The Protection of Privacy During the Covert Collection of Information for National Security Purposes

Findings of an Ex Officio Investigation

Attila Péterfalvi[*]

Abstract

In 2021 the Hungarian news portal Direkt36 published an article entitled "A tough Israeli spyware was exposed to have been used to target critics of the Orbán government and Hungarian journalists." In the article, Direct36 discovered that "'Pegasus', the spyware of an Israeli cyber company called NSO, suitable for jailbreaking smart phones, was used against targeted Hungarian persons years ago; investigative journalists and wealthy businessmen owning media companies and their close contacts were among the persons targeted. In the course of this research, we found a number of indirect evidence indicating that Hungarian state bodies may be behind the secret surveillance." Based on this information, the Hungarian National Authority for Data Protection and Freedom of Information (Authority) launched an ex officio examination. The article summarizes the findings of this examination, with due regard to the question whether according to the laws of Hungary and the EU, privacy shall be protected during the covert gathering of information.

Keywords: data protection, privacy, Pegasus, national security, external authorization.

1. Introduction

In 2021, the Hungarian news portal Direkt36 published an article entitled "A tough Israeli spyware was exposed to have been used to target critics of the Orbán government and Hungarian journalists." As a part of an international investigative project, Direct36 discovered that

> "Pegasus', the spyware of an Israeli cyber company called NSO, suitable for jailbreaking smart phones, was used against targeted Hungarian persons years ago; investigative journalists and wealthy businessmen owning media

* Attila Péterfalvi: president, Hungarian National Authority for Data Protection and Freedom of Information, Budapest; honorary professor of law, ELTE Law School & Pázmány Péter Catholic University, Budapest.

> companies and their close contacts were among the persons targeted. In the course of this research, we found a number of indirect evidence indicating that Hungarian state bodies may be behind the secret surveillance."[1]

In early July, a journalist of the French *Le Monde* newspaper, also taking part in the investigative project asked Minister of Justice Judit Varga in an interview whether she would authorize the monitoring of a journalist or a member of the opposition. She indignantly answered: "What a question! This is in itself is a provocation!" Varga said that only surveillance requests in compliance with the law may be authorized, adding that "there are so many threats to the state all over". Following the article mentioned above, the Hungarian National Authority for Data Protection and Freedom of Information (the Authority) ordered an *ex officio* investigation.

The article gives an overview of how the Hungarian legislation concerning the protection of privacy during the covert collection of information for national security purposes has changed since the change of political system (1989) and what role the Authority plays 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 enforce their rights under the Hungarian Privacy Act[2] is limited.

2. The Transformation of Relevant Hungarian legislation since the Change of Political System

2.1. Act X of 1990 on the Transitional Regulation for Authorizing Special Secret Service Means and Methods

At its session on 25 January 1990, shortly after the change of regime in 1989, the Hungarian Parliament adopted Act X of 1990 on the Transitional Regulation for Authorizing Special Secret Service Means and Methods. This legislation classified the application of every means and methods as special means if they were applied without the knowledge of the person concerned and whose use infringed the rights to the inviolability of private homes, private secrets, confidentiality of correspondence and the protection of personal data. It was stipulated already in this act that special means may only be applied in case the data cannot be obtained in any other way.

The legislation distinguished between cases in which special means can be applied for criminal acts or for national security purposes even though this term is not used. However, in terms of substance, it listed cases corresponding to national security interests. It was the competence of the Minister of Justice to

1 *See* (in Hungarian) at www.direkt36.hu/leleplezodott-egy-durva-izraeli-kemfegyver-az-orban-kormany-kritikusait-es-magyar-ujsagirokat-is-celba-vettek-vele/. Translation is provided by the author.

2 Act CXII of 2011 on the Right to Informational Self-Determination and the Freedom of Information.

doi: 10.5553/HYIEL/266627012022010001020

authorize the collection of information. The act included a safeguard clause providing that

> "where the application of special means does not give rise to a penal procedure against the person under surveillance, the entity requesting the authorization shall notify the person under surveillance of the measures applied and the data obtained in the course of the surveillance will subsequently be destroyed."[3]

2.2. Act CXXV of 1995 on the National Security Services

Act X of 1990 was repealed by Act CXXV of 1995 on the National Security Services (National Security Services Act). The regulation in force distinguishes between the *covert information gathering authorized (i) by a judge; and (ii) by the Minister of Justice*. In relation to the authorization powers of the minister, the question arises, whether locating the authorization competence within the executive power is appropriate from the viewpoint of protecting privacy. Where a judge authorizes the gathering of information this issue does not arise, since the judge is located in a branch of power separate from the executive.

With regard to the protection of privacy, in addition to the protection afforded by the EU Member States' constitutional, civil and penal law, it is equally important to take into account the ECHR as another source of international obligations, in particular, Article 8. With due regard to the jurisprudence of the ECtHR, *Decision No. 32/2013. (XI. 22.) AB* of the Constitutional Court of Hungary declared that:

> "As the secret gathering of intelligence by necessity excludes the possibility of effective legal remedy, it is of vital importance that procedural arrangements enabling its application provide sufficient guarantees to protect the individual's rights. In view of all this, the application must be subject to three-stage control: when the intervention is mandated, during the implementation of the intervention and following the completion of the intervention. Control will be carried out by bodies that are independent from the executive power. It is first and foremost the permanent and mandatory control that guarantees that the requirement of proportionality is observed in specific cases."[4]

As far as the constitutionality of the secret gathering of intelligence was concerned, the reasoning in *Decision No. 2/2007. (I. 24.) AB* of the Constitutional Court of Hungary gives important guidance:

> "In a democratic constitutional state, the circumstance that traditional means do not prove to be sufficient for successfully combating certain

3 Section 5(2) of Act X of 1990 on the Transitional Regulation of Authorization of Special Secret Service Devices and Methods.

4 Decision No. 32/2013. (XI. 22.) AB, Reasoning [72].

> criminal acts severely violating or jeopardizing the order of society is grounds for making use of the secret gathering of intelligence and the secret collection of data employed as instruments of criminal law. Hence, the restriction of the fundamental rights under scrutiny by way of methods applied in secret procedures cannot be considered as a constitutionally unnecessary means. The protection of the constitutional state and fundamental rights, however, require that the law regulate the procedure for using such instruments in detail and in a differentiated manner. Since the use of secret means and methods constitutes a severe intervention into the life of the individual, they may be applied only exceptionally, as a transitional and last resort."[5]

The ECtHR underlined that

> "precisely because the intervention in fundamental rights is secret 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."[6]

2.3. Bill to Amend the Law

Taking into account that the ECtHR in *Szabó and Vissy* did not consider the external authorization regime of the covert information gathering to be appropriate and declared that Hungary violated Article 8 ECHR, the Ministry of the Interior prepared a proposal to amend the law and issued it for public debate. *This proposal would have institutionalized the power of the Authority to override the authorization of the Minister of Justice*. According to the draft, journalists, Members of Parliament and clerics could be intercepted in the future only if approved by the Authority. The Authority could have monitored the lawfulness of data collection subject to external authorization. The Minister of Justice would have had to forward its decision granting authorization within 48 hours of signing and the Authority would have had 72 hours to render a decision on the issue. Had the Authority deemed that the gathering of information unlawful, and it would have been able to instruct the given entity to stop data collection and erase the data gathered. Whoever would have learned or suspected that an agency conducted covert data collection against him unlawfully, would have had the right to turn to the Authority, which would have had three months to investigate the complaint. If a person was put under surveillance unlawfully, the Authority would have been able to put a stop to this (provided that surveillance was still in progress), and in case it suspected a criminal act, it could file charges as well.

As the President of the Authority, I sent the recommendations of the Authority to improve the external authorization system of covert information collection for national security purposes to the Legislative Committee of the Parliament. In my point of view, the ECtHR judgment cited above, which found that Hungary infringed Article 8 ECHR, in a wider context called

5 Decision No. 2/2007. (I. 24.) AB, ABH 2007, 65, 100.

6 ECtHR, *Szabó and Vissy v Hungary,* No. 37138/14, 12 January 2016.

doi: 10.5553/HYIEL/266627012022010001020

> "attention to the fact that the rapid development of info-communication technology implies dangers also in addition to countless favorable effects: it renders the mass application of secret surveillance increasingly easy, which may be concomitant with other unfavorable social impacts in the longer term beyond intervention in the privacy of citizens. The attention of the public in advanced democratic constitutional states was directed to these problems first and foremost by the documents disclosed by Edward Snowden. Indirectly, the leakage led to the annulment of the Safe Harbor Convention regulating the Trans-Atlantic transfer and use of personal data. The Privacy Shield, which replaced Safe Harbor, reinforced the protection of the personal data of European citizens against secret surveillance by the intelligence agencies of the US and authorized the data protection authorities of the EU Member States to collaborate in the remedy procedures related to these data collections by secret services with a view to protecting the rights of citizens. Beyond this, the Privacy Shield[7] is essential from the viewpoint of our subject matter because the data protection expectations set against the US expressed common European fundamental values, which are naturally governing for European countries when the legislatures of the Member States decide under what conditions secret surveillance is possible and what safeguards are needed to protect the rights of the citizens."

The court procedure did not extend to obtaining the opinion of the Authority resulting in numerous legally and factually incorrect statements which remained unscrutinized in the course of litigation on the external control over the ministerial authorization in the Hungarian regulation. Thus, the ECtHR did learn of the experiences made by the Authority in the course of the independent external monitoring of the covert information gathering activities of the National Security Services.

Pursuant to Article VI(3) of the Fundamental Law, the enforcement of the right to the protection of personal data and access to data in the public interest shall be supervised by the Authority, an independent authority established by a cardinal law, *i.e.* the Privacy Act.[8] Based on the provisions of the Privacy Act, the Authority is an independent supervisory body responsible for the protection of personal data. The scope of the Privacy Act extends to *all the covert information gathering activities carried out by the National Security Services in the territory of Hungary and the Authority is authorized to supervise these activities*. Pursuant to Section 52(1), anyone may turn to the Authority, if in their view any of the Hungarian National Security Services has conducted or is conducting unlawful covert gathering of information, or there is a direct threat of unlawful covert gathering of information.

7 Judgment of 16 July 2020, *Case C-311/18, Schrems II,* ECLI:EU:C:2020:559. The CJEU declared Commission implementing decision (EU) 2016/1250 of 12 July 2016 on the adequacy of the protection provided by the EU–US privacy shield under Directive 95/46/EC of the European Parliament and of the Council invalid.

8 *See* especially Sections 1, 2(1), 38(2), 38(5), and 52(1) of the Privacy Act.

The Privacy Act provides adequate instruments to the Authority to explore possibly unlawful covert information gathering and to take action against any infringement. The rules of the investigative procedure[9] grant authorization to inspect, ask for copies, access data, entry, request information and initiate inquiries similarly to the Hungarian commissioner for fundamental rights' procedure. Section 71 of the Privacy Act sets forth rules which provide access to the necessary data for the Authority in case of procedures expressly affecting the National Security Services.

In addition, the Authority may use the data, including national classified data, accessed in the course of the investigative procedure also in its data protection procedure. As a result, for instance, it may prohibit the unlawful processing of personal data, order the erasure of unlawfully processed personal data, order that information be provided to the data subject, in case the controller had denied disclosure unlawfully, and it may impose fines. These are much stronger powers than that of the commissioner's procedure referred to as independent external control invoked in the ECtHR's judgment.

In its practice of applying the law, the Authority's point of departure is that covert surveillance by its very nature deprives the data subject from recourse to direct legal remedy, hence, independent external data protection control is the key element to the protection of informational privacy in this area. Accordingly, the Authority investigates every complaint or notification concerning covert surveillance received from citizens irrespective of whether the circumstances described in the submission referred to covert gathering of information, or whether the data subject can be informed of the results of the procedure. Annually, the Authority receives roughly 10-20 notifications with this subject matter.

In my opinion I also underlined that

> "Decision No. 32/2013. (XI. 22.) AB and the judgment focus on the preliminary supervision of covert information gathering, *i.e.* external authorization. Preliminary external authorization is one of the elements of the set of guarantees protecting informational privacy, which is important, but insufficient in itself. The procedural order of preliminary external authorization is characterized by tight timeframes, a rather tied supply of evidence (decision has to be made on the basis of a documentation selected, edited and formulated by the entity submitting it), the full exclusion of the public and the absence of the adversary procedure. Because of this, in accordance with the guidance of Decision No. 2/2007. (I. 24.) AB, it is expedient to look at the entire system of control over covert information gathering jointly and in context and seek a legal regulatory solution, which, overall, allows adequate protection against unlawful (unnecessary, disproportionate) surveillance of citizens by the secret services. In other words, a multi-stage (preliminary, interim and subsequent) and multi-agency (internal controls by the National Security Services, supervision by the

9 Sections 52-58 Privacy Act.

doi: 10.5553/HYIEL/266627012022010001020

> parliamentary committee, the entity entitled to external authorization and the data protection authority) control system has to operate adequately in total to achieve the above-mentioned goal."

It follows from its function stipulated in the Fundamental Law and its responsibilities set forth in the Privacy Act that the Authority is responsible for the subsequent control of covert information gathering, including the investigation of complaints and notifications, taking or initiating the necessary measures in relation to covert information gathering whether subject to external authorization or not. According to the Authority's position, therefore, the unity of the subsequent data protection supervisory system should not be disrupted, thus, the investigation of citizens' complaints concerning covert information gathering subject to external authorization should not be delegated to another entity. The safeguard role of subsequent control was reinforced through the amendment of the Privacy Act, on the basis of which the Authority may launch also *ex officio* investigations in relation to covert information gathering.

Several types of regulatory models can apply when the preliminary external authorization system of covert information gathering is transformed. In terms of the independence of external control and the principles of the separation of powers and public law, the transfer of external authorization powers, currently vested in the Minister of Justice, to the court of justice would be an unacceptable solution.

The judgment of the ECtHR, however, allows for an interpretation according to which the preliminary authorization powers of the Minister would be retained. In relation to this, the Authority's recommendations sent to the Legislative Committee of the Parliament in 2016 underlined the following:

> "The results of an earlier data protection investigation carried out using a statistical analysis of several years of data from external authorization procedures for covert information gathering indicated that, in the case of the external authorization powers of the Minister of Justice, single-person decision-making authority may clash with the requirement of informed decision-making. Every year, the directors-general of the National Security Services submit such a large number of submissions that a single person, the Minister, cannot possibly review in sufficient depth before making a decision on authorization. For this reason, should these powers remain within the ministerial framework, in the Authority's opinion, the establishment of a committee should be considered which should be entrusted with the task of screening submissions for lawfulness and necessity, and to put forward recommendations as to whether they can be authorized, prior to ministerial decision-making. The members of this committee would include experts with the necessary special national security knowledge, delegated by government agencies with an interest in the lawfulness of covert information gathering (such as the Ministry of the Interior, National Security Services). This committee would, therefore, not carry out independent external control, instead its role would be to facilitate the lawfulness and the informed

character of ministerial decisions to be made concerning external authorization, thereby fulfilling its role in protecting rights. The regulatory framework for establishing the committee can be created by amending the Act on National Security Services.

In view of the provisions of the judgment, should the minister's external authorization powers be upheld, it is inevitable to subject it to independent external control. From a public law point of view, there is nothing to impede the Authority from fulfilling this role, as it is an independent data protection supervisory authority as specified in the Fundamental Law, and whose powers in any case include the subsequent control of the lawfulness of covert information gathering. The Privacy Act provides the appropriate regulatory framework for the performance of this task, including the investigative authorizations needed to establish the facts of the case and to take the necessary measures in the event of a ministerial decision infringing informational privacy. Essentially, it would suffice to supplement the Privacy Act with the statement that the Authority continuously supervises the lawfulness of the ministerial authorization of covert information gathering."[10]

3. Comprehensive Data Protection Audit of the Covert Information Gathering Activities of National Security Services[11]

The Authority also conducts procedures aimed at facilitating the lawfulness of data processing related to the special activities of the National Security Services. In 2016, upon the initiative of, and in cooperation with one of the National Security Services, the Authority carried out a data protection audit whereby it supervised the lawfulness of the application of the individual means and methods for covert information gathering through practical tests. This activity by the Authority was based on a novel data protection supervisory method unprecedented even in international comparison.

The core of the method developed for the data protection audit of covert information gathering is that in the experimental situations designed by the Authority, National Security Services should carry out their service provider activities related to covert information gathering under circumstances as close to reality as possible.

The Authority examined the entire process of the procedures related to covert information gathering by the National Security Services under circumstances close to reality. Every test started off with the Authority handing over the documentation of the order corresponding to the fictitious facts of the text case to the National Security Services on behalf of the non-existent Civil Surveillance Service, including the service notes completed with fictitious data and the fictitious external authorization in the case of covert information

10 Case No. NAIH/2016/6396/3/J.

11 *See* in detail: Attila Péterfalvi, *25 éves az NBSZ*, Budapest, 2021, pp. 79-86.

doi: 10.5553/HYIEL/266627012022010001020

gathering subject to external authorization. In the course of preparing and implementing the tests, the National Security Service acted in every respect as a service provider within the meaning of Section 8(1)(a) of the National Security Services Act.

The implementation of the test was documented by a designated staff member of the National Securities Service in a protocol. (Incidentally, this would be the Authority's task, but this was the only way for us not have access to information to which the Authority is not authorized pursuant to the provisions of Section 71 of the Privacy Act and which was in any case not indispensable for the implementation of the tests.) At the same time, the staff members of the Authority documented in a memo drafted on the given test whether, as officers of the Civic Surveillance Service, they consulted the staff members of the National Security Service or, for instance, received extraordinary 'operative information' on the fictitious covert information gathering. In this way, the communication and interaction between the National Security Service and the commissioning organization became fully verifiable.

The National Security Service gathered, recorded and processed information in the course of the tests as if it was providing services 'in live mode'. The nature of the documentation handed over to the Authority as a result of the secret information gathering tests (*e.g.* protocol, video recording, sound recording, expert opinion, *etc.*), as well as the degree of information processing, their data content and format were the same as in the case of an actual gathering of covert information. In the period between April 2016 and February 2017, 34 covert information gathering tests were implemented.

The audit clearly confirmed the commitment of the National Security Services for the lawfulness of data processing, at the same time, the tests explored a few details of the activities related to covert information gathering, in relation to which the Authority made observations and recommendations with a view to ensure the enforcement of the data protection requirements at the highest standard.[12]

4. Evaluation of the Hungarian Legislation in Force from the Viewpoint of Safeguards – Investigation of the Use of the 'Pegasus' Spyware in Hungary

Let us now examine whether the authorization of covert information gathering for national security purposes as set forth in the Hungarian legislation in force meets the above criteria and provides sufficient guarantees for the protection of the privacy of the person under surveillance.

Based on the effective legislation applicable to covert information gathering for national security purposes, it can be established that as far as the authorization powers of the Minister of Justice are concerned, there have been

12 Report of the Authority on its activities in 2016, at www.naih.hu/eves-beszamolok?download=22:naih-beszamolo-a-2016-evi-tevekenysegrol.

no amendments to the legislation, thus, the rules in force at present are the same as those on account of which the ECtHR had condemned Hungary.

I, however, find it important to stress that when aligning the Privacy Act[13] with the GDPR[14] the Authority was authorized to initiate an investigation or data protection procedure *ex officio*. This empowers the Authority to launch investigations or data protection procedures to audit covert information gathering for national security purposes *ex officio*. This is the case also in relation to the use of the 'Pegasus' spyware.

From the perspective of the Privacy Act, covert information may be gathered for the purposes of *law enforcement* (prevention, investigation and detection of criminal acts) or for the 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, *i.e.* the Criminal Justice Directive[15] transposed into Hungarian law by the provisions of the Privacy Act, data processing for national security (and defense) 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 GDPR and Recital (14) and Article 2(3)(a) of the Criminal Justice Directive are unambiguous on the fact that the processing of personal data carried out in the course of activities related to national security falls outside the scope of EU law. This means that national security as the subject matter of legislation and the application of the law in this field is, according to EU law, within the exclusive scope of authority of the Member States.

I would not venture to predict how the ECtHR would assess the legislative amendments since 2016 with regard to external control over authorization within the executive power (by the Minister of Justice). However, I find it important to note the depth of the supervision carried out in relation to the use of the 'Pegasus' spyware and the types of documents the had Authority checked.

Pursuant to Section 54(1) of the Privacy Act, in the course of its investigation, the Authority has 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 has the right of access to, and may request copies of such documents, including documents stored in an electronic data storage medium. The Authority may learn about the data processing associated with the case under

13 Sections 20 and 23 of Act of XXXVIII of 2018, in force from 26 July 2018.

14 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).

15 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.

doi: 10.5553/HYIEL/266627012022010001020

investigation, it may enter the premises serving as the place of processing, it has access to the tools used for performing the processing operation and it may request written or verbal 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 investigation, including data stored in an electronic data storage medium not only from the controller, but also from any organization or person associated with the case subject to the inquiry. The controller subject to the inquiry and any other organization or person associated with the case under investigation shall comply with the instruction of the Authority within the period specified by the Authority. (It was on the basis of this provision that the Authority contacted the Amnesty International Magyarország Egyesület, as well as the Amnesty International Secretariat, however, unfortunately they declined to cooperate.)

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 by international comparison. In the course of its investigation, the Authority contacted the data protection authorities of the EU 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. In addition, the majority of the Member States' authorities, which, according to their national law are authorized to supervise data processing for national security purposes, have never carried out an investigation of this kind.

In the course of controlling the lawfulness of external authorization by the Minister of Justice, the Authority examined the submissions in every single case to see whether these complied with the formal and procedural requirements set forth in the legislation.

In this procedure, the Authority examined whether the submission for covert information gathering came from the director general of the National Security Service authorized to covertly gather information and whether it contained 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 scope of the person(s) concerned, and the available data suitable for identification, as well as the description of the covert information gathering (*i.e.* the means and methods to be applied) and the justification of its necessity and the start and end dates of the activity (and in the case of a submission related to an exceptional authorization according to Section 59 of the National Security Services Act, justification that it was indispensably necessary in the given case for the successful operation of the National Security Service).

When investigating the lawfulness of external authorization, the Authority examined whether there was adequate substantiation 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 comparing it with the facts of the case, to established or exclude that the interest of national security prevails. The Authority may investigate 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, even where no interest of national security is invoked. Therefore, it must be examined whether the enforcement of the interest of national security in a 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 in the course of covert information gathering.

The Authority also examined whether there was sufficient substantiation in the submission concerning the external authorization of covert information gathering, that the purpose of data processing cannot be achieved without such intervention, and whether the requested use of the means and methods is necessary. The submission must also to substantiate whether the covert information gathering is indispensably necessary for the requested period, and the Authority examines whether the authorization 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 of Justice reasonably 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 of Justice on the individual submissions.

It is important to examine in the case of every decision whether the Minister of Justice justifies the granting of the external authorization in view of the facts and circumstances detailed in the given submission. *Decision No. 32/2013. (XI. 22.) AB* of the Constitutional Court referred to the obligation to provide justification for the external authorization as a precondition to the enforcement of *ex post* external control by specifying a constitutional requirement. Consequently, the justification must be sufficiently detailed and individualized 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.

On the basis of the legal provisions mentioned, the Authority carried out its examination of the lawfulness of the external authorization in relation to the conformity of nearly one hundred submissions and related decisions of the Minister of Justice. The examination took place along the following questions: *(i)* Were the submissions compliant with formal and procedural rules? *(ii)* Was the submission received from the director general? *(iii)* Did the submission include all

doi: 10.5553/HYIEL/266627012022010001020

the data specified in Section 57(2) of the National Security Services Act? *(iv)* Was the authorization granted within the time limit? *(v)* Did the validity of the authorization exceed 90 days? *(vi)* Was the justification attached to the authorization? *(vii)* In case of exceptional authorization, were the relevant rules complied with? *(viii)* Did the submission substantiate that the covert information gathering was necessary in the interest of national security? *(ix)* Did the submission substantiate that the purpose of data processing could not be achieved without covert information gathering? *(x)* Did the submission substantiate that the use of all the means and methods requested were necessary? *(xi)* Did the submission substantiate that the duration of covert information gathering requested was necessary? *(xii)* Did the decision of the Minister of Justice reasonably follow from what was proposed in the submission? *(xiii)* Did the Minister of Justice justify the granting of the external authorization with sufficient detail reflecting on the facts and circumstances presented in the submission?

The procedure of the Authority is of outstanding significance also because data subjects have a limited opportunity to exercise their rights in the course of data processing for national security purposes, therefore, the Authority can exercise the rights according to the Privacy Act instead of, and on behalf of the data subjects.[16]

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,[17] 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,[18] 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), in the event of a refusal to provide information pursuant to Section 48 of the National Security Services Act, the data subject may exercise his rights in accordance with the above provisions of the Privacy Act[19] with the assistance of the Authority. Accordingly, the Authority will have to conduct an *ex officio* investigation in the case of every data subject appearing in the news, even if the data subjects do not wish to make use of the enforcement possibilities afforded to them.

16 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. As a safeguard the National Security Services have the obligation to keep records of requests received from data subjects, the mode of their adjudgment and the reasons for their refusal. The Services must report on these annually to the Authority.

17 *Cf.* Criminal Justice Directive, Articles 13(3), 15(3), 16(4).

18 Section 2(3) Privacy Act.

19 Sections 22, 51/A(2), and 60(1) Privacy Act.

In the course of the Authority's investigation, no information was found that the bodies authorized to covertly gather information subject to external authorization 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 their duties specified by law. According to the information made available to the Authority in the course of its investigation, the Specialized 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 also 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 unauthorized 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 the requisite guarantees for this purpose. No data was found in the course of the Authority's investigation that would cast doubt on whether the Specialized National Security Service has acted, and is acting, when using the technical tool, in accordance with the relevant legal regulations, the provisions regulating the organization of public administration and, in the case of contractual relationships, its obligations undertaken in the contract.

With respect to the conditions of using covert information gathering subject to external authorization, it is important to underline that the Hungarian law in force does not differentiate between vocations or professional activities, *i.e.* it does not restrict the authorization of the National Security Services to carry out the activities under Section 56 of the National Security Services Act in respect of any profession (*e.g.* journalist, human rights activist, opposition politician, lawyer and businessman).

In the course of its procedure, the Authority had to clarify how personal data indicating that covert information gathering took place against the data subjects were published. Unfortunately, the Authority's investigation 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. At the same time, it can be clearly established that such data should not have been disclosed because according to the principles of personal data processing as set forth in Section 4(1)-(3) of the Privacy Act, personal data can 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

doi: 10.5553/HYIEL/266627012022010001020

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 organizational measures during processing, in particular measures to protect against unauthorized or unlawful processing, accidental loss, destruction of, 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 organizational measures appropriate to the extent of the risks represented by the processing. In designing and implementing the technical and organizational 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 tool under investigation requires respect for the principles of integrity and confidentiality, including protection against unauthorized or unlawful processing and accidental loss, destruction or damage, by applying appropriate technical and organizational measures.

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, unauthorized transfer or disclosure of, or unauthorized access to, personal data transferred, stored or otherwise processed."

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. In the course of its procedures, the Authority made use of an expert in information security, who explained that in his opinion the circumstances of the data leakage are not known, it can, however, be assumed that data security was breached in some way, as presumably an unauthorized access to personal data took place, so it cannot be excluded that there was a personal data breach. In the event that there was no data breach but an unauthorized third party had unauthorized access to the personal data processed, it is punishable according to Act C of 2012 on the Criminal Code, several criminal offences may have been committed.[20] In view of the above, it cannot be ruled out that a criminal offence has been committed, therefore the Authority initiated criminal proceedings with the investigating authority pursuant to Section 70(1) of the Privacy Act.

20 *E.g.* Section 219: misuse of personal data; Section 265: misuse of classified data; Section 261: spying; Section 423: information system or data breach; Section 424: circumvention of a technical measure to protect an information system.

5. Annex – Facts about the 'Pegasus' Spyware

Presentation of the 'Pegasus' spyware based on the analysis of the expert in information security invited by the Authority.

5.1. The Leaked List Containing 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 into 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 organization or Amnesty International, nor is it known what other 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 to be responsible for selecting the targets.[21] There is a great deal of uncertainty surrounding the list. The statements related to the list can be misinterpreted and do not necessarily match their direct or underlying meaning. NSO Group firmly denied[22] 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 from public services, including among others Home Location Register (HLR) search service, which is not connected to NSO or the services of the company. 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.

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. NSO claimed that it had no servers in Cyprus, and they checked several data in the list and none of them are connected to any of their clients. The list included 300 Hungarian phone numbers. The appendix to the digital trace analysis report issued by Amnesty International shows only two Hungarian data subjects, but the Direkt36 investigative portal, the Hungarian partner of the Pegasus Project identified several phone numbers and continues to publish materials 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

21 Azerbaijan, Bahrein, Kazakhstan, Mexico, Morocco, Rwanda, Saudi-Arabia, Hungary, India and the United Arab Emirates.

22 *See* at www.theguardian.com/news/2021/jul/18/response-from-nso-and-governments.

doi: 10.5553/HYIEL/266627012022010001020

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.

Direkt36 published some material also about a person, whose phone number was not included in the leaked list, 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.

5.2. Pegasus Agent (The 'Spyware' Application)

Following successful infection, a 'spyware' application is installed on the device. Installation does not require the users' authorization; it takes place without the user noticing it. The application running on the infected device provides full authorization to the attacker for the device and the data stored on it. The Pegasus agent is integrated between 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 (*e.g.* phone calls, text messages, chat, *etc.*), which means that even though a chat application may use encryption from endpoint to endpoint, the attacker is able to access the data, which are yet unencrypted. Pegasus uses the vulnerabilities of the devices or the applications running on the devices to install the application.

5.3. Hiding, Survivability 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 to the user, at most the increased data traffic may betray that a fairly substantial exfiltration is taking place in the background. 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.

5.4. The Compromising Process and the Underlying Infrastructure

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, thus, it cannot be clearly determined, based on the contradictory and somewhat vague information what the role the NSO and the client played in 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.

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, also operate at the client's side.

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 the case when it comes to traditional external corporate IT support, and that is why such access is controlled by the security-minded organizations that are more mature from the viewpoint of IT security, for instance, by monitoring support activities even by recording such activities on video.

The Transparency Report issued by NSO contains a statement, which according to the Darknet Diaries professional podcast raises the possibility that NSO may 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 on 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 an 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 leads to the immediate suspension of the right to use the system.

5.5. Anonymizer and Proxy Network

Once the Pegasus agent is successfully installed at the target (or it is already launched), the Pegasus agent begins to communicate with the control server and the surveillance and interception, the forwarding and processing of the data begins.

5.6. The Possibility to Intercept and Detect 'Pegasus'

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.

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 for 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

doi: 10.5553/HYIEL/266627012022010001020

and technical/scientific examination of past digital events that have already taken place, providing answers and evidence as to 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 scrutiny has taken place.

Citizen Lab confirmed the results of the research by Amnesty International; based on the document they published, they found Amnesty International's methodology to be sound and the results of their examination correct, and both organizations 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 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 and French data subjects.