of Fundamental Rights
- Government Decree 156/2017. (VI. 16.) Korm. on the detailed rules for the licensing of military technology activities and the certification of companies
- Act XLIII of 2010 on central public administration bodies and the status of members of government and state secretaries
- Instruction 9/2019 (VIII.1) IM on the rules of organisational and operation of the Ministry of Justice
- EDPB Guidance No 4/2019 on the application of Article 25 of GDPR by design and by default, Date of adoption: 20 October 2020
- Act C of 2012 on the Penal Code (Penal Code)