Ügyszám: NAIH-423-2/2022.
Előzmény: NAIH-6583/2021.

A Nemzeti Adatvédelmi és Információszabadság Hatóság hivatalból indított vizsgálatának megállapításai a „Pegasus” kémszoftver Magyarországon történő alkalmazásával összefüggésben

(A Nemzeti Adatvédelmi és Információszabadság Hatóság jelen megállapítások alapját képező vizsgálatáról szóló részletes összefoglaló nem hozható nyilvánosságra, mivel a minősített adat védelméről szóló 2009. évi CLV. törvény 7.§-a szerinti megismételt „Szigorúan Titkos” minősítési szintű minősített adatokat tartalmaz. A minősítés érvényességi ideje: 2050.12.31.)

I. Előzmény

A Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: Hatóság) az információs önrendelkezési jogról és információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) 51/A. §(1) bekezdése alapján 2021. augusztus 9. napján hivatalból vizsgálatot indított a „Pegasus” nevű kémprogram Magyarországon történő alkalmazásával kapcsolatban, tekintettel arra, hogy a sajtóban megjelent hírek szerint a kémprogram használatával személyes adatok jogszerűtlen kezelésére kerülhetett sor.

I.1.
A médiában megjelent hírek

2021. július 19-én a Direkt36 hírportálon ***„Lelepleződött egy durva izraeli kémfegyver, az Orbán-kormány kritikusait és magyar újságírókat is célba vettek vele”*** címmel jelent meg Panyi Szabolcs és Pethő András cikke, amely cikkben többek között az alábbiak szerepeltek:

„Évekkel ezelőtt elkezdték használni magyar célszemélyek ellen is az NSO nevű izraeli kibercég okostelefonok feltörésére alkalmas kémprogramját, a Pegasust, és a célpontként kiválasztott emberek között voltak tényfeltáró újságírók, valamint médiacégeket is tulajdonló vagyonos üzletemberek, illetve az ő szűkebb környezetük is – derítette ki a Direkt36 egy nemzetközi tényfeltáró projekt részeként. A kutatás során számos olyan közvetett bizonyítékot is találtunk, amelyek arra utalnak, hogy a titkos megfigyelések mögött magyar állami szervek állnak.

Az összesen 17 szerkesztőség – köztük a Washington Post, a Guardian, a Süddeutsche Zeitung, a Die Zeit és a Le Monde – részvételével zajló nemzetközi nyomozást a Forbidden Stories nevű tényfeltáró újságírói hálózat vezette, amely az Amnesty International (AI) jogvédő szervezettel közösen jutott hozzá egy, az NSO ügyfeleinek tevékenységével kapcsolatos adatbázishoz. Ebben több mint 50 ezer olyan telefonszám van, amelyeket a tényfeltáró projekt

kutatásai szerint az NSO-ügyfelek megfigyelési célpontként választottak ki 2016-tól kezdve a világ több mint 50 országából.

Az, hogy az adatbázisban feltűnik egy telefonszám, még nem feltétlenül jelenti azt, hogy a célszemélyek ellen biztosan be is vetették a Pegasust és a telefonjukat fel is törték, de számos esetben a telefonok utólagos vizsgálata bizonyította, hogy valóban behatoltak az NSO programjával a készülékekbe.

A Pegasus a telefonok szoftvereinek olyan hibáit használja ki a távolról, észrevétlenül történő behatolásra, melyekről még maguk a fejlesztők, gyártók sem tudnak. Ezeken a réseken keresztül a telefonkészülékbe bejutva nemcsak a célszemélyek beszélgetéseit tudták lehallgatni, hanem hozzáfértek a legbizalmasabb információikhoz, például az emailjeikhez és egyéb üzeneteikhez, továbbá fotóikhoz és videóikhoz.

A Pegasus annyira komoly kiberfegyvernek számít, hogy az NSO csak az izraeli védelmi minisztérium engedélyével adhatja el más országoknak. Hivatalosan csak terrorizmussal és szervezett bűnözéssel gyanúsított személyek ellen lehetne bevetni, de a tényfeltáró projekt kiderítette, hogy az NSO ügyfelei legalább 10 országban használják újságírók, jogvédők, ellenzéki politikusok, ügyvédek és üzletemberek ellen."

„A több mint 300 magyarországi célpont közül egyelőre többek között a következő embereket azonosítottuk be:

- *Négy újságírót, köztük a Direkt36 két munkatársát, Panyi Szabolcsot és Szabó Andrást, akiknek esetében a telefonok utólagos vizsgálata ki is mutatta, hogy a készülékeiket feltörték az NSO szoftverével. Továbbá Dercsényi Dávidot, a Hvg.hu korábbi újságíróját, valamint egy negyedik újságírót, aki azt kérte, hogy ne írjuk le a nevét.*
- *Egy magyar fotóst, aki együtt dolgozott egy olyan amerikai újságíróval, aki az orosz vezetésű, Budapestre költöző Nemzetközi Befektetési Bank ügyeiről írt.*
- *Varga Zoltánt, a Centrál Médiacsoport tulajdonosát – akit már régóta érnek támadások kormányzati körökből –, valamint több olyan más üzletembert, akik Varga házában vettek részt egy közéleti témájú vacsorán 2018-ban. Az utólagos vizsgálatok megerősítették, hogy legalább egy vendég telefonját biztosan fel is törték az NSO programjával. A Varga-féle találkozón részt vett Chikán Attila közgazdászprofesszor is, az első Orbán-kormány gazdasági minisztere, akinek telefonszáma szintén feltűnt a kiszivárgott adatok között.*
- *Simicska Lajos egykori oligarcha fiát és egyik legközelebbi bizalmasát. Mindketten a 2018-as választások előtt kerültek célkeresztbe, amikor Simicska egy egész médiabirodalom tulajdonosa volt, és nyíltan támadta a kormányt. (Simicska nem használt okostelefont, ezért őt magát ezzel a szoftverrel nem lett volna értelme célba venni.)*
- *A CEU egyik külföldi diákját, Adrien Beauduint, akit a magyar hatóságok őrizetbe vettek egy 2018-as kormányellenes tüntetésen.*
- *Emellett több más magyar közszereplő is szerepel a célpontként kiválasztottak között,többek között egy tekintélyes ügyvéd és egy ellenzéki városvezető – az ő történetükről a következő napokban fogunk beszámolni.*

A nemzetközi tényfeltáró csapat birtokába jutott adatokból az nem derül ki egyértelműen, hogy pontosan ki vetette be a kémszoftvert. Több körülmény is erősen utal ugyanakkor arra, hogy a magyar hatóságok használták a programot a magyarországi célpontok ellen.

Az NSO határozottan állítja, hogy ők csak kormányoknak és állami szervezeteknek adják el a szolgáltatásukat, és számos információ mutatja azt, hogy Magyarországon az után jelent meg a kémszoftver, hogy 2017-ben és 2018-ban magas szintű találkozók voltak az izraeli és a magyar kormány között.

A Direkt36-nak egy korábbi magyar titkosszolgálati tiszt mondta, hogy infomációi szerint a nemzetbiztonsági szervek a magyar–izraeli kapcsolat szorosabbá válásával kezdték el használni a Pegasust 2018-tól. A nemzetközi tényfeltáró csapat egyik partnerének, a német Die Zeitnak az NSO egyik korábbi alkalmazottja szintén megerősítette, hogy Magyarország az NSO ügyfele lett. Emellett a kémprogram magyarországi használatának jeleire bukkant egy 2018-as nemzetközi elemzés során a Citizen Lab nevű kanadai kutatócsoport is.

Maguk a magyarországi célpontok is számos esetben arra utalnak, hogy magyar hatóságok állhatnak a célpontok kijelölése mögött. A telefonszámok alapján ugyanis olyan célszemélyeket is beazonosítottunk – például elítélt bűnözőket –, akik ellen a nyilvánosan elérhető információk alapján a magyar hatóságok folytattak nyomozásokat, büntetőeljárásokat. A nemzetközi tényfeltáró projekt több más ország esetében is arra jutott, hogy a helyi hatóságok a kiberfegyvert egyszerre használják az előírásoknak megfelelően és visszaélésszerűen.

Az újságírócsapat részletes kérdéssort küldött az NSO-nak, amely azonban nem reagált a Magyarországgal kapcsolatos felvetésekre. A cég azt vitatja, hogy a Forbidden Stories birtokába jutott telefonszámok valóban a Pegasus célpontjai lennének. Szerintük lehetséges, hogy ezek a számok egy nagyobb listának a részei, „amelyeket az NSO Group ügyfelei más célokra használták". A cég szerint lehetséges, hogy az adatbázisban szereplő számok csak egy nyilvánosan hozzáférhető úgynevezett HLR-adatbázisból származnak. A HLR (Home Location Register) egy olyan rendszer, amely a mobiltelefon-hálózatok működését segíti azzal, hogy nyilvántartja az egyes készülékek földrajzi helyét és más azonosítóit, és így lehetővé teszi a hívások és sms-ek irányítását.

Ez a nyilvántartás ugyanakkor épp emiatt egy hasznos lépése lehet a megfigyelések elindításának is. A HLR révén ugyanis az NSO ügyfelei ellenőrizhetik, hogy a számukra érdekes telefonszámhoz tartozó készülék valóban működik-e (vagyis be van kapcsolva), és hogy fizikailag hol található (ez azért fontos, mert vannak korlátozások, hogy az ügyfelek mely országokban használhatják a Pegasust). Egy, az NSO rendszereit közelről ismerő forrás a tényfeltáró projekt egyik tagjának azt mondta, hogy a HLR-t emiatt a cég ügyfelei használják is.

Az Amnesty International nemzetközi biztonsági stábja megvizsgált 67 olyan készüléket, amelyek a kiszivárgott adatbázis alapján célpontjai lehettek kémszoftveres támadásnak. Ezek közül 23 esetben megállapították, hogy valóban feltörték a telefont Pegasusszal, 14 esetben pedig a behatolásra tett kísérletre utaló nyomokat találtak. A maradék 30 vizsgálatnál nem volt ilyen eredmény, de számos esetben ennek az volt az oka, hogy a feltételezett megfigyelés időpontja óta az érintettek már lecserélték a telefonjukat, és emiatt elvesztek adatok. Emellett a vizsgált telefonok között volt 15 Android-készülék is, amelyek az iPhone-okkal ellentétben nem tárolnak olyan információkat, amelyek alapján az AI stábja egyértelműen meg tudja állapítani a készülék feltörését. De még az Android-telefonok között is volt három, amelyek megfigyelési kísérletek jeleit mutatták, találtak ugyanis rajtuk sms-eket, amelyek a Pegasus nyomait viselték.

Az AI megosztotta több készülék esetében is a vizsgálatok alapját képező adatokat a Citizen Lab kutatóival is, akik megerősítették, hogy azokat Pegasusszal törték fel. A Citizen Lab átnézte az AI vizsgálati módszerét is, és azt is szakmailag rendben találta.

A magyar kormány is részletes kérdéssort kapott, benne az ebben a cikkben szereplő összes lényeges állítással, és ezek egyikét sem tagadták, illetve nem reagáltak rájuk érdemben. Annyit közöltek, hogy „nincs tudomásunk a megkeresésben szereplő állítólagos adatgyűjtésről", és hozzátették, hogy Magyarország „jogállam, és így minden egyén esetében mindig a hatályos jogszabályoknak megfelelően jár el".

[…]

„Az NSO Groupot 2010-ben, az okostelefonok elterjedésének felívelő szakaszában alapította az izraeli hadsereg egyik korábbi tisztje, Shalev Hulio egy üzlettársával. A cégnél olyan technológiákat fejlesztettek ki, amelyekkel fel tudták törni az új típusú mobiltelefonokat, és hozzáfértek az azokon tárolt és továbbított adatokhoz, beleértve azokat az információkat is, amelyek titkosított csatornákon futnak keresztül.

Bár az NSO-nak ma már külföldi befektetői is vannak, a cég továbbra is izraeli központtal működik, és szorosan kötődik a zsidó állam kormányához is. Ha például az NSO el akarja adni a szolgáltatását egy külföldi országnak, akkor ezt csak az izraeli védelmi minisztérium engedélyével teheti meg.

Az NSO állítja, ez nem jelenti azt, hogy a cég „az izraeli diplomácia eszköze" lenne. Vannak példák ugyanakkor arra, amikor bizonyos országokban a Pegasus megjelenése egybeesett egy magas rangú izraeli találkozóval. Ez történt India esetében is, ahol a kiszivárgott adatok szerint Narendra Modi indiai miniszterelnök 2017. júliusi izraeli látogatása után szaporodott el a célpontok kiválasztása.

Magyarország esetében is észlelhető némi egybeesés az Izraellel fennálló viszony szorosabbá válása és a Pegasus megjelenése között."

[…]

„Egy volt magyar titkosszolgálati tiszt is azt mondta a Direkt36-nak, hogy tudomása szerint 2018 elejétől kezdte el használni a magyar állam a Pegasust, és hogy „a beszerzésnek sok köze van az Izraellel való kapcsolataink szorosra fonódásához". A névtelenséget kérő forrás szerint a magyar kormányt régóta zavarta az, hogy a hagyományos lehallgatási módszerekkel nem férnek hozzá olyan kommunikációhoz, ami a titkosított applikációkon (mint amilyen például a Signal vagy a WhatsApp) zajlik, ezért kaptak a lehetőségen, hogy használhassák az NSO termékét. Az okostelefon feltörésével ugyanis a Pegasus használói számára láthatóvá válik minden, ami a készülék kijelzőjén megjelenik, beleértve azokat a beszélgetéseket és üzeneteket, amelyek a titkosított appokon futnak keresztül.

A fejlett technológiának magas az ára is. Egy korábban nyilvánosságra került mexikói szerződés esetében a tarifa célpontonként 64 ezer dollárra (19 millió forint), míg egy panamai szerződésnél 89 ezer dollárra (27 millió forint) jön ki. A Pegasus Projekt újságírócsapatának tagjai több, az NSO belső ügyeit ismerő forrással is beszéltek, és elmondásuk alapján ma már ennél valószínűleg olcsóbb a kémszoftver. Konkrét összeget azért is nehéz mondani, mert az árazás számos tényezőtől függ (például hogy az ügyfél mely régióhoz tartozik, hány célpontot szeretne egyszerre megfigyelni, vagy hogy emberi jogok tiszteletben tartása szempontjából menynyire kockázatos vele szerződni).

A Pegasushoz hasonló kémprogramoknak nincs külön szabályozásuk a magyar törvényekben. A jogszabályok csak általánosságban foglalkoznak az úgynevezett titkos információgyűjtéssel, amibe beletartoznak például a hagyományos telefonlehallgatások vagy egy lakás bemikrofonozása is. Ezek a szabályok nagyon tág mozgásteret biztosítanak a hatóságoknak a különböző eszközök, így például a Pegasus használatára.

A titkos információgyűjtő műveleteknek alapvetően két kategóriájuk van, függően attól, hogy mely hatóságok végzik. Egyrészt folytathatnak ilyet a bűnüldöző hatóságok (rendőrök, adónyomozók stb.), ha valamilyen konkrét bűncselekmény gyanújával nyomoznak. Ezt csak akkor csinálhatják, ha kapnak hozzá bírói engedélyt, és utána is csak korlátozott ideig végezhetik ezt a tevékenységet. Ha nem sikerül ez idő alatt a bűncselekmény gyanújához elegendő in-

formációt szerezni, akkor elvileg meg kell semmisíteniük az adatokat. Ha pedig valakit meggyanúsítanak, akkor a titkos módon gyűjtött adatokat úgymond „nyílttá kell tenni", vagyis be kell kerülnie a hivatalos nyomozati iratokba, amelyeket később a gyanúsított is megismerhet.

Lazábbak a szabályok akkor, ha a nemzetbiztonsági szolgálatok végeznek ilyen titkos információgyűjtést. Számukra nem szükséges bírói engedély, hanem elég az igazságügyi miniszter jóváhagyása (bizonyos esetekben már az engedély megszerzése előtt is megkezdhetik a titkos információgyűjtést).

A Forbidden Stories és az AI által megszerzett több mint 300 magyar telefonszám mindössze azt mutatja, hogy konkrétan az NSO magyar ügyfelei kiket választottak ki megfigyelés célpontjának Magyarországon. A magyar hatóságok által végrehajtott megfigyelések száma ugyanakkor ennél jóval magasabb.

Nemrég számolt be róla a 168 Óra, hogy az elmúlt öt évben megszaporodtak az igazságügyi miniszter által jóváhagyott titkos információszerzési műveletek. Míg 2015-ben még 1038 ilyen engedélyt adtak ki, addig az elmúlt években már 1200-1300 körül volt az ilyen esetek száma. Ez azt jelenti, hogy átlagban naponta több mint 3 megfigyelési engedélyt adott ki a miniszter. Ehhez képest idén már csak az első három és fél hónapban közel 500 miniszteri engedély született, tehát minden napra jutott 5 jóváhagyás.

A jogszabályok meglehetősen tágan fogalmaznak arról, hogy milyen esetekben végezhetnek ilyen műveleteket a különböző szolgálatok – ide tartozik többek között a polgári titkosszolgálatként működő, Pintér Sándor belügyminiszter által felügyelt Alkotmányvédelmi Hivatal, a külföldi hírszerzésért felelős, Szijjártó Péter külügyminiszter alá tartozó Információs Hivatal és az Orbán Viktor egykori személyes testőre, Hajdu János által vezetett Terrorelhárítási Központ. A konkrét megfigyelések technikai lebonyolítását pedig egyfajta kiszolgálószervként egy ezektől különböző negyedik hivatal, a Nemzetbiztonsági Szakszolgálat végzi, szintén Pintér felügyelete alatt.

Jellemző példa arra, hogy milyen tág keretek között végzik ezek a szolgálatok a munkájukat, hogy az Információs Hivatal feladatkörét úgy írja le a törvény, hogy „megszerzi, elemzi, értékeli és továbbítja a kormányzati döntésekhez szükséges" információkat.

Július elején a tényfeltáró projektben részt vevő francia Le Monde újságírója egy interjúban megkérdezte Varga Judit igazságügyi minisztertől, hogy megadná-e a felhatalmazást egy újságíró vagy ellenzéki személy megfigyelésére, mire Varga felháborodottan azt válaszolta: „Micsoda kérdés! Ez önmagában provokáció!" Varga azt állította, hogy csak a jogszabályoknak megfelelő megfigyelési kérelmek kaphatnak engedélyt, és azt is hozzátette, hogy „annyi sok veszély leselkedik az államra mindenhonnan".

Később Varga is részletes kérdéssort kapott a célpontként kiválasztott, illetve konkrétan megfigyelés alá is vett magyar újságírókról és médiatulajdonosokról, de erre már nem érkezett válasz."[1]

II. Jogszabályi háttér

II.1.

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

Alkotmányossági és nemzetközi jogi keretek

Magyarország Alaptörvénye az alapvető jogok védelmével és érvényesülésük biztosításával kapcsolatban a következő alapvető követelményeket rögzíti:

„I. cikk (1) Az ember sérthetetlen és elidegeníthetetlen alapvető jogait tiszteletben kell tartani. Védelmük az állam elsőrendű kötelezettsége.
(2) Magyarország elismeri az ember alapvető egyéni és közösségi jogait.
(3) Az alapvető jogokra és kötelezettségekre vonatkozó szabályokat törvény állapítja meg. Alapvető jog más alapvető jog érvényesülése vagy valamely alkotmányos érték védelme érdekében, a feltétlenül szükséges mértékben, az elérni kívánt céllal arányosan, az alapvető jog lényeges tartalmának tiszteletben tartásával korlátozható. […]” [Magyarország Alaptörvénye I. cikk (1)-(3) bekezdés]

Az Alaptörvény VI. cikk (1) bekezdése alapján mindenkinek joga van ahhoz, hogy magán- és családi életét, otthonát, kapcsolattartását és jó hírnevét tiszteletben tartsák, (3)-(4) bekezdése szerint pedig mindenkinek joga van személyes adatai védelméhez, valamint a közérdekű adatok megismeréséhez és terjesztéséhez is. E cikk (4) bekezdése rögzíti továbbá azt, hogy a személyes adatok védelméhez és a közérdekű adatok megismeréséhez való jog érvényesülését sarkalatos törvénnyel létrehozott, független hatóság ellenőrzi.

Nemzetközi jogi kötelezettségként szükséges figyelemmel lenni az Emberi jogok és alapvető szabadságok védelméről szóló egyezményre (a továbbiakban: Egyezmény)[2] is, amelynek 8. cikke szerint *„mindenkinek joga van arra, hogy magán- és családi életét, lakását és levelezését tiszteletben tartsák. E jog gyakorlásába hatóság csak a törvényben meghatározott, olyan esetekben avatkozhat be, amikor az egy demokratikus társadalomban a nemzetbiztonság, a közbiztonság vagy az ország gazdasági jóléte érdekében, zavargás vagy bűncselekmény megelőzése, a közegészség vagy az erkölcsök védelme, avagy mások jogainak és szabadságainak védelme érdekében szükséges”*.

Az Alkotmánybíróság releváns gyakorlata szerint, ahogyan arra a 32/2013. (XI.22.) Alkotmánybírósági határozat is rámutat, a titkos információgyűjtési eszközök és módszerek alkalmazása szoros kapcsolatban áll a magánszférához való joggal, az információs önrendelkezési joggal és az emberi méltósághoz való joggal.

A titkos információgyűjtés alkotmányosságát illetően fontos iránymutatással szolgál emellett az Alkotmánybíróság 2/2007. (I. 24.) AB határozatának indokolása, mely szerint „*A titkos információgyűjtés és a titkos adatszerzés büntetőjogi eszközként való igénybevételét a demokratikus jogállamban megalapozza az a körülmény, hogy egyes, a társadalom rendjét súlyosan sértő vagy veszélyeztető bűncselekmények elleni eredményes fellépéshez a hagyományos eszközök nem bizonyulnak elegendőnek. A társadalom védelme érdekében olyan módszerekre, eszközökre van szükség, amelyek behozhatják a bűnüldöző szerveknek a bűnözéssel szemben esetlegesen fennálló lépéshátrányát. A vizsgált alapjogoknak a titkos eljárásban alkalmazható módszerek által okozott korlátozása tehát alkotmányosan nem szükségtelen eszköz. A jogállamiság és az alapjogok védelme azonban megköveteli azt is, hogy ezen eszközök felhasználásának rendjét a jog részletesen és differenciáltan*

[2] Magyarországon kihirdette az 1993. évi XXXI. törvény.

szabályozza. Minthogy a titkos eszközök és módszerek igénybevétele súlyos beavatkozást jelent az egyén életébe, alkalmazásuknak csupán kivételesen, átmeneti, végső megoldásként lehet helye."

A 32/2013. (XI.22.) Alkotmánybírósági határozat figyelembe veszi az Egyezmény végrehajtásának felügyeletére hivatott, az Emberi Jogok Európai Bírósága ítélkezési gyakorlatát is, amely alapján a következőket állapítja meg: „*Minthogy a titkos információgyűjtés szükségképpen kizárja a hatékony jogorvoslat lehetőségét, elengedhetetlenül fontos, hogy az alkalmazást lehetővé tévő eljárási rend kellő garanciát nyújtson az egyén jogainak védelmére. Minderre tekintettel az alkalmazást három szakaszból álló ellenőrzésnek kell alávetni: amikor a beavatkozást elrendelik, mialatt a beavatkozást végrehajtják, miután a beavatkozást befejezték. Az ellenőrzést a végrehajtó hatalomtól független testületeknek kell végezni. Elsősorban az állandó, folyamatos és kötelező ellenőrzés a garancia arra, hogy a konkrét ügyekben nem sértik meg az arányosság követelményét. Határozataiban a Bíróság rámutatott azokra a követelményekre, amelyeket a titkos eszközök használatára vonatkozó szabályozásnak minimálisan ki kell elégítenie. Kiemelte, hogy éppen azért, mert az alapjogokba történő beavatkozás titkos, s mert az ilyen eszközök használata a végrehajtó hatalomnak beláthatatlan lehetőségeket ad, elengedhetetlen, hogy már maguk az eljárások kellő garanciát nyújtsanak az egyén jogainak érvényesülésére. Ez pedig megkívánja, hogy az államok hangsúlyt helyezzenek a precíz és részletes, követhető, az állampolgárok számára is hozzáférhető szabályok megalkotására. A jogi szabályozásból világossá kell válnia az ilyen eszközöket alkalmazó hatóság hatáskörének, az intézkedések lényegének, azok gyakorlása módjának. A Bíróság a világos normatartalom követelménye körében arra is rámutatott, hogy a törvényeknek tartalmazniuk kell a beavatkozást indokoló eseteket, körülményeket és a beavatkozás feltételeit. Minimális biztosítékként szerepelnie kell bennük továbbá az érintett személyek körének meghatározására alkalmas feltételeknek, az alkalmazás dokumentálására és a dokumentáció megóvására, valamint megsemmisítésének szabályaira vonatkozó rendelkezéseknek. Az alkalmazásról szóló döntés meghozatala körében pedig a hatóságok nem kaphatnak túl széles mérlegelési jogot. Az alkalmazás garanciái közé tartozik továbbá, hogy (külső személyek számára) az információkhoz való hozzáférést korlátozni kell.*"

II.2.
A titkos információgyűjtés és a személyes adatok védelmére vonatkozó szabályozás

A titkos információgyűjtés általános adatvédelmi jogi kereteit a személyes adatok kezelését illetően az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) határozza meg.

A titkos információgyűjtés – az Infotv. perspektívájából tekintve – folytatható *bűnüldözési* (bűncselekmények megelőzése, nyomozása, felderítése) célból, illetve *nemzetbiztonsági* célból is. Az Infotv. 2. § (3) bekezdése szerint ezen adatkezelések, illetve azok felügyelete tekintetében mindkét esetkörben az Infotv. anyagi és eljárásjogi szabályai alkalmazandóak. Fontos megjegyezni azonban, hogy míg a bűnüldözési célú adatkezelés az uniós jog, a magyar jogba az Infotv. rendelkezéseivel átültetett irányelvi jogforrásban (Bűnügyi Irányelv[3])

[3] A személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről szóló, 2016. április 27-i (EU) 2016/680 európai parlamenti és tanácsi

szabályozott hatálya alá tartozik, addig a nemzetbiztonsági (és honvédelmi) célú adatkezelés az uniós jog hatályán kívül esik, az kizárólag a tagállamok szabályozási és jogalkalmazási kompetenciája. Mind az Általános Adatvédelmi Rendelet[4] (GDPR) 2. cikk (2) bekezdés a) pontja és (16) preambulum bekezdése, mind a Bűnügyi Irányelv (14) preambulum bekezdése és 2. cikk (3) bekezdés a) pontja ugyanis egyértelmű abban a tekintetben, hogy a nemzetbiztonsággal kapcsolatos tevékenységek során végzett személyesadat-kezelés nem tartozik az uniós jog hatálya alá. A nemzetbiztonság mint jogalkotási és jogalkalmazási tárgykör tehát az uniós jog szerint kizárólagosan tagállami hatáskörbe tartozik.

Az Infotv. az adatkezelés alapelveit meghatározó 4. §-a szerint személyes adat kizárólag meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében kezelhető. Az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának, az adatok felvételének és kezelésének tisztességesnek és törvényesnek kell lennie. Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas. A személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető. Az Infotv. 7. §-a alapján emellett az adatkezelő köteles az adatkezelési műveleteket úgy megtervezni és végrehajtani, hogy az Infotv. és az adatkezelésre vonatkozó más szabályok alkalmazása során biztosítsa az érintettek magánszférájának védelmét. Az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek az Infotv., valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek. Az adatokat megfelelő intézkedésekkel védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.

II.3.
A titkos információgyűjtő tevékenység típusai és alapvető feltételei

A nemzetbiztonsági szolgálatok titkos információgyűjtő tevékenysége alapvető jogokat, így a magánélet tiszteletben tartásához, valamint a személyes adatok védelméhez fűződő jogot is érinti, ezért az Alaptörvény I. cikk (3) bekezdésével összhangban törvényi szinten szabályozandó. A nemzetbiztonsági szolgálatok feladatait, működésük alapelveit, az általuk végzett adatkezelést, valamint a titkos információgyűjtő tevékenységük során igénybe vehető eszközöket és módszereket, továbbá az eszközalkalmazás feltételeit és rendjét a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény (a továbbiakban: Nbtv.) határozza meg.

A titkos információgyűjtő tevékenység során igénybevett eszközök és módszerek alkalmazására vonatkozó szabályokat az egyes, ilyen tevékenység végzésére jogosult szervek – adatvédelmi szempontból adatkezelők – ágazati törvényei rögzítik: az Nbtv., a Rendőrségről szóló 1994. évi XXXIV. törvény (a továbbiakban: Rtv.) a büntetőeljárásról szóló 2017. évi XC. törvény (a továbbiakban: Be.) az ügyészségről szóló 2011. évi CLXIII. törvény,

irányelv

[4] A természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló, 2016. április 27-i (EU) 2016/679 európai parlamenti és tanácsi rendelet (általános adatvédelmi rendelet)

a Nemzeti Adó- és Vámhivatalról szóló 2010. évi CXXII. törvény.

Titkos információgyűjtés folytatható bűnüldözési célból, illetve nem bűnüldözési célból is. A bűnüldözési célból folytatott titkos információgyűjtésre az Rtv. szerint egyes esetekben bírói engedélyhez kötötten [Rtv. 70. §], más esetekben bírói engedélyhez nem kötötten [Rtv. 66. §] kerülhet sor. A bírói engedélyhez kötött titkos információgyűjtés alkalmazását az Rtv. 75/B. § (1) bekezdése kilencven napos határidőre teszi lehetővé, amely újabb kérelem előterjesztése esetén legfeljebb kilencven nappal meghosszabbítható.

A rendőrség bűncselekmény felderítése, megszakítása, az elkövető kilétének megállapítása, elfogása, bizonyítékok megszerzése, illetve a bűncselekményből származó vagyon visszaszerzése érdekében kizárólag a Be.-ben meghatározottak szerint alkalmazhat leplezett eszközöket. Az általános rendőrségi feladatok ellátására létrehozott szerv és a belső bűnmegelőzési és bűnfelderítési feladatokat ellátó szerv a 64. §-ban meghatározott célokból titkos információgyűjtést kizárólag az Rtv.-ben meghatározott szabályok alapján folytathat. A terrorizmust elhárító szerv az Rtv. 7/E. § (1) bekezdés a) pont aa) alpontjában meghatározott, bűncselekmények megelőzésével kapcsolatos feladatai, illetve a 7/E. § (1) bekezdés b) pont ba) alpontjában, valamint c) pontjában meghatározott feladatai ellátása érdekében titkos információgyűjtést kizárólag az Rtv.-ben meghatározott szabályok alapján folytathat. A terrorizmust elhárító szerv a 7/E. § (1) bekezdés a) pont ad) alpontjában, valamint e) pontjában meghatározott feladata ellátása érdekében az Nbtv. 53-60. §-ának megfelelő alkalmazásával folytathat titkos információgyűjtést, amelynek ellátása során az Nbtv. 38-52. §-a szerint jogosult adatok igénylésére és kezelésére. Az Nbtv. 56. § a)-e) pontjában meghatározott titkos információgyűjtést az igazságügyért felelős miniszter engedélyezi.

Bűncselekmény elkövetésének megelőzése céljából akkor folytatható titkos információgyűjtés, ha megalapozottan feltehető, hogy attól a bűnözésre vonatkozó olyan információk megszerzése várható, amelyek elemzése és értékelése révén feltárhatók a bűncselekmények elkövetésére irányuló törekvések és lehetővé válik a bűncselekmények megelőzése, illetve megakadályozása. A rendőrség terrorizmust elhárító szerve akkor folytathat titkos információgyűjtést a 7/E. § (1) bekezdés b) pont ba) alpontjában meghatározott feladata ellátása céljából, ha attól a hatáskörébe tartozó bűncselekmény megszakításához vagy az elkövető elfogásához szükséges információk megszerzése várható. [Rtv. 65.§ (1)-(2) bekezdés]

A nem bűnüldözési célból – azaz nemzetbiztonsági célból – folytatott titkos információgyűjtés is lehet, jellegét tekintve, külső engedélyhez nem kötött [Nbtv. 54. §, 55. §] és külső engedélyhez kötött [Nbtv. 56-60. §]. A külső engedély a törvényben meghatározott esetekben vagy bírói vagy igazságügyért felelős miniszteri engedélyt jelent.

Ahogyan a fentiekben már hivatkozott 32/2013. (XI.22.) ABH is utal rá, a nemzetközi gyakorlatban számos példa van arra, hogy az államok különbséget tesznek a bűnüldözési (és az ahhoz szorosan kapcsolódó bűnmegelőzési, bűnfelderítési), valamint az egyéb nemzetbiztonsági célból történő információgyűjtés között.

Az Alkotmánybíróság az Emberi Jogok Európai Bírósága ítélkezési gyakorlatára utalva rögzíti, hogy az követelményként fogalmazza meg a *részletes, követhető, az állampolgárok számára is hozzáférhető szabályok alkalmazását, melyekből „világossá kell válnia az ilyen eszközöket*

alkalmazó hatóság hatáskörének, az intézkedések lényegének, azok gyakorlása módjának".

Ennek megfelelően az Nbtv. nevesíti a nemzetbiztonsági szolgálatokat, amelyek feladataik teljesítése érdekében titkos információgyűjtést folytathatnak, és felsorolja az egyes nemzetbiztonsági szolgálatok feladatait, valamint tartalmazza a titkos információgyűjtésre vonatkozó részletes szabályokat is. Ezek az alábbiakban foglalhatóak össze.

Az Nbtv. 53. § (2) bekezdése szerint a nemzetbiztonsági szolgálatok a titkos információgyűjtés speciális eszközeit és módszereit csak akkor használhatják, ha az Nbtv.-ben meghatározott feladatok ellátásához szükséges adatok más módon nem szerezhetők meg. A titkos információgyűjtés folytatására feljogosított nemzetbiztonsági szolgálat a titkos információgyűjtést önállóan vagy más nemzetbiztonsági szolgálat közreműködésével hajtja végre, vagy a végrehajtáshoz a Nemzetbiztonsági Szakszolgálatot veszi igénybe.

Ez utóbbi esetben a Nemzetbiztonsági Szakszolgálat eljárásának alapja, hogy az Nbtv. 8.§ (1)-(2) bekezdése alapján a Nemzetbiztonsági Szakszolgálat a jogszabályok keretei között, eszközeivel és módszereivel – írásbeli megkeresésre – szolgáltatást végez a titkos információgyűjtés, illetve a büntetőeljárásról szóló törvény szerinti leplezett eszközök alkalmazásának végrehajtásához a titkos információgyűjtés folyatatására, valamint a leplezett eszközök alkalmazására feljogosított szervek részére. A Nemzetbiztonsági Szakszolgálat a titkos információgyűjtés folytatására, valamint a leplezett eszközök alkalmazására feljogosított szervek igényei alapján biztosítja az e tevékenységhez szükséges különleges technikai eszközöket és anyagokat.

A nemzetbiztonsági szolgálatok az Nbtv. rendelkezései szerint külső engedély alapján lakást, egyéb helyiséget, bekerített helyet, illetve a közösségi közlekedési eszköz kivételével járművet, továbbá az érintett személy használatában lévő tárgyat titokban átkutathatnak, az észlelteket technikai eszközzel rögzíthetik, a lakásban, egyéb helyiségben történteket titokban technikai eszközzel megfigyelhetik és rögzíthetik, postai küldeményt vagy beazonosítható személyhez kötött egyéb zárt küldeményt titokban felbonthatnak, annak tartalmát megismerhetik, ellenőrizhetik és rögzíthetik. Külső engedély alapján elektronikus hírközlési szolgáltatás keretében elektronikus hírközlő hálózat vagy eszköz útján, illetve információs rendszeren folytatott kommunikáció tartalmát titokban megismerhetik és rögzíthetik.
A nemzetbiztonsági szolgálatok emellett az információs rendszerben kezelt adatokat titokban megismerhetnek, az észlelteket technikai eszközzel rögzíthetik, illetve az ehhez szükséges elektronikus adatot az információs rendszerben, illetve a szükséges technikai eszközt lakásban, egyéb helyiségben, bekerített helyen, illetve járműben, továbbá az érintett személy használatában lévő tárgyban elhelyezhetik, valamint a kibertérből érkező fenyegetés elhárítása céljából az információs rendszerbe beavatkozhatnak [Nbtv. 56. § a)-e) pont].

Az Nbtv. szabályozási rendszerében tehát a titkos információgyűjtés fent említett eszközeinek és módszereinek alkalmazása külső engedélyhez kötött, hiszen ezek az eszközök és módszerek közvetlen hatással vannak a magán- és családi élet, az otthon és a kapcsolattartás tiszteletben tartására, valamint a személyes adatok védelméhez fűződő alapvető jogra.

II.4.

A titkos információgyűjtés engedélyezésére irányuló eljárás

Az Nbtv. 57. § szerint a külső engedélyhez kötött titkos információgyűjtés engedélyezésére irányuló előterjesztést az Információs Hivatal, az Alkotmányvédelmi Hivatal, a Katonai Nemzetbiztonsági Szolgálat, és meghatározott feladat tekintetében a Nemzetbiztonsági Szakszolgálat főigazgatója nyújthatja be. Az előterjesztésnek tartalmaznia kell a titkos információgyűjtés helyét, az érintett vagy érintettek nevét vagy körét, a titkos információgyűjtés módját és szükségességének indokolását, illetve a tevékenység kezdetét és végét napban meghatározva. Az ún. kivételes engedélyezés esetén az előterjesztésnek tartalmaznia kell továbbá annak indokolását, hogy az adott ügyben a kivételes engedélyezésre a nemzetbiztonsági szolgálat eredményes működéséhez feltétlenül szükség volt.

A konkrét bűncselekmények felderítése tekintetében a titkos információgyűjtést a Fővárosi Törvényszék elnöke által e feladatra kijelölt bíró engedélyezi. Egyéb, az általános jellegű információgyűjtés során alkalmazott, az Nbtv. 56. §-ában meghatározott tevékenységet az igazságügyért felelős miniszter engedélyezi. Az engedélyező (bíró vagy az igazságügyért felelős miniszter) az előterjesztés benyújtásától számított 72 órán belül határozatot hoz, az előterjesztésnek helyt ad, vagy azt megalapozatlansága esetén elutasítja. A külső engedély tárgyában történő határozathozatal tehát tipikusan megelőzi az eszközalkalmazást, a külső engedély a titkos információgyűjtés megkezdésének előfeltétele. Ez alól kivétel az Nbtv. 59. § szerinti kivételes engedélyezés (ld. alább), de az eszközalkalmazás folytatása és az adatok későbbi felhasználása az Nbtv. 60. § (2) bekezdése szerint ebben az esetben is a külső engedély megadásához van kötve.

Az engedélyezési eljárás tehát az engedély iránti előterjesztés benyújtásával indul. Az engedélyező arról dönt, hogy a külső engedély iránti előterjesztés megalapozott-e, hogy az előterjesztésben foglaltak alátámasztják-e a titkos információgyűjtés szükségességét, az előterjesztés kellően pontosan megjelöli-e az alkalmazni kívánt eszközt és módszert, az alkalmazás helyét, időbeli kezdetét és végét, valamint az alkalmazással érintett személyi kört. Az engedélyező a titkos információgyűjtést esetenként legfeljebb kilencven napra engedélyezi, amely határidőt az engedélyező indokolt esetben, a főigazgatók kiegészítő előterjesztése alapján további kilencven nappal meghosszabbíthatja.

Az igazságügyért felelős miniszter engedélyezési eljárása fölött az Nbtv. 14. §-a alapján az Országgyűlés, a Nemzetbiztonsági Bizottság közreműködésével jogosult ellenőrzést gyakorolni. A titkos információgyűjtés kereteit minden esetben úgy kell meghatározni, hogy a személyes adatok célhoz kötött kezelésének követelményeivel összhangban az információgyűjtés céljának eléréséhez szükséges legkisebb mértékben korlátozza a magánélet tiszteletben tartásához, valamint a személyes adatok védelméhez való jog érvényesülését. A szükségesség követelménye nem csak arra vonatkozik, hogy a titkos információgyűjtés szükséges-e, – vagy a feladat ellátásához nélkülözhetetlen adatok más módon is beszerezhetőek-e –, hanem egyúttal arra is, hogy mikor, hol, milyen eszközzel és kivel szemben szükséges a titkos információgyűjtés.

Az általános szabályoktól eltérően a nemzetbiztonsági szolgálatok főigazgatói az engedélyező (bíró vagy igazságügyért felelős miniszter) döntéséig engedélyezhetik az Nbtv. 56. §-ában felsorolt titkos információgyűjtést, abban az esetben, ha a titkos információgyűjtés külső engedélyeztetése olyan késedelemmel járna, amely az adott ügyben nyilvánvalóan sértené a

nemzetbiztonsági szolgálat eredményes működéséhez fűződő érdeket (ún. kivételes engedély). A kivételes engedély legfeljebb az engedélyező döntéséig tart és a külső engedély iránti előterjesztést a nemzetbiztonsági szolgálatok főigazgatói kötelesek engedélyezésükkel egyidejűleg benyújtani. Egy adott ügyben titkos információgyűjtést kivételes engedélyezés alapján elrendelni az arra jogosult főigazgatónak főszabály szerint egyszer van módja. Az Nbtv. 60. § (2) bekezdése rögzíti, hogy kivételes engedélyezés esetén a titkos információgyűjtést haladéktalanul meg kell szüntetni, ha a titkos információgyűjtés folytatását az engedélyező bíró vagy igazságügyért felelős miniszter nem engedélyezi. Ebben az esetben a titkos információgyűjtés során nyert adatokat – a minősített adatok megsemmisítésére vonatkozó jogszabályi előírások szerint – haladéktalanul meg kell semmisíteni. Minden egyéb esetben a külső engedélyhez kötött titkos információgyűjtést haladéktalanul meg kell szüntetni, ha az engedélyben meghatározott célját elérte, ha a titkos információgyűjtés további alkalmazásától nem várható eredmény, ha a határideje meghosszabbítás nélkül lejárt, vagy ha a titkos információgyűjtés bármely okból kifolyólag törvénysértő.

II.5.
A titkos információgyűjtés végrehajtása

Ha a titkos információgyűjtés végrehajtására a Nemzetbiztonsági Szakszolgálat szolgáltatásainak keretein belül kerül sor, a titkos információgyűjtés folytatásához szükséges engedély beszerzése az alkalmazást megrendelő szerv feladata. Így az alkalmazás jogszerűségéért a megrendelő szerv, míg a végrehajtásáért a Nemzetbiztonsági Szakszolgálat felel. A titkos információgyűjtés belső eljárási és engedélyezési szabályait az Nbtv. 11. § (1) bekezdés h) pontja alapján a főigazgatók előterjesztésére az egyes nemzetbiztonsági szolgálatok irányításáért felelős miniszter hagyja jóvá. Mivel a Nemzetbiztonsági Szakszolgálat az Nbtv. 8. § (1) bekezdés szerinti szolgáltató tevékenységet végez, a titkos információgyűjtés során megszerzett valamennyi adatot törli a nyilvántartásából a megrendelőnek történő adattovábbítást követően.

A Nemzetbiztonsági Szakszolgálat szolgáltató feladataival kapcsolatosan nyilvántartást vezet, amely tartalmazza a megrendelő szervezet írásbeli megkeresését a szükséges engedéllyel, a megkeresésben megjelölt személyek azonosításához szükséges személyes adatokat, a titkos információgyűjtés során igénybe vett eszközök és módszerek leírását, valamint a személyes adatnak nem minősülő, műveleti értékkel bíró információkat, technikai adatokat és a megrendelő szervezet részére továbbított adathordozók jegyzékét. A Nemzetbiztonsági Szakszolgálat a szolgáltatói feladata ellátásához kapcsolódóan ezeken kívül más személyes adatot nem tárolhat.

Az Nbtv. hatálya alá nem tartozó titkos információgyűjtés folytatására feljogosított szerv az információs rendszer titkos megfigyelése eszköz alkalmazását kizárólag a Nemzetbiztonsági Szakszolgálat által nyújtott szolgáltatás igénybevételével hajtja végre. [Nbtv. 62/A. §]

Ennek magyarázatát az Nbtv. miniszteri indokolása részletezi, mely szerint: *„a Nemzetbiztonsági Szakszolgálat kizárólagos hatásköre a titkos információgyűjtés, illetve leplezett eszközalkalmazás külső engedélyhez kötött azon szegmensére vonatkozik, ahol műszaki-technikai szempontból egyedülálló, komplex, ebből kifolyólag jelentős anyagi ráfordítást, különleges szakértelmet és tapasztalatot igénylő rendszerek kiépítése vagy speciális szaktudással rendelkező humánerőforrás megléte szükséges. Az információs*

rendszer titkos megfigyelésének végrehajtását is indokolt a Nemzetbiztonsági Szakszolgálat kizárólagos hatáskörébe utalni, mivel az eszközalkalmazáshoz - a lehallgatáshoz hasonlóan - jelentős anyagi ráfordítást igénylő technikai rendszerekre és speciális szaktudással rendelkező humánerőforrásra van szükség. Ezen képességek a Nemzetbiztonsági Szakszolgálatnál történő koncentrálása biztosítja a költségvetési források hatékony és takarékos felhasználását, illetve a centralizálás eredményeként indokolatlan párhuzamos kapacitások sem kerülhetnek kiépítésre. Az információs rendszer titkos megfigyelése vonatkozásában azonban nincs hasonló törvényi vagy kormányrendeleti szintű ágazati szabályozás, mint amelyek a küldemény titkos megismerése, illetve a lehallgatás vonatkozásában lehetővé tették a rendelkezés meghatározását, így a rendelkezés kizárólag az Nbtv.-ben helyezhető el, amely speciális szabályként rögzíti, hogy az információs rendszer titkos megfigyelése esetében kizárólag a Nemzetbiztonsági Szakszolgálat útján lehet végrehajtani az eszköz alkalmazását".

Magyarországon a hatályos törvényi szabályozás alapján kilenc szervezet végezhet titkos információgyűjtést, illetve jogosult leplezett eszköz alkalmazására. A Nemzetbiztonsági Szakszolgálat törvényben meghatározott feladata a titkos információgyűjtés eszközeinek és módszereinek, illetve a leplezett eszközöknek az alkalmazására feljogosított szervezetek munkájának támogatása speciális szolgáltatások biztosítása útján.

A titkos információgyűjtés folytatására feljogosított szervek és a Nemzetbiztonsági Szakszolgálat közötti együttműködés rendjét a Kormány rendeletben határozza meg. A Nemzetbiztonsági Szakszolgálat a haditechnikai tevékenység engedélyezésének és a vállalkozások tanúsításának részletes szabályairól szóló 156/2017. (VI. 16.) Korm. rendelet 1. számú mellékletének XXVI. Fejezetében felsorolt titkosszolgálati eszköznek minősülő olyan szoftvert is alkalmaz, amely alkalmas az adatokat tároló és/vagy feldolgozó számítógépekből, számítástechnikai vagy egyéb eszközökből a hozzájuk használt adathordozókból a tárolt információ bármilyen módon történő titkos megszerzésére, továbbítására, rögzítésére, valamint a számítástechnikai eszközökön folytatott tevékenység valós idejű titkos megfigyelésére, rögzítésére illetve az elektronikus hírközlő hálózaton folytatott kommunikáció megszerzésére. Az ilyen eszközök és szoftverek alkalmasak a számítástechnikai eszközök ellenőrzésére, illetve az elektronikus hírközlő hálózaton (és az azt helyettesítő hálózaton) folytatott kommunikáció ellenőrzésére egyaránt.

II.6.
A titkos információgyűjtés jogszerűségének ellenőrzése

A nemzetbiztonsági szolgálatok működésének jogszerűségét az Országgyűlés Nemzetbiztonsági Bizottsága hivatott ellenőrizni. A szolgálatok parlamenti ellenőrzésének szabályait az Nbtv rögzíti. Eszerint a Nemzetbiztonsági Bizottság az ellenőrzési tevékenysége keretében tájékoztatást kérhet a minisztertől és a szolgálatok főigazgatóitól a szolgálatok működéséről, tájékoztatást kérhet az illetékes miniszterektől, valamint a főigazgatóktól a külső engedélyhez kötött titkos információgyűjtéssel kapcsolatos engedélyezési eljárásról, kivizsgálhatja a nemzetbiztonsági szolgálatok jogellenes tevékenységére utaló panaszokat, és vizsgálat lefolytatására kérheti fel a minisztert, ha valamely szolgálat jogszabályellenes tevékenységét feltételezi. Amennyiben a bizottság valamely nemzetbiztonsági szolgálat jogszabályellenes működését észleli, ténymegállapító vizsgálatot folytathat le, mely során betekinthet a szolgálatok nyilvántartásában lévő, az adott ügyre vonatkozó iratokba,

meghallgathatja a szolgálatok munkatársait, valamint felhívhatja a minisztert a szükséges intézkedés megtételére. [Nbtv. 14.§-16.§]

Ahogy a fentebb hivatkozott 23/2013. (XI.22.) AB határozatban az Alkotmánybírósági kifejti, a titkos információgyűjtés szükségképpen kizárja a hatékony jogorvoslat lehetőségét, ezért annak megítéléséhez, hogy a szabályozás megfelelő garanciát nyújt-e az egyén jogainak védelmére az alkalmazást három szakaszból álló ellenőrzésnek kell alávetni; amikor a beavatkozást elrendelik, mialatt a beavatkozást végrehajtják, miután a beavatkozást befejezték. Az ellenőrzést a végrehajtó hatalomtól független „testületnek" kell végezni. Elsősorban az állandó, folyamatos és kötelező ellenőrzés a garancia arra, hogy a konkrét ügyekben nem sértik meg az arányosság követelményét. A titkos információgyűjtés elrendelésének és végrehajtásának tehát alapvető garanciális eleme a külső ellenőrzés. Az Alkotmánybíróság 2013-as határozatában megállapította, hogy az Nbtv. lehetővé teszi az igazságügyért felelős miniszter engedélyezési eljárásának a végrehajtó hatalomtól független szervek általi ellenőrzését az által, hogy az ellenőrzést az Országgyűlés Nemzetbiztonsági Bizottsága (amely a minisztertől általánosan és konkrét ügyekre vonatkozóan is beszámolót kérhet) és az Ombudsman látta el. Az Emberi Jogok Európai Bíróságának 2016-ban megfogalmazott álláspontja szerint azonban a miniszternek az Országgyűlés Nemzetbiztonsági Bizottsága felé történő beszámolási kötelezettsége, valamint az Ombudsman korlátozott vizsgálati jogosultságai nem voltak elegendő garanciának tekinthetők.

II.7.
A Hatóság feladat- és hatásköre a titkos információgyűjtések tekintetében

A Hatóság feladat- és hatásköre az Infotv. 2018-as módosításával bővült a korábbi ombudsmani típusú vizsgálati eljárás nyújtotta lehetőségekhez képest. A Hatóság bejelentés alapján és hivatalból is folytathat vizsgálatot, és az Infotv. szerint az érintett kérelmére valamint hivatalból is folytathat adatvédelmi hatósági eljárást. Megjegyzendő azonban, hogy Hatóság feladat- és hatásköre a nemzetbiztonsági célú adatkezelések ellenőrzésének tekintetében nem új keletű, ilyen hatásköre már az adatvédelmi biztosnak is volt az akkoriban hatályos adatvédelmi törvény (Avtv.)[5] alapján.

A Hatóság mint a végrehajtó hatalomtól független ellenőrző testület, megfelel az Alkotmánybíróság határozatában részletezett kritériumnak, mivel a hatásköre kiterjed a beavatkozás végrehajtása és a beavatkozás befejezése utáni szakaszban történő ellenőrzésre. Az, hogy a Hatóság hatásköre az előzetes ellenőrzésre nem terjed ki, azért nem jelent törvényességi szempontból akadályt, mert, ahogy arra az Alkotmánybíróság határozata utal, az ellenőrzésnek nem az egyes szakaszokban, hanem összességében a három szakaszban kell megfelelőnek és hatékonynak lennie.

A Hatóság feladat- és hatásköre a nemzetbiztonsági szolgálatok adatkezelése, valamint azon belül is a titkos információgyűjtés törvényességi ellenőrzése szempontjából meglehetősen széles körű nemzetközi viszonylatban is. A Hatóság a vizsgálat során megkereste a tagállami adatvédelmi hatóságokat és információt kért a tekintetben, hogy milyen feladat- és hatáskörük van eljárni az adott tagállamok felügyeleti hatóságainak a nemzetbiztonsági célú adatkezelések ellenőrzése során. Az uniós tagállamok adatvédelmi hatóságainak válaszaiból

[5] 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról

megállapítható, hogy számos tagállam felügyeleti hatósága egyáltalán nem rendelkezik a nemzetbiztonsági szolgálatok adatkezelését, így különösen a titkos információgyűjtést érintően felügyeleti-ellenőrzési hatáskörrel, azon tagállamok többsége pedig, amelyek a nemzeti joguk szerint jogosultak a nemzetbiztonsági célú adatkezelések felügyeletére, még soha nem végeztek ilyen jellegű vizsgálatot.

Az előbbiek alátámasztásaként megemlítendő az is, hogy a Hatóság – tudomása szerint – nemzetközi viszonylatban is egyedülálló módon, 2017-ben, egy átfogó audit tevékenység keretében vizsgálta a Nemzetbiztonsági Szakszolgálat adatkezelésének megfelelőségét.

A személyes adatok bűnüldözési, nemzetbiztonsági és honvédelmi célú kezelésére az Infotv.-t kell alkalmazni. Az Infotv. 51/A. § (1) bekezdése szerint a Hatóság hivatalból vizsgálatot indíthat a személyes adatoknak az Infotv. tárgyi hatálya alá tartozó kezelésével összefüggésben.

A jogalkotó az Infotv. tárgyi hatályát az adatkezelési cél alapján állapítja meg, különbséget téve a bűnüldözési célú adatkezelés, a nemzetbiztonsági célú adatkezelés, valamint a honvédelmi célú adatkezelés között. Ezen adatkezelések értelmezési tartományát az Infotv. a következők szerint állapítja meg:

bűnüldözési célú adatkezelés *„a jogszabályban meghatározott feladat- és hatáskörében a közrendet vagy a közbiztonságot fenyegető veszélyek megelőzésére vagy elhárítására, a bűnmegelőzésre, a bűnfelderítésre, a büntetőeljárás lefolytatására vagy ezen eljárásban való közreműködésre, a szabálysértések megelőzésére és felderítésére, valamint a szabálysértési eljárás lefolytatására vagy ezen eljárásban való közreműködésre, továbbá a büntetőeljárásban vagy szabálysértési eljárásban megállapított jogkövetkezmények végrehajtására irányuló tevékenységet folytató szerv vagy személy ezen tevékenység keretei között és céljából - ideértve az ezen tevékenységhez kapcsolódó személyes adatok levéltári, tudományos, statisztikai vagy történelmi célból történő kezelését is - végzett adatkezelés;* [Infotv. 3. § 10.a. pont]

nemzetbiztonsági célú adatkezelés: – *ha törvény eltérően nem rendelkezik – a nemzetbiztonsági szolgálatok jogszabályban meghatározott feladat- és hatáskörében végzett adatkezelése, valamint a rendőrség terrorizmust elhárító szervének jogszabályban meghatározott feladat- és hatáskörében végzett, a nemzetbiztonsági szolgálatokról szóló törvény hatálya alá tartozó adatkezelése;* [Infotv. 3. § 10.b. pont]

honvédelmi célú adatkezelés*: a honvédségi adatkezelésről szóló törvény, továbbá a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről szóló törvény, és a Magyar Köztársaság területén szolgálati céllal tartózkodó külföldi fegyveres erők, valamint a Magyar Köztársaság területén felállított nemzetközi katonai parancsnokságok és állományuk nyilvántartásáról, valamint jogállásukhoz kapcsolódó egyes rendelkezésekről szóló törvény hatálya alá tartozó adatkezelés* [Infotv. 3. § 10.c. pont].

A Hatóság vizsgálatának megindításához tehát nem szükségszerű az érintett bejelentése, konkrét panasza, amellyel az eljárás megindítását kezdeményezi. A Hatóság saját hatáskörében mérlegelve az adott tényállást – azaz, azon körülményeket, hogy személyes

adatok kezelésével, illetve a közérdekű adatok vagy a közérdekből nyilvános adatok megismeréséhez fűződő jogok gyakorlásával kapcsolatban jogsérelem következett-e be, vagy annak közvetlen veszélye fennáll-e – hivatalból is vizsgálatot indíthat.

A Hatóság a vizsgálata során a vizsgált adatkezelő kezelésében lévő, a vizsgált üggyel összefüggésbe hozható összes adatot megismerheti, arról másolatot készíthet, és az összes ilyen iratba – ideértve az elektronikus adathordozón tárolt iratokat is – betekinthet, illetve azokról másolatot kérhet az Infotv. 54. § (1) bekezdése alapján.

A Hatóság a vizsgált üggyel összefüggésbe hozható adatkezelést megismerheti, az adatkezelés helyszínéül szolgáló helyiségbe beléphet, az adatkezelési műveletek végzéséhez használt eszközökhöz hozzáférhet, valamint a vizsgált adatkezelőtől, illetve az adatkezelő bármely munkatársától írásbeli és szóbeli felvilágosítást kérhet. Ezen vizsgálati jogosultsága azonban nem korlátozódik az adatkezelőre, a Hatóság ugyanis nem csak az adatkezelőtől, hanem a vizsgált üggyel összefüggésbe hozható bármely szervezettől vagy személytől írásbeli felvilágosítást és a vizsgált üggyel összefüggésbe hozható adatról – ide érte az elektronikus adathordozón tárolt adatokat is – másolatot kérhet. A Hatóság megkeresésének a vizsgált adatkezelő, illetve a vizsgált üggyel összefüggésbe hozható más szervezet vagy személy a Hatóság által megállapított határidőn belül köteles eleget tenni.

A Hatóság hatásköre csak az igazságügyért felelős miniszter általi külső engedélyezés jogszerűségének ellenőrzésére terjed ki, a bírósági adatkezelési műveletekkel kapcsolatban a személyes adatok védelméhez való jog érvényesülésének ellenőrzésére – a bírósági szervezetrendszeren belül – adatvédelmi kifogás útján kerül sor.

A Hatóság az igazságügyért felelős miniszter általi külső engedélyezés jogszerűségének ellenőrzése során minden egyes esetben megvizsgálja az előterjesztést, hogy az megfelel-e a jogszabályban meghatározott formai és eljárási követelményeknek.

A Hatóság ennek keretein belül vizsgálja, hogy a titkos információgyűjtésre irányuló előterjesztés a titkos információgyűjtés folytatására feljogosított nemzetbiztonsági szolgálat főigazgatójától származik-e, valamint hogy tartalmaz-e minden, az Nbtv. 57. § (2) bekezdésében meghatározott adatot. Az előterjesztésnek tartalmaznia kell a titkos információgyűjtés helyét, az érintett vagy érintettek nevét vagy körét, illetőleg az azonosításra alkalmas – rendelkezésre álló – adatokat. Az előterjesztésnek tartalmaznia kell továbbá a titkos információgyűjtés megnevezését (vagyis az alkalmazni kívánt eszközt és módszert) és szükségességének indokolását, a tevékenység kezdetét és végét napban meghatározva, valamint az Nbtv. 59. § szerinti kivételes engedély iránti előterjesztés esetén annak indokolását, hogy az adott ügyben arra a nemzetbiztonsági szolgálat eredményes működéséhez feltétlenül szükség volt.

A külső engedélyezés jogszerűségének vizsgálata során a Hatóság megvizsgálja, hogy az előterjesztő megfelelően igazolta-e, hogy a titkos információgyűjtés nemzetbiztonsági érdekből szükséges. A Hatóság vizsgálata tehát kiterjed a *nemzetbiztonsági érdek* meglétének és mibenlétének vizsgálatára is. A *„nemzetbiztonsági érdek”* értelmezési tartományát az Nbtv. 74. § a) pontja rögzíti, amelyet adott tényállással összevetve megállapítható vagy kizárható a nemzetbiztonsági érdek fennállása. Mivel a Hatóság minden adatkezelés tekintetében vizsgálhatja, hogy az szükséges és arányos mértékben korlátozza-e az érintettek információs

önrendelkezési jogát, ezért a nemzetbiztonsági érdekre való hivatkozás esetén is vizsgálandó, hogy a nemzetbiztonsági érdek érvényesítése adott esetben a szükséges és arányos mértékben korlátozza-e a titkos információgyűjtéssel érintettek információs önrendelkezési jogát, illetve a magánszférájuk bizalmasságához való jogot.

A Hatóság azt is megvizsgálja, hogy a titkos információgyűjtés külső engedélyezésére vonatkozó előterjesztésben az előterjesztő megfelelően igazolta-e, hogy az adatkezelés célja a titkos információgyűjtés nélkül nem érhető el, valamint, hogy az általa kért eszköz és módszer alkalmazása szükséges-e. Az előterjesztőnek azt is igazolnia kell, hogy a titkos információgyűjtés az általa kért időtartamra nézve feltétlenül szükséges, a Hatóság pedig megvizsgálja, hogy az engedélyt legfeljebb kilencven napra kérték-e, vagy ha kilencven nappal meghosszabbították a titkos információgyűjtés időtartamát, az a törvényi előírás szerint újabb előterjesztéssel és indokolással történt-e.

A Hatóság feladata annak vizsgálata is, hogy az előterjesztésben foglaltakból okszerűen következik-e az igazságügyért felelős miniszter döntése. A miniszter az előterjesztés benyújtásától számított 72 órán belül határozatot hoz arról, hogy az előterjesztésnek helyt ad, vagy azt megalapozatlansága esetén elutasítja. A Hatóság tehát nem csak az előterjesztések formai és eljárási követelményeit ellenőrzi, hanem az egyes előterjesztésekhez tartozó – igazságügyért felelős miniszter által hozott – határozatokat is.

Minden határozat esetében fontos annak a vizsgálata, hogy az igazságügyért felelős miniszter a külső engedély megadását az adott előterjesztésben részletezett tényekre és körülményekre tekintettel megindokolja-e. A 32/2013. (XI.22.) AB határozat 1. pontja alkotmányos követelmény meghatározásával az utólagos külső kontroll érvényesülésének előfeltételeként utalt a külső engedély indokolási kötelezettségére. Ebből következően az indokolásnak olyan részletesnek és egyéniesítettnek kell lennie, hogy az utólagos külső kontroll során ellenőrizni lehessen a döntés során figyelembe vett tényeket és körülményeket, valamint az azok alapján hozott döntés tartalmi megfelelőségét.

Az Infotv. 71. § (1) bekezdése szerint a Hatóság az eljárása során – az annak lefolytatásához szükséges mértékben és ideig – kezelheti mindazon személyes adatokat, valamint törvény által védett titoknak és hivatás gyakorlásához kötött titoknak minősülő adatokat, amelyek az eljárással összefüggnek, illetve amelyek kezelése az eljárás eredményes lefolytatása érdekében szükséges. Az Infotv. 71. § (3) bekezdése szerint a Hatóság az alapvető jogok biztosáról szóló 2011. évi CXI. törvény (a továbbiakban: Ajbtv.) 23. § (2) bekezdésében meghatározott adatokat az Ajbtv. 23. § (7) bekezdésében[6] meghatározottak szerint ismerheti meg. E korlátozás értelmében a vizsgálat nem terjedhetett ki a titkos információgyűjtésre használt eszközök és módszerek működésének és működtetésének műszaki-technikai adataira, az azokat alkalmazó személyek azonosítását lehetővé tevő adatokra, valamint a rejtjeltevékenységgel és kódolással kapcsolatos adatokra.

[6] Ajbtv. 23. § (7) bekezdés: *Ha az alapvető jogok biztosa az ügy teljes körű feltárása érdekében az Ajbtv. 23.§ (1)-(6) bekezdésben meghatározott iratok megvizsgálását is szükségesnek tartja, a feladatkörrel rendelkező minisztertől kérheti azok megvizsgálását. A feladatkörrel rendelkező miniszter köteles az alapvető jogok biztosa által megkívánt vizsgálatot elvégezni vagy elvégeztetni, és a vizsgálat eredményéről az alapvető jogok biztosát az általa megállapított határidőn belül tájékoztatni.*

A Hatóság az Infotv. 71. § (3) bekezdésre tekintet nélkül megismerheti az Ajbtv. 23. § (3) bekezdés e) pontjában, (4) bekezdés f) pontjában és (5) bekezdés d) pontjában meghatározott adatot, ha az az együttműködő személy személyes adatainak védelmével kapcsolatban indult vizsgálati eljárásban, adatvédelmi hatósági eljárásban vagy titokfelügyeleti hatósági eljárásban szükséges. Megismerheti továbbá az Ajbtv. 23. § (3) bekezdés f) pontjában és (4) bekezdés g) pontjában meghatározott, a titkos információgyűjtés folytatása vagy a leplezett eszközök alkalmazása érdekében használt eszközöket és módszereket alkalmazó személyek azonosítását lehetővé tevő adatot, ha az e személyek személyes adatainak védelmével kapcsolatban indult vizsgálati eljárásban, adatvédelmi hatósági eljárásban vagy titokfelügyeleti hatósági eljárásban szükséges. Ha a Hatóság által vizsgálni kívánt irat olyan adatot is tartalmaz, amelyet a Hatóság csak a (3) bekezdés szerint ismerhet meg, az irat megismerését a meg nem ismerhető adat felismerhetetlenné tételével kell a Hatóság részére lehetővé tenni. [Infotv. 71. § (3a), (3b), (3c) bekezdések]

Az Infotv. tehát a Hatóság adat megismerési lehetőségei tekintetében differenciált szabályozást vezet be aszerint, hogy az érintett adatok Hatóság általi közvetlen megismerése milyen mértékben járhat más alapvető jogok sérelmének veszélyével, illetve milyen mértékű az adat közvetlen megismeréséhez fűződő jogvédelmi igény.

III. A Hatóság vizsgálatának menete

III.1.
A vizsgálat megindítása

A Hatóság – az Infotv. 51/A. § (1) bekezdése alapján – 2021. augusztus 9. napján hivatalból vizsgálatot indított annak megállapítására, hogy a magyar bűnüldöző szervek és nemzetbiztonsági szolgálatok alkalmazzák-e a sajtóhírekben megjelent „Pegasus” nevű kémszoftvert, és ha igen, e tevékenységük összhangban van-e a személyes adatok kezelésére és védelmére vonatkozó jogszabályi előírásokkal.

A Hatóság feladata annak kivizsgálása volt, hogy az Nbtv. 56. § szerinti eszközök és módszerek alkalmazása során az igazságügyért felelős miniszter által engedélyezett titkos információgyűjtésre feljogosított szervek adatkezelése a jogszabályoknak megfelelően működik-e, valamint, hogy a nyilvánosságra került személyek esetében történt-e titkos információgyűjtés, és ha igen, az jogszerűen történt-e. Az érintett szerveknél (megrendelőknél) a vizsgálat tárgyát képező alkalmazással végzett titkos információgyűjtéssel összefüggésben történő adatkezelések általános vizsgálatához a Hatóság egy ún. mintavételezési vizsgálati metódust használt.

A tárgyban publikált sajtómegjelenésekben hivatkozott, 300 magyar állampolgár nevét és telefonszámát tartalmazó lista[7] a vizsgálat megindításának időpontjában nem állt a Hatóság rendelkezésére. Ezen állítólagos lista beszerzése iránt a Hatóság – az előzőekben ismertetett vizsgálati jogosultságait gyakorolva – eljárási cselekményeket végzett az alábbiak szerint.

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

2021. augusztus 11-én kelt levelében a Hatóság arra kérte az Amnesty International Magyarország Egyesület igazgatóját, hogy az Infotv. 54. § (1) bekezdés d) pontjára tekintettel 15 napon belül küldje meg a Hatóság részére az Amnesty International rendelkezésére álló, vélelmezhetően magyar állampolgárságú személyek személyazonosító adatait és telefonszámait tartalmazó listát. Mivel az Amnesty International Magyarország Egyesület a Hatóság megkeresésére nem válaszolt, a Hatóság 2021. szeptember 13-án újra megkereste az igazgatót, és ismételten kérte, hogy az Infotv. 54. § (1) bekezdés d) pontjára tekintettel küldje meg a listát.

Az Amnesty International Magyarország Egyesület 2021. szeptember 16-i válaszában arról tájékoztatta a Hatóságot, hogy *„az érintett telefonszámokkal kapcsolatban, ideértve a potenciálisan magyar állampolgárokhoz kapcsolódó telefonszámokat is, az 50 000 érintett telefonszám közül azon esetekben, ahol az Amnesty International Security Lab nem végzett saját vizsgálatot, nem tudjuk adatok átadásával segíteni a Hivatal vizsgálatát, mert sem az Amnesty International Magyarország Egyesületnek, sem az Amnesty International Nemzetközi Titkárságának nincs hozzáférése ehhez a listához. Azokban az esetekben, ahol az Amnesty International forenzikus vizsgálatot végzett és bizonyítani tudta a megfertőződét vagy az érintettséget, az eredményeket a készülékek tulajdonosainak tudomására hozta, valamint nyilvánosságra hozta a forenzikus vizsgálat módszertanát a fentiek szerint.”*

A Hatóság 2021. október 6-án kelt újabb megkeresésében arra kérte az Amnesty International Magyarország Egyesület igazgatóját, hogy a válaszlevelében hivatkozott azon személyek nevének és telefonszámának listáját küldje meg, akik esetében elvégezték a forenzikus vizsgálatot, és bizonyítani tudták az érintettséget.

Az Amnesty International Magyarország Egyesület igazgatója 2021. október 18-án kelt válaszában arról tájékoztatta a Hatóságot, hogy *„az Egyesület egy Magyarországon bejegyzett jogi személy és adatkezelőként elválik a Nemzetközi Titkárságtól és egyéb Amnesty International entitásoktól”,* az igazgató hangsúlyozta továbbá, *hogy „[e]gyesületünk nem rendelkezik a levelében kért adatokkal, azokat az adatokat nem kezeltük és nem kezeljük, illetve az adatok vonatkozásában adatfeldolgozónak sem minősülünk. Annak érdekében, hogy vizsgálatát minél nagyobb sikerrel folytathassa le, kérjük, vegye fel a kapcsolatot az Amnesty International Nemzetközi Titkárságával”.*

A Hatóság 2021. november 19-én kelt levelében tájékoztatta az Amnesty International Magyarország Egyesület igazgatóját, hogy a Hatóság a vizsgálata során a vizsgált üggyel összefüggésbe hozható bármely szervezettől vagy személytől írásbeli felvilágosítást, illetve a vizsgált üggyel összefüggésbe hozható adatról, iratról – ideértve az elektronikus adathordozón tárolt iratokat is – másolatot kérhet. Az Infotv. 54. § (1) bekezdés d) pontja alapján a Hatóság felszólításának akkor is köteles eleget tenni az Amnesty International Magyarország Egyesület – mint a vizsgált üggyel összefüggésbe hozható szervezet – ha a kért adatok tekintetében sem adatkezelőnek, sem adatfeldolgozónak nem tekinti magát.

A Hatóság 2021. november 29-én kelt levelében megkereste az Amnesty International londoni székhelyű Nemzetközi Titkárságát, és kérte, hogy küldje meg a Hatóság részére az Amnesty International rendelkezésére álló magyar személyek személyazonosító adatait és telefonszámait tartalmazó listát a Hatóság sikeres vizsgálatának lefolytatásához.

Tekintettel arra, hogy az Amnesty International Nemzetközi Titkársága nem válaszolt a Hatóság megkeresésére, a Hatóság 2021. december 10-én ismételten elküldte a megkeresését a londoni székhelyű szervezetnek.[8]

Az előzőekben jelzetteken túl tisztázandó kérdés volt továbbá, hogy a magyar személyekhez köthető telefonszámok – amelyek esetében az Amnesty International Security Lab elnevezésű egysége megállapította, hogy azok a kémszoftverrel megfertőződtek – miként kerülhettek nyilvánosságra az izraeli székhelyű NSO csoport szoftverét érintő úgynevezett Pegasus Project nevű tényfeltáró vizsgálat során, amelyben 10 ország, 17 médiavállalatának 80 újságírója vett részt.

III.2.
A tényállás tisztázásának módszere

A Hatóság a tényállás tisztázásának érdekében első lépésként egy vizsgálati tervet dolgozott ki, amelyben rögzítette a vizsgálat lefolytatásához szükséges vizsgálati cselekmények tervezett menetét, a vizsgálni kívánt adatkezelők lehetséges körét, valamint a vizsgálat módszertanát. A vizsgálati tervről készült feljegyzés mellékletét képezi az egyes ügyirat- és engedélyszámok mintavételezéshez történő leválogatásának módszertana.

A Hatóság ennek megfelelően a Nemzetbiztonsági Szakszolgálattól kért statisztikai adatszolgáltatást követően, kikérte a megrendelő szervektől az eszközalkalmazásra vonatkozó összes ügy ügyirat- és engedélyszámát, amely ügyirat- és engedélyszámokból mintavételezés során előállított ügyiratlistán szereplő összes iratot és dokumentációt leellenőrzött a helyszíni vizsgálatok során.

A Hatóság a vizsgálat során a tényállás tisztázása érdekében a következő vizsgálati cselekményeket foganatosította:

- A Hatóság a vizsgálat keretében megkereste a Nemzetbiztonsági Szakszolgálat főigazgatóját a tényállás tisztázása érdekében szükséges információk rendelkezésre bocsátása érdekében, valamint statisztikai adatszolgáltatást kért *az* eszközalkalmazást illetően.
- A Hatóság helyszíni vizsgálatot tartott a Nemzetbiztonsági Szakszolgálatnál, szóbeli felvilágosítást, valamint iratmásolatokat kért, továbbá betekintett a vonatkozó dokumentációkba.
- A Hatóság helyszíni ellenőrzést tartott az egyes megrendelő szerveknél is, amelynek során a vonatkozó iratanyagba történő betekintéssel vizsgálta meg a külső engedélyezés jogszerűségét.
- A Hatóság elnöke részt vett az Országgyűlés Nemzetbiztonsági Bizottságának zárt ülésén, amelyen a vizsgálat tárgyára vonatkozó tájékoztató hangzott el.
- A Hatóság elnöke kikérte azon további zárt üléseknek a jegyzőkönyvét is az Országgyűlés Nemzetbiztonsági Bizottságától, amely ülések napirendjén szerepelt a vizsgálat tárgyát képező „Pegasus“ kémszoftver.

[8] Jelen kézirat lezárásának időpontjáig az Amnesty International Nemzetközi Titkársága érdemi választ nem küldött a Hatóságnak, de 2022. január 7-én egy e-mailben jelezte, hogy a megkeresést megkapta.

- A Hatóság a sajtóban megjelent hírekre hivatkozva az Amnesty International magyarországi egyesületét is megkereste és az Infotv. 54. § (1) bekezdés d) pontjára tekintettel kérte, hogy küldje meg a Hatóság részére a vizsgálattal összefüggésben a sajtóban megjelent információk alapján rendelkezésére álló, vélelmezetten magyar állampolgárságú érintettek személyes adatait és telefonszámait tartalmazó listát.
- A Hatóság megkereste az Amnesty International Nemzetközi Titkárságát is és kérte, hogy küldje meg a Hatóság részére a vizsgálattal összefüggésben a sajtóban megjelent információk alapján rendelkezésére álló, vélelmezetten magyar állampolgárságú érintettek személyes adatait és telefonszámait tartalmazó listát.
- A Hatóság informatikus szakértőt vont be a vizsgálatába annak érdekében, hogy a szoftverrel kapcsolatos minden elérhető információt ellenőrizni tudjon.

Fontos megjegyezni, hogy a vizsgálat tárgyát képező dokumentációkban az Infotv. 71. § (3) – (3c) bekezdések értelmében lehetnek olyan adatok, amely adatokat a Hatóság nem ismerhet meg. A Hatóság e szerint nem ismerheti meg a titkos információgyűjtésre használt eszközök és módszerek működésének és működtetésének műszaki-technikai adatait tartalmazó vagy az azokat alkalmazó személyek azonosítását lehetővé tevő iratokat, a rejtjeltevékenységgel és kódolással kapcsolatos iratokat, az olyan iratokat, amelyeknek megismerése az információforrás azonosítását lehetővé tenné, valamint az olyan iratokat, amelyeknek megismerése a nemzetbiztonsági szolgálatok külföldi partnerszolgálatok irányában vállalt kötelezettségeit sértené. Ezen adatok előfordulása esetén a Hatóság ezen adatok felismerhetetlenné tétele mellett iratmásolatokat kérhet, illetve a tárgykör szerint illetékes minisztert kérheti fel az iratok megvizsgálására.

Tekintettel arra, hogy a vizsgálat tárgyát képező dokumentumok minősített adatokat tartalmaznak, a vizsgálat eredményének dokumentálása során a minősített adat védelméről szóló 2009. évi CLV. törvény (Mavtv.) 7. § (1) bekezdés szerint került sor a minősítési jelölés megismétlésére.

III.3.
A titkos információgyűjtésre vonatkozó törvényi feltételek fennállásának vizsgálata

A titkos információgyűjtés utólagos külső kontrollja érvényesülésének előfeltétele az engedélyezés indokolása. Az igazságügyért felelős miniszteri engedélyt olyan részletes indokolással kell ellátni, hogy a Hatóság utólagos ellenőrzése alkalmával vizsgálni lehessen a döntés során figyelembe vett tényeket és körülményeket, és a döntés tartalmi megfelelőségét. A Hatóság az egyes adatkezelőknél végzett helyszíni ellenőrzés keretében megvizsgálta a külső engedélyhez kötött titkos információgyűjtés engedélyezésére irányuló előterjesztéseket és a külső engedélyezésről szóló döntést tartalmazó igazságügyi miniszteri határozatokat is.

A Hatóság a fentebb részletezett vizsgálati metódusok (konkrét személyek listája és mintavételezéssel leválogatott ügyszámok szerinti lista) használatával összesen közel száz előterjesztés, valamint ahhoz tartozó igazságügyi miniszteri határozat megfelelőségét vizsgálta meg, az alább felsorolt – a külső engedélyezés jogszerűségére vonatkozó – kérdések mentén:

- Betartotta-e az előterjesztő a formai és eljárási szabályokat?
- A főigazgatótól származik-e az előterjesztés?
- Valamennyi, az Nbtv. 57. § (2) bekezdésben meghatározott adatot tartalmaz-e az előterjesztés?
- Határidőn belül történt-e az engedélyezés?
- Az engedély érvényessége nem haladja-e meg a 90 napot?
- Tartozik-e indokolás az engedélyhez?
- Amennyiben sor került kivételes engedélyezésre, úgy betartották-e annak szabályait?
- Igazolta-e az előterjesztő, hogy a titkos információgyűjtés nemzetbiztonsági érdekből szükséges?
- Igazolta-e az előterjesztő, hogy az adatkezelés célja a titkos információgyűjtés nélkül nem érhető el?
- Igazolta-e az előterjesztő, hogy valamennyi általa kért eszköz és módszer alkalmazása szükséges?
- Igazolta-e az előterjesztő az általa kért titkos információgyűjtés időtartamának szükségességét?
- Okszerűen következik-e az előterjesztésben foglaltakból az igazságügyért felelős miniszter döntése?
- Kellő részletességgel, az adott előterjesztésben elé tárt tényekre és körülményekre reflektálva indokolta-e meg az igazságügyért felelős miniszter a külső engedély megadását?

A fentiek kapcsán fontos kitérni a „*nemzetbiztonsági érdek”* fogalmára, amelynek értelmezési tartományát az Nbtv. 74. § a) pontja meghatározza meg:

„Magyarország függetlenségének biztosítása és törvényes rendjének védelme, ennek keretén belül
aa) az ország függetlensége és területi épsége elleni támadó szándékú törekvések felderítése,
ab) az ország politikai, gazdasági, honvédelmi érdekeit sértő vagy veszélyeztető leplezett törekvések felfedése és elhárítása,
ac) a kormányzati döntésekhez szükséges, külföldre vonatkozó, illetve külföldi eredetű információk megszerzése,
ad) az ország az alapvető emberi jogok gyakorlását biztosító törvényes rendjének, a többpárti rendszeren alapuló képviseleti demokráciának és a törvényes intézmények működésének jogellenes eszközökkel történő megváltoztatására vagy megzavarására irányuló leplezett törekvések felderítése és elhárítása, valamint
ae) a terrorcselekmények, az illegális fegyver- és kábítószer-kereskedelem, valamint a nemzetközileg ellenőrzött termékek és technológiák illegális forgalmának felderítése és megakadályozása;”.

A titkos információgyűjtés igazságügyért felelős miniszter általi engedélyezésének ellenőrzése során a Hatóság figyelembe vette az igazságügyért felelős miniszter által a sajtóban tett korábbi nyilatkozatát is, mely szerint *„az engedélyek ki vannak szervezve, az aláírásra az államtitkár úrnak, Völner Pál államtitkár úr az, aki az engedélyeket megadja vagy éppen megtagadja, az Igazságügyi Minisztérium ebben a titkos információgyűjtésnek az alkotmányos rendjében egyedül a jogszabályok betartásáért, a jogszabályi kellékek meglévő tartalmáért*

felel, nem azért, hogy milyen szakmai tartalom kerül az asztalunkra”.[9]

Az Nbtv. 58. § (2) bekezdése kifejezetten az igazságügyért felelős miniszter jogkörébe utalja az engedélyezési jogkört és nem ad felhatalmazást az engedélyezési jogkör átruházására. A központi államigazgatási szervekről, valamint a Kormány tagjai és az államtitkárok jogállásáról szóló 2010. évi XLIII. törvény 5. § (3) bekezdése lehetővé teszi, hogy a központi államigazgatási szerv szervezeti és működési szabályzata a szerv vezetőjének hatáskörébe tartozó egyes ügyekben a kiadmányozási jogot a törvényben felsorolt posztokat betöltő személyre átruházhassa, aki a döntés meghozatala során a szerv vezetője nevében jár el. Az Igazságügyi Minisztérium Szervezeti és Működési Szabályzatáról szóló 9/2019. (VIII.1) IM utasítás (a továbbiakban: IM SZMSZ) 5. § (1) és (2) bekezdései a helyettesítés rendjét határozzák meg arra az esetre, ha a miniszter akadályoztatva van. A kiadmányozás szabályai az IM SZMSZ V. fejezet 31. címe alatt találhatók. Ebben a titkos információgyűjtés engedélyezésére vonatkozó kiadmányozás átruházása nincs megemlítve.

Ezzel összefüggésben rögzíteni szükséges, hogy az Alkotmánybíróság a 23/2018. (XII.28.) AB határozatában rámutatott arra, hogy *„a kiadmányozási jogkörben eljáró személynek csak aláírási joga van, amely aláírási jog nem tartalmaz döntési jogosultságot, viszont tanúsítja azt, hogy a kiadott döntés hiteles, egyező tartalmú azzal, amelyet eredetben a hatáskör címzettje hozott és aláírt. A hatáskör gyakorlójának tehát van hatásköre mind a kiadmányozásra, mind a kiadmányozási jog átruházására, az a személy azonban, akinek jogszerűen átengedték a kiadmányozást, nem jogosult a hatáskör gyakorlására, nem jogosult közigazgatási jogviszonyban döntés hozatalára”.*

A fentiek miatt a Hatóság a vizsgált igazságügyi miniszteri határozatok kapcsán megkereste dr. Völner Pált, az Igazságügyi Minisztérium államtitkárát, aki 2021. november 8-án kelt válaszában úgy nyilatkozott, hogy a Hatóság megkeresésében *„felsorolt iktatószámú engedélyek esetében a miniszter akadályoztatása miatt helyettesítési jogkörben kerültek aláírásra az engedélyek”.*

A Hatóság az eljárásában kizárólag a vizsgálattal érintett igazságügyi miniszteri határozatokat ellenőrizte, nem általánosságban vizsgálta azt, hogy az engedélyezési eljárásban hogyan alakul a kiadmányozás rendje. Ez utóbbira a hatályos jogszabályi rendelkezések szerint az Országgyűlés Nemzetbiztonsági Bizottsága jogosult. Ahogy ugyanis arra a 32/2013. (XI.22.) AB határozat is utal, *„az igazságügy miniszter engedélyezési eljárása fölött az Nbtv. 14. § (4) bekezdése értelmében az Országgyűlés Nemzetbiztonsági Bizottsága gyakorol ellenőrzést”*. Az Alkotmánybíróság által hivatkozott Nbtv. 14. § (4) bekezdés b) pontja szerint az Országgyűlés Nemzetbiztonsági Bizottsága tájékoztatást kérhet az igazságügyért felelős minisztertől, a polgári nemzetbiztonsági szolgálatok irányításáért felelős minisztertől, a polgári hírszerzési tevékenység irányításáért felelős minisztertől, a honvédelemért felelős minisztertől és a főigazgatóktól az 56. §-ban és az 59. §-ban meghatározott engedélyezési eljárásról.

IV. A vizsgálat tárgyát képező szoftver

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

A Hatóság a „Pegasus” kémszoftverrel kapcsolatos hírek és információk elemzésére az Alverad Technology Focus Kft.-t kérte fel. Az információbiztonsági szakértő az alábbi összefoglaló elemzést készítette a „Pegasus” szoftverről.

IV.1.
Összefoglaló elemzés

Az események háttere és szereplői

Az NSO Group vállalati és személyi háttere

A Pegasus kémprogramot az Izraelben működő NSO Group alkotta meg. Az NSO Group a kiberhírszerzés területén működő, általában „Surveillance-For-Hire[10]” vállalatnak tekintett szervezet, amely megfigyelési technológiákat fejleszt, illetve megfigyelési infrastruktúrát épít fel és ad bérbe ügyfelei, jellemzően nemzetállamok és kormányok részére.

Az NSO az alapítók nevének kezdőbetűiből nyerte saját nevét, a vállalatot Niv Karmi, Shalev Hulio és Omri Lavie hozta létre 2010-ben. Míg Hulio és Lavie esetében ismert tény, hogy korábban az izraeli hadsereg jelfelderítő és kiberhírszerző részlegénél szolgáltak (Unit 8200), addig Karmi esetében csak annyi ismert, hogy őrnagyként szolgált a különleges erőknél, illetve a hírszerző közösség egyik „legkiemelkedőbb” szervezeténél[11] (esetében is felmerült a Unit 8200 neve, ezt azonban még a vele készült interjúban sem erősítette meg).

Az NSO hivatalos története szerint a cég egy civil felhasználású eszközt fejlesztett ki, amely segítségével a szolgáltatók távolról karbantarthatták és beállíthatták a felhasználók mobiltelefonjait. Az SMS-ben küldött linkre a felhasználó rákattintott, a szolgáltató pedig hozzáfért az eszközhöz és elvégezhették a beállításokat. Később a titkosszolgálatok azzal keresték meg Huliot és Laviet, hogy igényeik és céljaik szerint alakítsák át a megoldást. Az átalakítás után született meg a Pegasus kémprogram.

Karmi állítása szerint azonban a másik két alapító maga látott új üzleti lehetőséget a civil eszköz kémprogrammá történő átalakításában és ők keresték meg Karmit és kérték a közreműködését. Karmi néhány hónappal később elhagyta az NSO-t, mivel nem értett egyet a társai üzleti döntéseivel és Polus Tech[12] néven megalapította saját vállalkozását, amely hordozható, mobil cellatorony-rendszereket fejleszt és épít ki.

2014-ben a Francisco Partners technológiai befektetési társaság megvásárolta a céget 130 millió dollárért, de 2019-ben Lavie és Hulio az európai Novalpina Capital befektetési csoporton keresztül többségi részesedést vásárolt vissza az akkor már egymilliárd dollár értékre becsült

---

[10] Surveillance-For-Hire – Bérelhető megfigyelési, lehallgatási, nyomkövetési szolgáltatás. Az ilyen szervezetek megfigyelést vagy lehallgatást nem végeznek, csak fejlesztik és bérbe adják a tevékenységhez szükséges technológiákat és szolgáltatásokat. A megfigyelést vagy lehallgatást a technológia vagy a szolgáltatás felhasználásával az ügyfelek végzik, de jelen pillanatban több szempontból sem biztos, hogy az NSO tevékenysége kimerül a rendszer és a licenszek leszállításával és beüzemelésével. Egyes jelek arra is utalhatnak, hogy az NSO olyan központi szolgáltatásokat is biztosít, amelyek jelentősen közrejátszanak az eszközök megfertőzésében, ez pedig operatív tevékenységet jelenthet.

[11] Forrás: https://www.zeit.de/digital/datenschutz/2021-10/nso-group-technologies-gruender-niv-karmi-pegasus-ueberwachungssoftware

[12] https://polustech.com/

vállalatból.

A jelentős értéknövekedés annak is köszönhető, hogy 2014-ben a szintén a Francisco Partners tulajdonába került Circles kiberhírszerző cég és az NSO Group összeolvadt[13]. A Circles is izraeli alapítású vállalat, amely mobil megfigyelésre és nyomon követésre szakosodott. A mára csaknem 500[14] alkalmazottat foglalkoztató NSO Group értéke jelenleg 1,5 milliárd dollárra becsülhető.

Az NSO Group az egyik legerősebb képességekkel rendelkező, bérelhető megfigyelési szolgáltatásokat biztosító és kiberhírszerzési igényeket kiszolgáló vállalat. A bérelhető megfigyelési infrastruktúra szolgáltatás, illetve a magán kiberkémkedési szektor sokmilliárd dolláros piacot jelent, amelyen az NSO Groupnak több jelentős versenytársa is akad, például 2021 decemberében a Facebookot tulajdonló Meta és a Citizen Lab együttesen azonosított további négy izraeli hátterű magán kiberhírszerző vállalatot (Cobwebs, Cognyte, Black Cube, Blue Hawk) és három egyéb szervezetet, akik a Facebook platformját használták fel műveleteikhez[15].

Ian Beer és Samuel Groß, a Google Project Zero kiberbiztonsági kutatói a Pegasus vizsgálata után egyenesen az egyik legfejlettebb technológiájú támadókódnak nevezték a Pegasust, amelyet valaha csak láttak, és véleményük szerint Pegasust létrehozó képesség legfeljebb csak néhány nemzetállamra jellemző.

A vizsgálatokban résztvevő szervezetek és szerepük

Pegasus Project

A Pegasus Project[16] ernyőszervezet alatt 17 olyan nemzetközi médiaszervezetet fog össze, amelyek közreműködtek a Pegasus tevékenységével kapcsolatos oknyomozói munkában és vizsgálatban, illetve tagja az Organized Crime and Corruption Reporting Project[17] (OCCRP) nemzetközi újságíró szervezet is. Az ernyőszervezet alatt 10 ország[18] 80 újságírója működött közre a vizsgálatban.

Forbidden Stories

A Riporterek Határok nélkül (Reporters Without Borders) és Freedom Voice Network által 2017-ben alapított nonprofit szervezet célja, hogy nemzetközi és helyi konzorciumokon keresztül biztosítsa a szabad sajtó működését. A szervezet olyan nemzetközi hálózatot[19] és platformot épített ki, amelyek segítségével a megfenyegetett, elhallgattatott vagy meggyilkolt

---

[13] Az NSO Group (amely ekkor már a Francisco Partners érdekeltségébe tartozott) az OSY Technologies nevű luxemburgi leányvállalatán keresztül vásárolta fel a Circles-t tulajdonló céget. Forrás: https://forensicnews.net/the-covert-reach-of-nso-group/
[14] A 2014-es felvásárlás időszakában az NSO Group 50 alkalmazottal működött.
[15] A Meta az érintett vállalatokat eltiltotta a platform használatától, illetve a műveletekhez használt 1500 profilt is törölte.
[16] https://forbiddenstories.org/about-the-pegasus-project/
[17] Szervezett Bűnözést és a Korrupciót Feltáró Projekt
[18] Egyesült Királyság, Franciaország, Németország, Egyesült Államok, Izrael, Mexikó, Belgium, India, Szíria, Magyarország
[19] https://web.archive.org/web/20210719090134/https://forbiddenstories.org/our-network/

újságírók munkája folytatható, publikálható és terjeszthető[20].

A Forbidden Stories és az Amnesty International szerezte meg azt az 50 000 telefonszámot tartalmazó listát, amely alapjául szolgált a vizsgálatokhoz és a lehetséges érintettek azonosításához. A lista forrása nem ismert, forrásvédelmi okokra hivatkozva a Forbidden Stories és az Amnesty International nem hozta nyilvánosságra, honnan származik a lista és hogyan jutottak hozzá. Még a Pegasus Projectben közreműködő médiaszervezetek és újságíróik sem ismerik a forrást.

Amnesty International (AI)

Az Amnesty International az egyik legnagyobb és legismertebb jogvédő civil szervezet, amelyet 1960-ban alapítottak, és amely hétmillió taggal, támogatóval és aktivistával rendelkezik csaknem 150 országban. A szervezet helyi irodákat üzemeltet a régiókban, így Magyarországon is működik helyi iroda.

Az Amnesty Tech[21] az AI technikai divíziója, amely a technológiák felhasználásának emberi és személyiségi jogokra gyakorolt hatását kutatja és ellenőrzi, illetve fontos feladata a civil társadalom elleni kibertámadások (beleértve a kémprogramokat vagy más, egyéb lehallgató vagy megfigyelő rendszereket) felderítése és kivizsgálása. Az Amnesty Tech égisze alatt 2019-ben létrejött Security Lab csoport biztosította a Pegasus Project keretein belül a szükséges technikai kompetenciát és támogatást[22].

Az Amnesty International 2021 július 18-án publikálta azt a vizsgálati riportot[23], amely részletesen dokumentálja az általuk alkalmazott vizsgálati módszertant és a vizsgálat eredményeit.
Az Amnesty International már 2018-ban észlelte az NSO Group által fejlesztett Pegasus tevékenységét, egyik munkatársuk mobilkészülékén azonosították[24] a Pegasus kártevőt.

Citizen Lab

A Torontói Egyetemen működő Citizen Lab egy független kutatólaboratórium, amely főleg civil társadalom elleni digitális kémkedéssel és egyéb, kiberbiztonsággal kapcsolatos kutatásokat és vizsgálatokat végez. A Citizen Lab jellemzően vegyes, több területet is átfedő módszertant használ a kutatásai során, politikai, jogi és informatikai elemzéseket alkalmaznak. A Citizen Lab több más, az NSO Grouphoz hasonló szervezet működését is nyomon követi. Az NSO Group tevékenységének vizsgálatával 2016 óta foglalkoznak, első jelentésüket[25] 2016 augusztusában publikálták, Ahmed Mansoor emberi jogi aktivista mobilkészülékén találták meg a Pegasus fertőzést.
Mivel a Citizen Lab már korábban is vizsgálta az NSO Group tevékenységét, illetve a Pegasus

---

[20] https://rsf.org/en/news/launch-forbidden-stories-project
[21] https://www.amnesty.org/en/tech/
[22] Az Amnesty Tech méretére a társalapító korábbi vezető Tanya O'Carroll LinkedIn profiljából lehet következtetni, a feltüntetett munkatapasztalatok között szerepel, hogy az Amnesty Tech igazgatójaként 20 főt irányított 6 országon keresztül.
[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/
[25] https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/

eszköz nyomait, az Amnesty International felkérte a Citizen Lab-ot arra, hogy vizsgálják meg és validálják az AI módszertanát, illetve ellenőrizzék az Amnesty International vizsgálatának eredményét. A Citizen Lab megerősítette az Amnesty International kutatásának eredményeit, a kiadott dokumentum alapján[26] az AI módszertanát megalapozottnak, a vizsgálati eredményeket helyesnek találta, illetve a két csoport egymástól függetlenül ugyanazon eredményekre jutott.

Az Amnesty Tech Security Lab továbbá négy olyan iPhone eszköz biztonsági másolatát osztotta meg a Citizen Lab szakembereivel, amelyeket a Security Lab is megvizsgált. A Citizen Lab a saját vizsgálataival mind a négy esetben igazolta a Security Lab eredményeit, egymástól függetlenül a két csoport is megtalálta az eszközökön a Pegasus kártevő nyomati.

A kiszivárgott telefonszámokat tartalmazó lista

A Pegasus Project kulcsfontosságú eleme egy 50 000 telefonszámot tartalmazó, „kiszivárgott" lista. A listán szereplő telefonszámok a Pegasus Project szerint 2016 óta valamilyen módon érintettek a Pegasus kémprogram tevékenységében. Az adatok tartalmazzák a számok kiválasztásának, illetve a rendszerbe való bevitelének időpontját és dátumát is.

A lista forrása ismeretlen, illetve a kiszivárgás körülményeiről sem áll rendelkezésre információ. Nem lehet tudni, hogy ki és mi alapján állította össze a listát és hogyan jutott el a lista a Pegasus Project ernyőszervezethez vagy az Amnesty International-hoz, illetve az sem ismert, hogy a telefonszámok és időpontok mellett milyen egyéb adatok szerepelnek a listán.

A kiszivárgott listában szereplő adatok alapján a Pegasus Project médiapartnerei tíz olyan kormányt azonosítottak, amelyekről úgy vélik, hogy felelősek a célpontok kiválasztásáért[27].
A lista körül nagy a bizonytalanság. A listával kapcsolatos megfogalmazások, félreértelmezhetők és nem feltétlenül egyeznek meg közvetlen vagy mögöttes jelentésükben:

- *„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 israeli company NSO Group" – Forbidden Stories*

Az NSO Group határozottan visszautasítja[28], hogy a tevékenységükkel vagy ügyfeleik tevékenységével állna kapcsolatban a lista, álláspontjuk szerint lista nem az NSO ügyfelek célpontjainak vagy potenciális célpontjainak listája.

Az NSO válaszában megjelent egy célzás arra, hogy a listán szereplő telefonszámok származhatnak publikus szolgáltatásokból, többek között akár HLR keresési szolgáltatásból, amely nem áll kapcsolatban az NSO-val vagy a vállalat szolgáltatásával.

A Honos Előfizetői Helyregiszter (Home Location Register) a mobil szolgáltatók egyik olyan „adatbázisa", amely az adott szolgáltatóval kapcsolatban tartalmazza az előfizetőre vonatkozó

---

[26] https://citizenlab.ca/2021/07/amnesty-peer-review/
[27] Azerbajdzsán, Bahrein, Kazahsztán, Mexikó, Marokkó, Ruanda, Szaúd-Arábia, Magyarország, India és az Egyesült Arab Emírségek
[28] https://www.theguardian.com/news/2021/jul/18/response-from-nso-and-governments

adatokat, szolgáltatási jogosultságokat, aktuális tartózkodási helyet, az eszköz állapotát (ki- vagy bekapcsolt) vagy egyéb előfizetői adatokat. A nyilvános HLR keresési szolgáltatások segítségével egyébként bárki végezhet lekérdezéseket, de az ilyen szolgáltatásokból visszakapott adatokra már szigorú szabályok vonatkoznak[29], a legtöbb ilyen nyilvános szolgáltatásból legfeljebb annyi adat érkezik vissza, hogy a telefonszám létező vagy nem létező, mely operátorhoz tartozik az eszköz, illetve be- vagy kikapcsolt állapotban van. A nyilvánosan elérhető HLR keresési szolgáltatásokat jellemzően csalás megelőzési, illetve kereskedelmi célokra használják, például egy SMS kampány esetében a HLR keresésekkel biztosítható, hogy csak létező és működő telefonra küldjék az üzeneteket.

A forrásul szolgáló és az NSO-hoz nem kapcsolódó HLR keresési szolgáltatás használata vagy jelenléte a folyamatokban nem merül fel az Amnesty International eredeti vizsgálati jelentésében, a felbukkanása közvetlenül az NSO válaszához köthető, azonban nem is zárja ki, hogy a lista (akár mint egy HLR keresési szolgáltatótól származó adathalmaz) és az NSO szolgáltatása között kapcsolat van, mert a HLR keresés felhasználása elképzelhető a Pegasus terjesztésének folyamatában, vagy akár további kapcsolódó műveletekben is.

Például a közreműködő operátor (a támadási folyamatot indító és menedzselő személy vagy szervezet) egy HLR kereséssel megállapíthatja, hogy a célba vett eszköz létezik-e, regisztrált, be van-e kapcsolva, azaz megkezdhető-e az eszköz elleni támadás. Egy másik aspektus, hogy az SMS-ek kézbesítési folyamatában is megtalálható a HLR keresés, és a Pegasus korábbi időszakokban, SMS üzenetekben helyet kapó linkeken keresztül jutott el a célpontokhoz. Az is elképzelhető, hogy a Pegasus háttér infrastruktúrája (például kezelőfelület) használ HLR kereséseket, vagy akár az NSO használhat egy külső, megfelelő jogosultságokkal rendelkező HLR keresési szolgáltatót az ilyen lekérések lekezelésére és adatszolgáltatásra.

A Pegasus Project az NSO válaszára reagálva megemlíti, hogy egy neve elhallgatását kérő, az NSO rendszerét közvetlenül ismerő forrás szerint a HLR kereséseket integrálták a rendszerbe azután, hogy az NSO és a Circles egyesült. Az integráció egy másik forrás szerint[30] nem volt igazán sikeres, az NSO 2020-ban be is zárta a Circles ciprusi irodáját és elbocsátotta az ottani alkalmazottakat[31].
Az Amnesty International egy közleményben[32] válaszolt az NSO Group cáfolatára, illetve a médiában megjelent információkra. A szervezet kiáll az adatok és a vizsgálati eredmények validitása mellett, illetve rögzíti, hogy a listán potenciális célpontok szerepelnek[33].

A lista körüli „félreértések" egyik forrása lehetett, hogy az egyik izraeli médiaszervezet[34] feltehetőleg hibás megfogalmazást alkalmazott a riportban, amely alapján más médiaszervezetek is hajlamosak voltak kész tényként kezelni, hogy a lista olyan számokat tartalmaz, amelynek tagjait a Pegasus már megfertőzte, azaz a listán szereplő összes telefonszámot az NSO ügyfelei lehallgatták vagy megfigyelték. Az Amnesty International állítása szerint a listán olyan telefonszámok szerepelnek, amelyek az NSO ügyfeleinek

---

[29] Korábban ez nem mindig volt így, meglehetősen alulszabályozott volt a terület, mára azonban szigorú szabályok vonatkoznak az ilyen szolgáltatásokra és erősen szűrt, hogy milyen adatokat kaphat vissza a lekérdező.
[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 is irrefutably linked to potential targets of NSO Group's Pegasus spyware"
[34] Már nem fellelhető anyag (Forrás: https://www.calcalist.co.il/home/0,7340,L-8,00.html)

érdeklődési körébe tartozhatnak[35], de nem feltétlenül kémkedtek utánuk (bár a technikai vizsgálatok alapján néhány, a listán szereplő után feltehetőleg kémkedtek, az ő eszközeiken ugyanis azonosították a Pegasus kártevő nyomait).

A Guardian összefoglalója[36] szerint a listán szereplő telefonszámok azt jelzik, hogy az NSO ügyfelei milyen potenciális célpontokat azonosítottak és jelöltek meg egy lehetséges lehallgatás alanyaként. A cikk szerint ez a szándékot jelzi, azonban a lista adatai nem árulják el, hogy az eszközöket megkísérelték-e megfertőzni és lehallgatni, illetve, hogy megfertőzték és lehallgatták az eszközöket.
A Guardian összefoglalója felveti, hogy az Amnesty Tech Security Lab vizsgálata a (listához képest csekély számú) fizikailag is megvizsgált eszközökön nem csak hogy kimutatta a Pegasus kémprogram nyomait, de a nyomok keletkezésének időpontjai és a listán szereplő időpontok között kapcsolat van, egyes esetekben a készüléken a Pegasus tevékenység kezdete és a listán szereplő időpont között csak néhány másodperces eltérés van. Ez úgy értelmezhető, hogy az ilyen esetekben a kiválasztás (amikor a listára felkerült a telefonszám, például akár egy HLR kereséssel) után szinte azonnal meg is célozták az eszközt és sikeresen kompromittálták a készüléket.

Tehát annyi megállapítható, hogy a listán való szereplés csak akkor jelent konkrét megfigyelési aktivitást, ha mellé párosítani lehet a készülék vizsgálatának és digitális nyomelemzésének pozitív eredményét (ez azonban csak 37 telefonszám esetében került megállapításra a vizsgálati jelentésben). Ilyen esetben láthatóvá válhat, hogy a listára való felkerülés és a konkrét fertőzés időpontja között kapcsolat van.

Több elemzésben is megjelent, hogy elképzelhetetlennek tűnik, hogy több nemzet titkosszolgálata vagy egyéb kormányszerve egy közös (akár közösen használt felhős) rendszerbe vinne fel esetleges célpontokkal kapcsolatos adatokat, mert az ilyen adatokat a minősítés és bizalmasság miatt minden hasonló szervezet házon belül kezeli.

Ezt a véleményt megerősíti egy olyan kiszivárgott dokumentum, amely a Pegasus működtetéséhez szükséges infrastruktúrát mutatja be. A dokumentum egy termékbemutató anyag[37], amely feltehetőleg 2013 időszakából származik, és amelyet az NSO termékfelelőse készített[38]. A dokumentum alapján az ügyfelek a saját oldalukon működő rendszerben tevékenykednek, azaz a „célzás" az ügyfél oldalon történik[39].

A telefonszámokat tartalmazó lista kiszivárgásával kapcsolatban, több esetben is felmerült, hogy az adatok ciprusi szerverről kerültek ki. Shalev Hulio, az NSO alapító-ügyvezetője egy interjúban[40] megemlítette, hogy adatbrókerek keresték meg a vállalatot az adatcsomaggal

---

[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] A dokumentumot Claudio Guarnieri, az Amnesty Tech Security Lab vezetője is megosztotta (Forrás: https://www.documentcloud.org/documents/4599753-NSO-Pegasus.html#document/p12/a437979)
[38] A dokumentum metaadatai szerint a készítés dátuma 2013, ezt alátámasztják az akkor támogatott célpont operációs rendszerek verziószámai. A dokumentumot Guy Molho készítette, aki 2013 és 2018 között az NSO product management igazgatója volt.
[39] Ez persze nem zárja ki műszakilag annak a lehetőségét, hogy az ügyféloldalon futó rendszerből a felvitt számok később, valamilyen módon egy külső forrásba kerüljenek át.
[40] https://www.calcalistech.com/ctech/articles/0,7340,L-3912882,00.html

kapcsolatban, és az állították, hogy azok az NSO ciprusi szervereiről kerültek ki. Az NSO azt állítja, hogy nincsenek szerverei cipruson[41], illetve több adatot is ellenőriztek a listáról és egyik sem kapcsolódik egyetlen ügyfelükhöz sem. Ezzel kapcsolatban az ügyvezető megemlítette, hogy az NSO 45 ügyféllel rendelkezik világszerte, és minden ügyféllel közösen ellenőrizték a listán szereplő telefonszámokat és a számok nem tartoznak egyetlen ügyfelükhöz sem.

A Pegasus Project újságírói 1000 körüli telefonszámot azonosítottak, ezekhez képesek voltak a tulajdonosok személyét hozzárendelni. Az Amnesty Tech Security Lab 67 olyan eszközt vizsgált meg, amelyek telefonszáma szerepel a listán.

A vizsgálatok 23 esetben megtalálták a sikeres Pegasus fertőzés nyomait az eszközökön, illetve 14 további esetben csak a behatolási kísérlet nyomait azonosították. A fennmaradó 30 eszköz esetében a tesztek nem voltak eredményesek, sok esetben a készülékeket már kicserélték. A telefonok közül 15 Android-alapú eszköz volt, amelyek közül egyik sem mutatott sikeres fertőzésre utaló nyomokat[42], azonban 3 Androidos telefonon célzott támadásra utaló jeleket találtak, például a Pegasus-hoz kapcsolódó SMS-üzeneteket.

A listán 300 magyar telefonszám szerepel. Az Amnesty International által kiadott digitális nyomelemzési riport mellékletében[43] csak két magyar érintett tűnik fel, a Pegasus Project hazai partnereként a Direk36 oknyomozó portál azonban több telefonszámot is beazonosított, illetve folyamatosan publikálja a hazai érintettekkel kapcsolatos anyagokat.

A Direkt36 több olyan érintettel kapcsolatban is megjelentetett anyagokat, akiknek az eszközét nem lehetett megvizsgálni, azonban a telefonszámuk szerepelt az eredeti listában. A Direk36 terminológiájában a listán szereplőket „célba vették", azonban ez nem jelenti azt, hogy az érintett eszközét meg is fertőzték és/vagy lehallgatták: „A kiszivárgott adatok még nem feltétlenül jelentik azt, hogy a célszemélyek ellen biztosan be is vetették a Pegasust, és a készülékekbe ténylegesen be is hatoltak, de számos esetben – köztük több magyar célpontnál – a telefonok utólagos vizsgálata bizonyította, hogy valóban behatoltak az NSO programjával a készülékekbe[44]."

A Direkt36 olyan személlyel kapcsolatban is megjelentetett anyagot, akinek a telefonszáma nem volt rajta a kiszivárgott listán[45], azonban korábban saját kezdeményezéséből kért vizsgálatot a Citizen Lab és az Amnesty International munkatársaitól, akik megtalálták a Pegasus 2021-ben keletkezett nyomait a vizsgálatra átadott eszközön.

Nemzetközi szinten több olyan validáció is történt, amelyet az adott ország kormánya vagy annak megbízásából egy független szervezet végzett el. Ilyen vizsgálat volt a francia kormány által kezdeményezett és a francia állam kibervédelmi szervezete, az ANSSI[46] által elvégzett

---

[41] Illetve az NSO és a Circles egymástól teljesen függetlenül és szeparáltan működik.
[42] Az iPhone-okkal szemben az Android nem naplózza azokat az információkat, amelyekre az Amnesty nyomelemző munkájához szükség volt.
[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)

hatósági vizsgálat[47], amely a listán szereplő két francia újságíró esetében műszaki vizsgálattal igazolta a Pegasus fertőzést, illetve a vizsgálat során az Amnesty International elemzésével azonos eredményre jutott. Belgiumban a katonai hírszerzés vizsgálta meg[48] a listán szereplő belga újságíró és felesége két eszközét és mindkét eszköz esetében feltételezik, hogy az eszközöket a Pegasus fertőzte meg.

A Pegasus és az infrastruktúra működése, észlelése

A Pegasus és az NSO által épített infrastruktúra működése evolúción ment keresztül a korábbi időszakokban. Alapvetően öt olyan információhalmaz létezik, amelyekből együttesen körvonalazódhat a rendszer működése, és az esetleges, verziók közötti eltérés:

- *A megfertőzött mobileszközökön futó „spyware" alkalmazás, amelyet több szakértő cég is elemzett már,*
- *Az NSO-tól korábban kiszivárgott, feltehetőleg 2013 környékére datálható termékbemutató dokumentum („Product Description"), amely az akkori Pegasus infrastruktúra működését mutatja be[49],*
- *A Pegasus Project vonatkozó anyagai,*
- *A Citizen Lab 2018-as felderítési riportja[50],*
- *A WhatsApp perbeadványa, amely tartalmaz egy kiszivárgott, 2015-ben aláírt szerződést az NSO és a ghánai ügyfél között[51].*

Természetesen sok egyéb forrás is publikált a Pegasus működésével kapcsolatban információkat, de azok jellemzően azokat a sérülékenységeket elemezték, amelyeken keresztül a kártékony alkalmazás megfertőzhette az eszközöket. Ha a Pegasus, mint komplex rendszer kerül vizsgálatra, akkor nem csak a készülékek sérülékenységeit kihasználó, majd az eszközöket megfertőző, kémtevékenységet végző alkalmazást érdemes szemügyre venni.

Pegasus Agent (a „spyware" alkalmazás)

A sikeres fertőzést követően egy „spyware" vagy kémprogram alkalmazás települ a készülékre. A telepítéshez nincs szükség a felhasználó engedélyére, a felhasználó számára észlelhetetlenül történik. A megfertőzött eszközökön működő alkalmazás teljes jogosultságot biztosít a támadónak az eszköz és az eszközön tárolt adatok felett.

A Pegasus agent beépül az eszköz operációs rendszerének magja (kernel) és az eszközön futó, legitim alkalmazások közé. Ez biztosítja, hogy az agent hozzáférjen a rendszerfunkciókhoz és a legitim alkalmazásokhoz, illetve a bennük tárolt adatokhoz. Az agent az alkalmazások (például telefonhívás, SMS, chat, stb.) működésébe „belelát", azaz hiába

---

[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] A hasonló területen működő Hacking Team meghackeléséből származó információk között megtalálhatók olyan levelek, amelyekben az ügyfelek osztottak meg a Hacking Team munkatársaival az NSO termékekkel kapcsolatban információkat. A mexikói kormányzat továbbította ezt a dokumentumot a Hacking Team részére.

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

[51] Az NSO és a feltételezetten a ghánai kormány egyik fedőcégeként működő Infraloks Development Limited 2015. december 17-én írta alá a 8 millió dolláros szerződést 25 telefon egyidejű megfigyeléséről.

használ egy chat alkalmazás végponttól végpontig terjedő titkosítást, a támadó képes hozzáférni a még titkosítatlan adatokhoz. Az alkalmazások és a kernel közé való beépülés lehetővé teszi, hogy az agent fogadja az alkalmazások kernel felé induló rendszerhívásait, illetve az alkalmazások által a rendszerfunkciókon keresztül a kernel felé küldött adatokat. A kernel közeli működés teremti meg a passzív és aktív lehallgatási lehetőségeket és az adatgyűjtést.

Az alkalmazás telepítéséhez a Pegasus az eszközök, illetve az eszközön futó alkalmazások sérülékenységeit használja ki. A Pegasus evolúciója során a kutatók több olyan sérülékenységet is azonosítottak, amelyeken keresztül a kártékony kód a felhasználó tudta és közreműködése nélkül települni tudott.

Evolúció

A Pegasus korábbi verziói esetében a felhasználónak kattintania kellett a támadó által küldött linkre ahhoz, hogy a tudta és közreműködése nélkül letöltődjön és települjön a kártékony alkalmazás. A 2019-et megelőző időszakban ezért a legtöbb esetben a támadó megtévesztő tartalmakat küldött az áldozatnak, például e-mailben vagy SMS-en vagy egyéb chat-jellegű alkalmazáson (például WhatsApp) keresztül. A Citizen Lab által vizsgált legkorábbi 2016-os eset során Ahmed Mansoor[52] jogvédő kapott egy SMS-t, amelyben börtönben megkínzott fogvatartottakkal kapcsolatban ígért új információkat. Az SMS egy linket tartalmazott, amelyet Mansoor elküldött a Citizen Lab elemzőinek, akik a vizsgálatuk során azonosították az NSO támadó infrastruktúráját[53].

A linken elérhető weboldal támadó kódot tartalmazott, amely addig ismeretlen sérülékenységeket kihasználva fertőzte volna meg a készüléket. A Citizen Lab és a mobil eszközök biztonságával foglalkozó cég, a Lookout megvizsgálta a kódot és ekkor azonosítottak három olyan addig ismeretlen, „zeroday" sérülékenységet, amelyek később a Trident[54] nevet kapták.

Az NSO tehát már 2016-ban olyan sérülékenységeket használt ki, amelyek addig ismeretlenek voltak és lehetővé tették, hogy a felhasználó egyetlen kattintásával („one-click") települjön a rosszindulatú alkalmazás és teljes mélységben kompromittálja a készüléket.

2019-től azonban már a felhasználónak kattintania sem kellett ahhoz, hogy a Pegasus agent letöltődjön és települjön az eszközén. A fejlődés következő lépcsőfoka már a „zeroday – zeroclick" behatolás volt, amikor már a felhasználónak kattintania sem kellett ahhoz, hogy a Pegasus agent települjön az eszközére.

2019-ben WhatsApp szerint az NSO által értékesített technológiával több, mint 1400 felhasználó mobiltelefonját célozták meg húsz országban egy 14 napos támadási kampány során. A támadáshoz egy olyan, addig ismeretlen WhatsApp sérülékenységet[55] használtak ki,

---

[52] Nem ez volt az első alkalom, amikor Mansoor készülékét kémprogramokkal igyekeztek távolról kompromittálni. 2011-ben a FinFisher/FinSpy, 2012-ben pedig a Hacking Team megoldásával igyekeztek a készülékébe behatolni. 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] A Trident sérülékenységi-lánc: https://support.apple.com/hu-hu/HT207107
[55] https://nvd.nist.gov/vuln/detail/CVE-2019-3568

amely lehetővé tette, hogy egy WhatsApp hívással a felhasználó tudta és interakciója nélkül települjön a kártékony kód a megcélzott eszközre. A kártékony kód még akkor is települni tudott, ha a felhasználó nem fogadta a hívást. A WhatsApp a Citizen Lab kutatóival működött közre az esemény kivizsgálásában. A Citizen Lab a vizsgálatok alatt több mint száz olyan esetet azonosított, amely során civil jogvédőket, emberi jogi aktivistákat és újságírókat vettek célba a Pegasussal. A WhatsApp kiértesítette a feltételezett érintetteket, majd 2021-ben a kaliforniai bíróságon beperelte[56] az NSO-t. Bár a WhatsApp sérülékenységének kihasználása nem igényelt a felhasználó részéről interakciót, azonban a hívás vagy a nem fogadott hívás akár gyanút is kelthet a felhasználóban. A fejlődés következő fázisában a Pegasus már ilyen nyomokat sem hagy, a támadás teljesen észrevétlenül történik.

2020-ban a Citizen Lab azonosított egy 36 eszközt érintő támadást, amely az Al Jazira TV csatorna munkatársai ellen irányult, és amely a minden Apple telefonon jelenlévő iMessage addig ismeretlen sérülékenységét használta ki. A későbbi vizsgálatok alapján a KISMET névre keresztelt sérülékenységet már 2019 októbere és decembere között is kihasználták például az Al Araby TV munkatársai ellen[57]. A KISMET sérülékenység pontos működése nem ismert. A Citizen Lab lejelentette az esetet az Apple felé, akik jelezték, hogy kivizsgálják a jelenséget, azonban erről konkrét publikáció nem született. A Citizen Lab és más kutatók, például a Google Project Zero munkatársa, Samuel Groß feltételezése szerint az Apple az iOS14-ben javított az iMessage sérülékenységeken, például ekkor jelent meg a BlastDoor védelmi funkció az Apple operációs rendszerében, amely homokozóként felelős[58] az üzenetküldőben érkező csatolmányok és nem megbízható adatok kibontásáért és vizsgálatáért[59].

Az iOS 14 operációs rendszerben bevezetett BlastDoor ugyan ellehetetlenítette a KISMET sérülékenység kihasználását, azonban 2021 februárjától az NSO egy új, szintén az iMessage alkalmazást célzó támadókódot kezdett el használni. A támadási módszert a Citizen Lab egy szaudi aktivista fertőzött eszközén azonosította márciusban, majd szeptember elején értesítette az Apple-t a sérülékenységről. A FORCEDENTRY[60] névre keresztelt sérülékenységgel kapcsolatban bőséggel áll rendelkezésre információ, mivel az Apple alig egy hét alatt validálta a sérülékenységet[61], majd ki is adta a javítást[62]. Az Apple a WhatsApp-hoz hasonlóan a kaliforniai bíróságon beperelte[63] az NSO-t, és közleményében bejelentette, hogy 10 millió dollárral és a perből befolyt kártérítés összegével fogja támogatni a hasonló biztonsági kutatásokat végző szervezeteknek.

A FORCEDENTRY sérülékenységet számos biztonsági kutató és biztonsági cég is

---

[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" funkcionalitás. Minden alkalmazás egy zárt térben fut, onnan kilépni nem tud, a folyamataihoz más alkalmazás nem férhet hozzá.
[59] https://appleinsider.com/articles/21/01/29/apples-ios-14-integrates-new-messages-security-sandbox-called-blastdoor
[60] Bár szélesebb körben a sérülékenység a FORCEDENTRY néven említett, az Amnesty International vizsgálati riportjában az 5. fejezetben szerepeltetett MEGALODON sérülékenység ugyanaz, csak nem ez a megnevezés terjedt el.
[61] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30860
[62] Például az iOS/iPadOS 12.5.5 és az iOS/iPadOS 15 verziók biztonsági frissítései közel 25 sérülékenységet javítottak (Forrás: 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), bár külön a FORCEDENTRY sérülékenységet már az iOS 14.8-al javította.
[63] https://index.hu/techtud/2021/11/24/apple-nso-per-pegasus-botrany/

kielemezte, illetve a Google Projekt Zero is publikált egy nagyon részletes elemzést[64]. A sérülékenységen keresztül a Pegasus képes megkerülni a BlastDoor biztonsági szolgáltatást, mivel az iMessage alkalmazásban a GIF képek feldolgozása nem a BlastDoor szolgáltatásban valósul meg. A támadás során egy hamisított GIF képi állományban PDF-be ágyazott kód jut be az iMessage alkalmazásba, amelyet a képi feldolgozó helyett a CoreGraphics modul kezd el feldolgozni, amely olyan sérülékenységgel rendelkezik, amelyen keresztül a támadó a legmagasabb jogosultsággal képes kódot futtatni.

Nem csak az iMessage, hanem például az Apple Music[65] vagy az Apple Photo[66] alkalmazás sérülékenysége is lehetővé teheti a behatolást. Az Amnesty International vizsgálati riportjában bemutatásra kerülnek olyan evidenciák, amelyek alapján ezeknek az alkalmazásoknak a sérülékenységei is lehetővé tettek a „zeroday-zeroclick" alapú támadásokat.
Ahhoz, hogy a Pegasus agent ilyen magas jogosultsággal működjön, illetve, hogy be tudjon épülni az operációs rendszer magja és az alkalmazások közé, meg kellett kerülnie az Android és az iPhone védelmi rendszereit és biztonsági funkcióit. Ilyen lépéseket maguk a felhasználók is megvalósíthatnak (rootolás, illetve jailbreaking[67]), azonban ezt a Pegasus távolról és észrevétlenül is képes megtenni.

Bár a Pegasus agent többféle módon is települhet az áldozat eszközére, a „zeroday-zeroclick" módszer, azaz az ismeretlen sérülékenységek interakciót nélkülöző kihasználása, a távolról és észrevétlenül végrehajtott teljes kompromittálás (rootolás vagy jailbreaking) mutatja be legjobban az NSO technológia, illetve a rendelkezésre álló mögöttes humán erőforrás igazi képességét és értékét[68], ezzel együtt pedig a kockázatot, amelyet az eszközökre és felhasználókra jelenthet.

Érintett eszközök

A Pegasus agent az iPhone iOS operációs rendszer esetében iOS 14.8-ig bezárólag képes (jelenlegi ismeretek szerint) kompromittálni az operációs rendszert és eszközt, az adott rendszer, vagy a futtatott alkalmazások sérülékenységein keresztül. Tehát első sorban nem az eszköz típusa, hanem az operációs rendszer és az alkalmazások verziója, az azokban található és kihasználható sérülékenységek határozzák meg, mely eszközök támadhatók a távoli, „zeroday-zeroclick" módszerekkel.

Az NSO 2013 környékére datálható termékbemutató dokumentuma részletesen foglalkozik az agent képességével, megadva a támogatott eszközök és operációs rendszerek listáját. A 2013-as NSO dokumentumban az iOS 4 és iOS 6.1.4 operációs rendszerig szerepelnek az iPhone 4, 4S és iPhone 5 eszközök. Az Amnesty International és a Citizen Lab riportjából látható, hogy a modernebb készülékek fejlettebb operációs rendszereit is képes a Pegasus megfertőzni, például az iPhone 11, iPhone 12, iPhone 12 Pro Max, iPhone 6S és iPhone SE

---

[64] https://googleprojectzero.blogspot.com/2021/12/a-deep-dive-into-nso-zero-click.html
[65] „5. Apple Music leveraged to deliver Pegasus in 2020"
[66] „3. Pegasus processes following potential Apple Photos exploitation"
[67] Mint az Android és az iOS világban ismert eljárások vannak a rootolás vagy a jailbreaking végrehajtására. Ez még a készülék tulajdonosaként sem egyszerű megoldás, amelyet azért szoktak alkalmazni, hogy a készülékek nem elérhető funkcióihoz is hozzáférjen a felhasználó, vagy az adott gyártó ökoszisztémáján kívülről is tudjon alkalmazásokat telepíteni, illetve hogy olyan funkciókat vagy alkalmazásokat tudjon használni, amelyet az eszköz biztonsági funkciói nem engednének.
[68] Az értékkel kapcsolatban érdemes abba belegondolni, hogy a Zerodium, a sérülékenység bróker piac egyik vezető szereplője akár 1.5-2 millió dollárt fizet a „kutatóknak" egy remote jailbreaket lehetővé tévő sérülékenységért.

2 eszközöket, az operációs rendszerükben vagy alkalmazásaikban található sérülékenységeken keresztül. A FORCEDENTRY sérülékenység az iOS 14.8 verzió alatt minden iOS verziót érintett[69], azaz gyakorlatilag minden modernebb iPhone készülék érintetté vált.

A 2013-as NSO dokumentum támogatottként említi az Android (2.1-4.2), BlackBerry (5.0-7.1), Symbian (S60 OS9, Symbian 3 és egyéb verziók) eszközöket és operációs rendszereket. A kiszivárgott 2015-ös NSO szerződés műszaki mellékletében már támogatott eszközök között szerepelnek a 7.x-9.1 iOS, 4.x-5 Android, valamint az 5.x-7.1 BlackBerry eszközök. Az Amnesty International vizsgálati riportja kitér az általuk megvizsgált 15 darab Android-alapú eszközre, amelyek esetében megállapításra került, hogy az Android operációs rendszer nem tárolja a vizsgálathoz szükséges információkat, ezért az Android eszközök esetében nem tudtak egyértelmű bizonyítékokat találni a sikeres fertőzésekre. Három eszközön azonban találtak olyan SMS üzeneteket, amelyek a Pegasus SMS-alapú terjesztési vektorához köthető, azaz ezeken az eszközökön a behatolási kísérlet azonosítható volt.

Az iOS-t érintő Trident sérülékenységi-lánc időszakában szélesebb körben is megjelentek a Android eszközök érintettségével kapcsolatos hírek (noha az NSO dokumentum alapján tudható, hogy már korábban is volt képessége a Pegasusnak az Android eszközök fertőzésére). Ebben az időszakban a Pegasus Android-alapú verziója még Chrysaor néven volt ismert, amelyet először a Lookout, a mobileszközök biztonságával foglalkozó vállalat elemzett[70]. Képességekben hasonló alkalmazásról volt szó, azonban az Android esetében a telepítéshez nem feltétlen volt szükség ismeretlen sérülékenységekre és „zeroday-zeroclick" módszerre, mivel az Android eszközökön a rootolás egyszerűbben is megvalósítható volt[71]. Az Android esetében az is könnyebbséget jelent, hogy ott van a lehetőség a felhasználó engedélyét kérni a telepítés során, ahogyan egyéb rosszindulatú alkalmazások és APK csomagok is megteszik, így akkor is működni fog, ha a rootolás nem sikerül a készüléken. 2017-ben a Lookout és Google néhány tucat érintettet talált[72], akiknek Android készülékét a Pegasus (vagy Chrysaor) megfertőzte.

Képességek

Bár az iOS és az Android jelentősen eltérő operációs rendszerek, azonban a Pegasus mindkét operációs rendszeren teljes jogosultságot szerez, azaz minden adat és folyamat bizalmassága és sértetlensége nullára degradálódik. Ha a Pegasus agent sikeresen települt a készülékre, az SMS rekordok, kontakt listák, hívási naplók, naptárbejegyzések, e-mailek, üzenetküldő alkalmazások forgalma, böngészési előzmények, favoritok - azaz minden fontosabb tárolt adat kiolvasásra kerül[73] és a Pegasus agent elküldi az adatokat a vezérlő szerver felé[74].

Az agent passzív monitorozó funkciója biztosítja, hogy a kezdeti adatkiolvasás után minden új adatrekord elküldésre kerüljön a vezérlőszerver felé. Ezt a funkciót lehet valós idejű módban

---

[69] *Valamint érintett bizonyos OSX és watchOS verziókat is.*
[70] *https://www.lookout.com/blog/pegasus-android*
[71] 2017-ben ez például a Farmaroot módszer és alkalmazás.
[72] *https://www.techtarget.com/searchsecurity/news/450416359/Pegasus-malware-expands-from-iOS-to-Android*
[73] A 2013-as NSO dokumentum „*Initial Data Extraction*" funkciónak hívja.
[74] Nem közvetlenül, hanem egy anonimizációs hálózat felé küldi, majd az anonimizációs hálózat továbbítja a Pegasus operátor infrastruktúrájába az adatokat. A közbülső hálózat célja az operátori szerverek és hálózat elrejtése.

használni, azaz, ha megjelenik az új adat a készüléken, akkor azonnal tovább küldésre kerül, de lehet speciális ütemezési kondíciókat is meghatározni, hogy csak bizonyos időszakonként vagy egyéb feltételek teljesülésekor történjen meg az adattovábbítás. Ez a funkció teszi például lehetővé az eszköz lokációjának cellainformáció-alapú követését is.
Az agent rendelkezik aktív adatgyűjtő funkcióval, amely a Pegasust működtető operátor manuálisan indított lekérdezéseire szolgáltat adatot az eszközökről. Ebben az esetben tehát az operátor kér be adatokat a megfertőzött eszközről, ilyenek lehetnek például a GPS információkon alapuló lokációs adatok, vagy az eszközön tárolt fájlok, de ez a funkció felelős a mikrofon bekapcsolásáért és hangrögzítésért, hívások lehallgatásáért, a fényképek készítéséért, videó felvételért vagy képernyőkép rögzítésért. A 2013-as NSO dokumentumban a hívások lehallgatása (Call Interception) csak az Android eszközök esetében volt támogatott, azonban a 2015-ös kiszivárgott szerződés műszaki mellékletében már az iOS és a BlackBerry eszközöknél is szerepel ez a funkció.
A fejlesztők apróságokra is nagy figyelmet fordítottak. Például amikor az operátor az aktív adatgyűjtésen keresztül fényképet készít az eszköz elő- vagy hátlapi kamerájával, a kamera nem használja a vakut, így a felhasználó egyáltalán nem észleli, hogy a készüléke fényképezett.
A 2013-as kiszivárgott NSO dokumentumból lehet megismerni a mikrofon bekapcsolásának és a hangrögzítésnek akkori működését. Az akkori infrastruktúrában (a Pegasus operátor és NSO ügyfél oldalán működő háttérrendszer) egy Asterisk PBX IP telefonközpont is helyet kapott. A mikrofon bekapcsolásakor az operátornál működő IP telefonközpont felhívta az áldozat telefonszámát, de ez a hívás és a hívás automatikus felvétele nem volt észlelhető a felhasználó számára. Ha a készülék aktív volt, mert a felhasználó éppen használta és a képernyő be volt kapcsolva, akkor a funkciót nem lehetett igénybe venni, illetve abban a pillanatban, ahogy a felhasználó elkezdte használni az eszközt, például bekapcsolta a képernyőt, a hívás azonnal bontásra került és törlődött az addig rögzített adat. Az újabb Pegasus változatokban ez a funkció már feltehetőleg nem igényli az IP telefonközpontot, a Lookout 2017-es elemzésében olyan kódrészletek láthatók, amelyek alapján feltételezhető, hogy egy sokkal egyszerűbb és hatékonyabb mikrofon-alapú lehallgatást sikerült megvalósítani.

A Pegasus operátor az agenten keresztül a telefon belső memóriájában, illetve az esetlegesen SD kártyán tárolt minden fájlhoz hozzáférhet. Az operátor lekérheti a könyvtárak és fájlok listáját, majd az alapján lekérheti bármely fájlt az eszközről, amelyeket az agent a vezérlőszerver felé továbbít.

A Pegasus Android verziójának 2017-es elemzésekor a Lookout hívta fel a figyelmet a billentyűzet használatát rögzítő (keylogger) funkcióra. Ez a funkció a 2013-as NSO dokumentumban az Android és az iOS alapú eszközök esetében sem szerepelt, lehetséges, hogy már új funkcióról van szó. A Lookout 2016-ban készített elemzése sem dokumentált keylogger funkciót az iOS-en futó Pegasussal kapcsolatban, és a 2015-ös kiszivárgott szerződésben is csak az Android mellett szerepel ez a funkció.

A Pegasus agent képes kiolvasni a felhasználók jelszavait, de képes a készülék által észlelt WiFi hálózatok listáját, valamint az elmentett WiFi hálózatok kulcsait is elküldeni a vezérlőszervernek.
A különféle csevegő alkalmazások (Skype, WhatsApp, Viber, BlackBerry Messenger) esetében a 2013-as NSO dokumentum csak a beszélgetések szövegére és a fájltranszferekre

tért ki (a 2015-ös ghánai szerződésben is csak több chat alkalmazás szerepel, a hívás rögzítése nem), azonban a Lookout 2017-es elemzése a Skype, WhatsApp és Viber esetében már a hívások rögzítésének lehetőségére is felhívja a figyelmet.

Telepítési vektorok, terjesztés

Az Amnesty International riportja és a Citizen Lab korábbi vizsgálatai alapján a 2016-2018 közötti időszakban a kártékony oldal linkjét tartalmazó SMS-ekkel induló támadásokat 2019-re kezdte felváltani az iMessage és más alkalmazások sérülékenységét kihasználó támadási forma.
A 2017-es Trident sérülékenységen keresztül történő kompromittáció után jelentős erőforrást fektetett be az NSO a „zeroday-zeroclick" módszerek kifejlesztésébe, de alapvetően a vizsgálati riportok csak a távolról történő behatolással foglalkoznak, az Amnesty International vizsgálati módszertana is ezekre fókuszál.

Távoli behatolási lehetőségek:

- *WAP/Push üzeneten keresztül, a tartalmazott linket a telefon automatikusan, felhasználói interakció nélkül betölti. Az NSO 2013-as dokumentumában „Over-the-Air" néven szerepel, azonban a WAP megszűnésével ez a támadási forma is kiment a divatból.*
- *SMS, email vagy egyéb üzenet megtévesztő tartalommal és a kártékony oldalra vezető linkkel, ahol megtörténik az eszközbe való behatolás[75] és a Pegasus agent telepítése. Korábban több Amnesty International, illetve Citizen Lab riport dokumentálta az SMS-alapú terjesztési vektort, például 2016-ban Ahmed Mansoor is SMS-ben kapta[76] a kártékony oldalra hívó linket, de 2017-ben és 2018-ban is sikeresen alkalmazták az SMS-alapú kézbesítést[77]. Több példa is látható az Amnesty International vizsgálatához tartozó „D" mellékletben az SMS-alapú terjesztésre, az egyik érintett (INHRD1 – SAR Geelani) 2018 februárjában közel egymást követő napokon 3 SMS üzenetet kapott, áprilisban 8 üzenetet, májusban pedig 5 üzenetet.*
- *Alkalmazás és szolgáltatás sérülékenységen keresztül, például a WhatsApp, iMessage, Apple Music, stb. „zeroday-zeroclick" módszerekkel. 2019-től egyértelműen ez a támadási forma a legjellemzőbb. Az Amnesty International riportjában a vizsgált iPhone eszközök esetében legtöbb alkalommal az iMessage alkalmazás sérülékenységén keresztül történt a kompromittáció.*

Az NSO-tól kiszivárgott 2013-as termékbemutató dokumentum két további lehetőséget is bemutat a Pegasus agent telepítésére:

- *Taktikai és hálózati eszközök segítségével is kompromittálhatók az eszközök. Az NSO 2013-as dokumentuma is említi „Tactical Network Element" néven a módszert, amely során az NSO által fejlesztett hordozható bázisállomás segítségével megszerezhető a célpont telefonszáma és távolról bejuttatható rá a Pegasus agent. 2019-*

[75] *A kártékony oldal exploit kódot tartalmaz, amely lefutásakor képes rootolni/jailbreakelni az eszközt, majd magas privilégiumú kódfuttatással képes telepíteni a Pegasus agentet az eszközre.*
[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/*

ben a Milipol párizsi belbiztonsági konferencián[78] az NSO bemutatott egy saját fejlesztésű és egy furgon hátuljába telepített hordozható bázisállomást (BTS). Az eszköz magát legitim mobil adótoronynak mutatja és egy adott területen belül kikényszeríti, hogy a mobileszközök rácsatlakozzanak. A támadó a rácsatlakozott eszközök GSM forgalmát manipulálhatja, és ez lehetővé teszi, hogy távolról telepítse a Pegasus agentet az eszközre. Már a 2013-as NSO dokumentum is említi ezt a módszert, azonban a technológia jelentősen fejlődhetett a Circles integrációjával, amely már 2008-tól hasonló, mobileszköz lehallgatási technológiákat fejlesztett.

- *A fizikai telepítés lehetőségét is a 2013-as NSO dokumentum veti fel. Ha a támadónak van hozzáférése a mobilkészülékhez, a dokumentum szerint kevesebb, mint 5 perc alatt telepítheti rá a Pegasus agentet. A manuális telepítés után az agent ugyanúgy működik és ugyanazokat a szolgáltatásokat biztosítja, mint a korábban ismertetett távoli telepítésű módszerek. A manuális eljárással kapcsolatban nem áll rendelkezésre egyéb információ, például hogyan lehet megkerülni a képernyőzárat, de feltehetőleg ez a legkevésbé alkalmazott módszer.*

Rejtőzés, túlélőképesség és önmegsemmisítés

Ha már települt, a Pegasus agent elrejti a működését, mivel az operációs rendszer kernelszintjén működik, a tevékenysége csaknem észlelhetetlen a felhasználó számára, legfeljebb a megnövekedett adatforgalom árulkodhat arról, hogy a háttérben jelentősebb exfiltráció történik.
Bár a Pegasus agent láthatatlan működésre törekszik, van, amikor pont ez vezet a lelepleződéséhez. A WhatsApp felhasználókat érő támadás során a legnagyobb gyanút azt keltette a felhasználókban, hogy tapasztaltak egy bejövő hívást, meg is jelent a nem fogadott hívás jelzése, majd később a nem fogadott hívás jelzése eltűnt, mert a Pegasus agent törölte.

A kiszivárgott 2015-ös szerződés műszaki melléklete részletezi a telepített Pegasus Agent túlélőképességét. Az agent, mint telepített alkalmazás működőképes marad az eszköz újraindítása után, illetve blokkolja az operációs rendszer automatikus frissítését, bár megjegyzésre került, hogy a manuális OS frissítésre lehetősége marad a felhasználónak. Android operációs rendszer esetében az eszköz gyári állapotra történő visszaállítását is képes elviselni az agent és működőképes marad.

A későbbi Pegasus verziók esetében az Amnesty International vizsgálatai megállapították, hogy az iOS esetében a kártevő már nem perzisztens, az eszköz újraindítása után a támadónak ismét meg kell fertőznie az eszközt. A Citizen Lab 2021 decemberében azonosította az NSO-hoz hasonló tevékenységgel foglalkozó észak-macedóniai vállalat, a Cytrox spyware alkalmazását, a Predatort[79]. A Predator is ismeretlen alkalmazás sérülékenységet használ ki, azonban nem képes „zero-click" módszerrel fertőzni, a Pegasus korábbi verzióihoz hasonlóan szüksége van a felhasználói interakcióra, a felhasználó kártékony linkre kattintására. A Predator a Pegasushoz hasonló funkcionalitással rendelkezik, azonban képes túlélni az iPhone újraindítását is.

---

[78] *https://www.milipol.com/Invisiblegoogle/Catalogue-2019/Liste-des-exposants/NSO-GROUP*
[79] *https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/*

A Pegasus agent önmegsemmisítő mechanizmusokat tartalmaz arra az esetre, ha az agent nem tud kommunikálni a vezérlőszerverével. Ilyenkor alapértelmezetten 60 nap után automatikusan eltávolítja magát, de ez az időintervallum szabadon állítható.

Több oka is lehet annak, hogy az agent nem tud kommunikálni a vezérlőszerverével, például offline állapotban van, vagy a vezérlőszerverek nem elérhetők (lekapcsolt infrastruktúra), esetleg a mobilinternet ki van kapcsolva és a WiFi kapcsolaton keresztül szűrés miatt nem elérhető a vezérlőszerver, stb.

A 2013-as kiszivárgott NSO termékbemutató dokumentum utal arra, hogy az agent akkor is elindíthatja az önmegsemmisítést, ha úgy észleli, hogy lelepleződik a működése, de nem részletezi, hogy milyen feltételek indítják be a mechanizmust.

A kompromittálási folyamat és a mögöttes infrastruktúra

A kiszivárgott 2013-as NSO dokumentum egyik ábrája mutatja be, hogyan történik a kompromittálási folyamat egy SMS-alapú terjesztés során. Az operátor, azaz az NSO ügyfelének munkatársa kezdeményezi a folyamatot a célpont telefonszámának beírásával. Az operátor elküldi a telefonszámot, azaz az installációs kérést. A rendszer innentől az operátor közreműködés nélkül, automatikusan működik. Az ügyfél saját infrastruktúrájában működő GSM modemek vagy SMS átjárók elküldik az üzenetet a célpont telefonszámára, az üzenet tartalmazza a kártékony oldal linkjét, amelyet meglátogatva a kliens eszközre települ a Pegasus agent.

Ez az a pont, ahol ismét felmerül, hogy életszerűtlenek lehetnek azok a feltételezések, hogy a Pegasus Project által megszerzett 50 000 telefonszám közvetlenül valamilyen központi Pegasus infrastruktúrából származik. A 2013-as kiszivárgott NSO dokumentum tartalmaz egy magas szintű architektúra tervet és követelményrendszert az ügyfél által saját magánál működtetett infrastruktúrával kapcsolatban. Az ábrán a „Customer site" oldalon szerepelnek azok az infrastruktúra elemek, amelyeket az ügyfélnek (vagy operátornak) működtetnie kell. Jól látható, hogy a célzás és a telepítési kérelem inicializálása is az ügyfél oldalán indul, a saját rendszerében.

A dokumentum és más elemzések sem tartalmaznak konkrét információkat arról, hogy például az SMS alapú terjesztés esetében ki, mikor és hol fogalmazza meg az üzenet szövegét vagy állítja össze az agentet telepítő kártékony oldalt. Feltételezhető, hogy ez a tevékenység is az ügyféloldalon történik, mivel a megtévesztésen alapuló „Social Engineering" támadások esetében kiemelt fontosságú a megtévesztő (lokalizált és célpontra szabott) tartalom, mert ez a tartalom csalja az áldozatot a kártékony oldalra. Ha a tartalom nem elég vonzó, a felhasználó nem fog a linkre kattintani, és a támadás meghiúsul.

A sérülékeny alkalmazásokon (például iMessage) keresztül történő terjesztés esetében nincs szükség megtévesztő tartalomra, azonban a telepítést elvégző infrastruktúrára (Pegasus Installation Server) ott is szükség van. Ilyen esetben is feltételezhető, hogy nem az NSO által központilag szolgáltatott szerverekről lehet szó, hanem az ügyfél által működtetett infrastruktúráról, az iMessage ökoszisztémán keresztül bejuttatott kódnak a felhasználó

interakciója nélkül és a felhasználó által észlelhetetlenül le kell tudnia tölteni és telepítenie kell a Pegasus agentet, ehhez viszont kapcsolódnia kell a telepítőt tartalmazó szerverhez. Nem tűnik életszerűnek, hogy egy titkosszolgálat vagy ilyen tevékenységet végző kormányszerv[80] akár a legkevesebb információt is megosszon harmadik féllel.

Az NSO több alkalommal is határozottan állította, hogy ők csak értékesítik a technológiát, a használat és a működtetés már az ügyfél tevékenysége, azonban a WhatsApp szerint az NSO működtette azt az infrastruktúrát, amelyen keresztül korábban az 1400 felhasználót érintő, „zeroday-zeroclick" támadás történt. A fellelhető bírósági anyag azt a megfogalmazást tükrözi, hogy WhatsApp szerint a támadási tevékenységet az NSO hajtotta végre[81], így az ellentétes és meglehetősen ködös információk alapján egyértelműen nem lehet meghatározni, hogy egy támadási folyamatban milyen szerepe van az NSO-nak és az ügyfelének. Ez a kérdés azért is kiemelt fontosságú, mert ha a támadási folyamatokban az NSO által központilag működtetett eszközök is részt vesznek, az NSO információkhoz juthat az operátor által végzett tevékenységről, például a megfigyelt személyekről és akár begyűjtött adatokhoz is hozzáférhet.

Ami jelenleg biztosnak tűnik, hogy a kiszivárgott 2013-as NSO dokumentum, illetőleg a 2015-ben aláírt ghánai szerződés az ügyfélnél működő infrastruktúrát dokumentál, ez azonban a technológia fejlődésével és a telepítési vektorok változásával akár jelentősen módosulhatott az azóta eltelt időben.

Az ügyfél oldalon működő infrastruktúrával kapcsolatban a kiszivárgott szerződés és az NSO korábbi termékbemutatója részletes követelményeket határoz meg.
A 2013-as NSO dokumentumban 5 szerver és 10TB adattárolási kapacitás az elvárt, illetve a szükséges GSM modemek, szünetmentes tápegység, PBX eszközök és más hálózati berendezések is szükségesek a rendszer működéséhez. A hardver környezetet bemutató rajzon egy 42U-s rackszekrény ábrája szerepel, amelyből összesen 23U helyet foglal el a szükséges hardverkörnyezet.

A 2015-ös szerződés ennél sokkal részletesebben határozza meg az elvárt eszközöket és ajánlatot is tartalmaz az eszközök beüzemelésére. A szerződés műszaki mellékletében 5db Dell szerver szerepel különféle konfigurációkkal (összesen csaknem 10TB tárkapacitással), 3db CISCO tűzfal, 4db CISCO switch, 9db Cinterion GSM modem, 15db Dell munkaállomás (feltehetőleg operátori munkaállomások), 30db Dell monitor, 2db APC szünetmentes tápegység, stb. A szerződés a szoftverkörnyezetre is kitér, 6 scoket licensztű Veeam virtuális mentőrendszert, 2db Windows 2012R2 licenszt, 2db MS SQL 2014 licenszt és a rendszerfelügyeletet ellátó Nagios Enterprise licenszt tartalmazza. A szerződésben említésre kerül, hogy ezeket, vagy ezekkel egyenértékű eszközöket szállítani is tudja a szerződő partner.

A két dokumentum alapján, az ügyféloldalon üzemelnek azok a szerverek, amelyek az agentek telepítéséért felelnek, az agentek irányítása, konfigurálása és frissítése is ezekről a szerverekről valósul meg. Ugyancsak az ügyféloldalon működnek azok a szerverek, amelyek a megfertőzött eszközökről fogadják a kinyert adatokat, a GSM kommunikációs modulok vagy SMS átjárók, a begyűjtött adatok tárolása is itt valósul meg, illetve itt üzemelnek a rendszer

---

[80] *Az NSO Group állításai szerint ellenőrzött körülmények között és csak kormányzatnak értékesíti a megoldást.*
[81] *https://cases.justia.com/federal/appellate-courts/ca9/20-16408/20-16408-2021-11-08.pdf?ts=1636394536*

működtetését lehetővé tévő operátori munkaállomások.

Bár a 2013-as NSO termékbemutató dokumentumban nem szerepel, a 2015-ös ghánai szerződés további infrastruktúra-elemmel bővíti a Pegasus háttérrendszerével kapcsolatos ismereteket és vélhetőleg indokolja a korábbi elemzői véleményeket, amelyek szerint jelenleg a Pegasus a legfejlettebb spyware és kiberkémkedési alkalmazás.

Az NSO ghánai szerződésének technikai mellékletében említésre kerül, hogy a telepítés során egy vagy több helyi mobil telekommunikációs szolgáltatóhoz elhelyezhető egy vagy több SS7 átjáró eszköz. Ez azt jelenti, hogy a Pegasus háttérrendszere és az operátor rákapcsolódhat a mobilszolgáltató vagy szolgáltatók interconnect hálózatára, amely például a szolgáltatók közötti roamingot is biztosítja, illetve többek között lehetővé teszi, hogy a szolgáltatók egymás HLR-étől kérdezzenek le információkat.

Ezen a kapcsolaton keresztül a Pegasus operátora annak a szolgáltatónak a nevében jár el, ahova elhelyezte az SS7 átjárót, tehát az általa indított HLR keresés, vagy bármely más telekommunikációs kérés vagy továbbítás (például akár SMS küldés, hívásátirányítás kérés, stb) az érintett mobilszolgáltató nevében fog megtörténni. Az SS7 átjárón keresztül a Pegasus operátora minden olyan szolgáltató HLR-jében kereshet, akikkel az érintett mobilszolgáltató roaming szerződést írt alá, vagy engedélyezik egymás rendszereiben a HLR kereséseket.

A kapcsolat felhasználható arra is, hogy mint roaming partner kikérjen a másik szolgáltatótól egy érvényes, eszköz (munkamenet/session) hitelesítő kulcsot, arra hivatkozva, hogy az adott készülék az ő régiójában tartózkodik és a hazai roaming miatt szükség van a hitelesítő kulcsra. A munkamenet vagy session hitelesítő kulcs beállítható az NSO mobil vagy más, támadó célú bázisállomásban, így az áldozat rádiós adatforgalma a bázisállomáson kititkosítható, a GSM adatforgalom (illetve a 2G, 3G[82] adatforgalom) lehallgatható, manipulálható[83].
Speciális körülmények között a fejlett titkosszolgálatok használnak ilyen technológiát, azonban itt egy magáncég műveleti képességeként jelenik meg a funkció, amely a Pegasus rendszerrel integrálva a szignál-alapú lehallgatás és manipulációs képességgel ruházza fel az NSO ügyfelét. Az NSO a szerződésben felhívja az ügyfél figyelmét arra, hogy csak kiemelten fontos esetekben használják ezt a képességet, ne küldjenek túl sok kérést, mert a tevékenység a különféle szolgáltatói küszöbértékeket túllépve riasztásokat generálhat.

Valóban, a mobil szolgáltatók egyre jobban figyelnek az interconnect hálózat forgalmára, elkezdtek például SS7 protokoll tűzfalakat és anomália észlelőket alkalmazni, azonban a fejlett védelmi funkciók lassan és körülményesen jelennek meg a szolgáltatóknál, a rendelkezésre állás és a működésfolytonosság prioritása sokkal magasabb, mint az ilyen jellegű biztonsági megoldások bevezetésének fontossága. A küszöbértékek pedig más nagyságrendűek, mint az SS7 implanton keresztül bonyolított forgalmak mennyisége, így a ritka és kisebb mennyiségű forgalom jó eséllyel átcsúszhat a védelmen.

Az SS7 implant vagy egyéb szignál-alapú támadó, vagy lehallgató eszközök és vagy egyéb szürkezónás csatlakozások meglehetősen nehezen helyezhetők el és alakíthatók ki az Európai Unión belül, illetve a demokratikus országokban működő mobilszolgáltatók

---

[82] A 4G nem SS7, hanem Diameter protokollt használ, léteznek az SS7 átjáró vagy implant eszközökhöz hasonló berendezésekkel, amelyekkel a funkciók megvalósíthatók.
[83] Amennyiben a céleszköz USA vagy izraeli illetőségű, a rendszer nem kérheti, és nem kéri ki a 3G kulcsokat.

rendszerében. Erre csak akkor van lehetőség, ha az adott ország kormányának jelentős beleszólása van a szolgáltató működésébe (például tulajdonolja a mobilszolgáltatót, vagy annak többségi részét), vagy egyéb módszerekkel képes nagy nyomás alá helyezni az adott szolgáltatót[84].

Az NSO szerződés erre vonatkozólag is tartalmaz utalást, amennyiben nincs lehetőség a helyi szolgáltatóknál SS7 átjárókat elhelyezni, igénybe lehet venni (más, külső szolgáltatásként) felhős SS7 átjárókat, de ilyenkor már funkcióvesztés is bekövetkezhet. Az NSO termékbemutató dokumentumából és a kiszivárgott ghánai szerződésből látható, hogy a Pegasus háttérrendszerének hardveres és szoftveres telepítése, illetve a működő, használatra kész környezet kialakítása az NSO feladata, de a 2015-ös ghánai szerződésben a hardver eszközök szállítására is lehetőséget ajánlott fel az NSO.

A 2013-as NSO termékbemutató dokumentumban a rendszer telepítésénél 10-15 hét beüzemelési tevékenység került különböző fázisokban lebontásra, ahol a 15. héten kerül sor a működő rendszer átadására és az ügyfél általi tesztelésére. A szolgáltatás tartalmazza a két hét időtartamú oktatást[85], ahol az operátorok megismerkedhetnek a rendszer architektúrájával, működésével és üzemeltetési feladataival, a rendszer használatával és gyakorlati szimulációkban vehetnek részt. Az oktatás megvalósulhat az ügyfél telephelyén vagy általa kijelölt helyen, de akár az NSO központi irodájában is lebonyolíthatják az oktatást. A 2015-ös ghánai szerződésben is szerepel az oktatás a szolgáltatás részeként, ugyancsak két hét időtartammal, illetve itt meghatározásra került a rendszer átadás-átvételi folyamatának időtartama, amely egy hét helyszíni tevékenységet igényel az NSO részéről.
A dokumentumokból jól látható, hogy az NSO a kereskedelmi forgalomban kapható nagyvállalati megoldásokhoz hasonló integrációs szolgáltatásokat nyújt, ebből a szempontból a Pegasus rendszer szállítása sem más, mint bármely komplex, nagyvállalati IT infrastruktúra szállítása és bevezetése[86]. Az NSO a szolgáltatásban folyamatos termékkövetést és frissítést, Sevice Desk/Help Desk támogatást és supportot biztosít, illetve garanciális feltételeket és SLA-alapú rendelkezésre állást is meghatároz. A termékkövetés és támogatás díja a teljes projektdíj 22%-a, amely évente fizetendő[87], ez is megegyezik a nagyvállalati megoldások esetében jellemző árazással.

A különféle támogatási szintek, illetve a hibaelhárítási tevékenységek részletezése alapján feltételezhető, hogy a tevékenység elvégzéséhez az NSO támogató mérnökök távoli hozzáférést kaphatnak, vagy hozzáféréssel rendelkezhetnek az ügyfélnél működő rendszerekhez. Ezzel kapcsolatban felmerülhet a kérdés, hogy a mély szintű technikai támogatáson és a szükséges (akár ideiglenes vagy időszakos) hozzáféréseken keresztül az NSO hozzáférhet a rendszerben tárolt adatokhoz is. Ez a hagyományos, külsős, vállalati IT

---

[84] Például 2004-ben, a görög „Watergate" néven elhíresült események során az Egyesült Államok a görög kormányra nyomást gyakorolva elérte, hogy a kormány rávegye a görög Vodafone szolgáltatót arra, hogy az olimpia idejére engedélyezzen hozzáférést az Ericson központ legális és jogszerű lehallgatást lehetővé tévő rendszeréhez. A cél az olimpia védelme és a terrorizmus elleni küzdelem volt, azonban az USA az Olimpiai Játékok lezárulta után „ottfelejtette" a hardvereket és a betelepített szoftvereket, sőt titokban kártékony kódot is telepített a rendszerbe, és elkezdte a görög kormány vezetőit, például a miniszterelnököt is lehallgatni. Forrás: https://theintercept.com/2015/09/28/death-athens-rogue-nsa-operation/
[85] A tervezet szerint a 12. héttől a 14. hétig.
[86] Természetesen akadnak azért eltérések is, például a telepítési előfeltételek között szerepel egy, az ügyféllel nem kapcsolatba hozható, 4000 dollár kreditet tartalmazó bankkártya, a hozzá tartozó, és az ügyféllel nem kapcsolatba hozható útlevél szkennelt képe.
[87] Ezzel együtt a szerződés teljes értéke a 9,7 millió dollár.

támogatások esetében is így van, a biztonságtudatosabb vagy IT biztonsági szempontból érettebb szervezetek ezért kontrollálják az ilyen hozzáféréseket, például a támogató tevékenységének megfigyelésével, akár a tevékenység videó rögzítésével[88].

Az NSO által kiadott Transparency Report [89] dokumentum tartalmaz egy olyan kijelentést[90], amely például a Darknet Diaries szakmai podcast[91] szerint felveti annak a lehetőségét, hogy az NSO bizonyos körülmények között beleláthat az ügyfelek adataiba. A podcast házigazdája és a Citizen Lab NSO kutatásainak vezetője, John Scott-Railton között elhangzik, hogy az ügyfelek kötelesek adatokat szolgáltatni az NSO felé a termék használatával kapcsolatban.

Az átláthatósági jelentésben valóban szerepel ilyen kijelentés, de abban a kontextusban, hogy az NSO vizsgálatot indíthat az adott ügyféllel szemben, ha felmerül a termék jogellenes használatának a gyanúja. Ilyenkor az ügyfél köteles információkat szolgáltatni, például a rendszer naplóállományainak adatait, vagy akár a konkrét célpontok célbavételéhez kapcsolódó adatokat. Az adatszolgáltatás megtagadása magával vonja a rendszer használati jogának azonnali felfüggesztését. Shalev Hulio, az NSO ügyvezetője több interjúban[92] is hivatkozott arra, hogy a visszaélések gyanúja esetén ellenőrzéseket végeznek az ügyfeleknél, ezért biztos abban, hogy az 50 000 telefonszámot tartalmazó lista nem származhat az ügyfelektől, illetve, hogy az Amnesty International riportjában szereplő 37 megvizsgált eszköz sem szerepelt a célpontok között.

Anonimizer és proxy hálózat

A Pegasus agent telepítése a Pegasus Installation Server feladata, amely a Citizen Lab 2018-as elemzése[93] szerint az ügyfél vagy operátor saját infrastruktúrájából történik. A megfertőzött eszközökön működő Pegasus agentek azonban nem közvetlenül kommunikálnak a vezérlőszerverekkel és az ügyfél vagy operátor saját infrastruktúrájával. Ennek oka, hogy az NSO és az ügyfél is megpróbálja elrejteni a mögöttes rendszereket, hogy ne lehessen közvetlenül kapcsolatba hozni a megfertőzött eszközt a megfigyelést végző ügyféllel. Ennek érdekében közbülső kommunikációs és adatátviteli réteg került kialakításra, a Pegasus Anonymizing Transmission Network (PATN).

Például az SMS-ben érkező megtévesztő tartalomban szereplő linkre kattintás az eszköz böngészőjét külső VPS szolgáltatóknál (például Amazon, DigitalOcean, stb.) elhelyezett weboldalakra irányítja. A kiszolgálók további proxy szerverek láncolatán keresztül irányítják a böngészőt az operátornál működő Pegasus Installation Server felé. A több közvetítő szerver használata biztosítja, hogy ne lehessen a tevékenységgel kapcsolatba hozni az adott ügyfelet.

A Pegasus agentet telepítő szerver megvizsgálja a kérés és az eszköz különböző jellemzőit, hogy meghatározza, hogy az egyáltalán támogatott-e a fertőzéshez. Ha az eszköz támogatott,

---

[88] Kiemelt privilégiumú felhasználók kezelése (PIM), session recording tevékenység.
[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/
[92] Például: 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/

a telepítő szerver az anonimizáló hálózaton keresztül leküldi az eszközre a megfelelő támadókódot (exploit) és megkísérli a fertőzést. Ha ez valamilyen okból nem sikerül, az eszköz böngészőjét átirányítja az ügyfél által meghatározott csali vagy legitim weboldalra, hogy a felhasználó ne találkozzon hibaüzenetekkel vagy egyéb gyanús jelenségekkel, amelyek alapján esetleg felismerhetné, hogy támadás alatt áll.

Ha a célponton sikeresen települt (vagy elindult) a Pegasus agent, azaz az eszköz megfertőződött, a Pegasus agent elkezd kommunikálni a vezérlőszerverrel és megkezdődik a megfigyelés és lehallgatás, az adatok továbbítása és feldolgozása. A vezérlőszerver a fertőzést végrehajtott infrastruktúrától szeparáltan, feltételezhetően az ügyfél infrastruktúrájában üzemel. A Citizen Lab korai vizsgálatai során az anonimizátor infrastruktúra került felfedésre, majd azon keresztül jutottak el az operátorok vagy ügyfelek rendszeréig. Az Amnesty International összegyűjtötte a Pegasus, illetve a PATN evolúciós szakaszaira jellemző címeket és egyéb indikátorokat[94]. 2021-g összesen 1406 domain cím, 17 email cím és 75 rosszindulatú eszközfolyamat került azonosításra.

A PATN esetében feltételezhető, hogy ezeket a web és domain címeket az NSO működteti, mivel a 2013-as NSO termékismertető dokumentumban rögzítve van, hogy az anonimizációs címek (egy időben?) csak egyetlen ügyfelet szolgálnak ki, és erre a pontra nem lenne szükség a dokumentumban, ha ezeket a címeket az ügyfél üzemeltetné, mert az ügyfél által működtetett web és domain címek értelemszerűen csak a saját célpontjait szolgálják ki. Feltételezhetően kiválasztható, hogy mely anonimizációs címeket használja az adott fertőzési és kommunikációs folyamat, és a lefoglalt címeket más ügyfél már nem választhatja ki. Az NSO általi működtetésre utalhat az Amnesty International korábbi riportja[95] is, amely megemlíti, hogy megvizsgálták a domain címek regisztrációs időpontjait és megállapították, hogy a domainek túlnyomó többségét vasárnap és csütörtök között regisztrálták, ez pedig megegyezik az izraeli munkahéttel (hozzátéve, hogy természetesen egyéb országokban is lehet hasonló munkahét). Tehát vannak arra utaló jelek, hogy a PATN működtetése az NSO feladata, azonban az sem kizárható, hogy az ügyfelek is hozhatnak létre ilyen anonimizációs célra használt címeket, ahogyan erre a Citizen Lab 2018-as riportjában is található egy utalás[96].

A Pegasus felderítési és észlelési lehetősége

Ha már települt (vagy elindult), a Pegasus agent tevékenysége csaknem észlelhetetlen a felhasználók számára, azonban az iOS eszközök olyan rendszernaplózást végeznek, amelyekben digitális nyomelemzéssel fellelhetők a Pegasus tevékenység jelei, illetve az Android eszközök esetében is lehetséges a fertőzésre utaló jelek némelyikének feltárása[97].

A digitális nyomelemzés egy összetett, dokumentált és hiteles vizsgálati módszertanon alapuló

---

[94] https://github.com/AmnestyTech/investigations

[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 cloudbased virtual private servers (we call these front-end servers) rented either by NSO Group or the operator" Forrás: https://tspace.library.utoronto.ca/bitstream/1807/95391/1/Report%23113--hide%20and%20seek.pdf

[97] Az Amnesty International szerint az Android eszközök nem naplózzák és tárolják azokat az információkat, amelyek alapján hitelesen megállapítható a Pegasus jelenléte.

műszaki és adminisztratív folyamat, amely a digitális nyomrögzítésből, a digitális nyomok feltárásából (tevékenység, eseményadatok, naplóadatok, folyamatinformációk, fájljellemzők, adattartalmak, tranzakciós adatok, forgalmi adatok, időpontok, stb.), a gyűjtött információk közötti kapcsolatok kereséséből, elemzésből és kiértékelésből, illetve a digitális nyomelemzési riport elkészítéséből áll.

A digitális nyomelemzés tehát a megtörtént, múltbéli digitális események rekonstruálása és műszaki/tudományos vizsgálata, amely válaszokat ad és bizonyítékkal szolgál arra, hogy egy esemény vagy tevékenység bekövetkezett-e, miért, hogyan és mikor következett be, milyen kiterjedésű, milyen folyamatokat érintett, stb. Fontos kritérium, hogy a vizsgálat reprodukálható, így hiteles bizonyítékokat szolgáltat a vizsgált tevékenységgel vagy egy esemény bekövetkezésével kapcsolatban.

A Citizen Lab megerősítette az Amnesty International kutatásának eredményeit, a kiadott dokumentum alapján[98] az Amnesty International módszertanát megalapozottnak, a vizsgálati eredményeket helyesnek találta, illetve a két szervezet egymástól függetlenül ugyanazon eredményekre jutott a vizsgálataik során.

Bár a Pegasus Project, illetve az Amnesty International nem fedte fel a forrást, amelyen keresztül hozzájutott az 50 000 telefonszámot tartalmazó listához, illetve magát a listát, a francia és a belga kormány független vizsgálatai megerősítik az Amnesty International vizsgálati eredményét a belga[99] és francia[100] érintettekkel kapcsolatban.

Az Amnesty International kiadott egy ingyenesen használható eszközkészletet (Mobile Verification Toolkit - MVT[101]), amellyel ellenőrizhető, hogy a készülék kapcsolatba került-e a Pegasus kémprogrammal.

Az MVT alkalmazáshoz az Amnesty International rendelkezésre bocsátott olyan IoC[102] adatbázist, amelynek elemeit[103] az MVT eszköz végig keresi az eszközön, és az egyezés vagy találat megmutatja, hogy a készülék kapcsolatba került a Pegasussal. Az adatbázis 2018-2021 közötti időszakra vonatkozólag tartalmazza a Pegasus működésével és működtetésével kapcsolatos vizsgálatok során felfedett domain és email címeket, és a megfertőzött eszközökön azonosított folyamat és fájlneveket.

Az MVT használata jelentősebb szakértelmet igényel, azonban az iMazing[104] implementálta az MVT eszköz funkcionalitását a saját alkalmazásába, amellyel gyakorlatilag bárki képes a saját telefonját néhány egyszerű kattintással ellenőrizni. Mindkét alkalmazás az Amnesty International IoC adatbázisát használja fel a keresésekhez.

---

[98] https://citizenlab.ca/2021/07/amnesty-peer-review/
[99] Forensic traces for FRJRN1&FRJRN3 – Lenaig Bredoux, Edwy Plenel – Forrás: https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-appendix-d/
[100] Forensic traces for BEJRN1 – Peter Verlinden, Journalist - Forrás: 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 – a Pegasus jelenlétére utaló nyomok listája
[103] https://github.com/AmnestyTech/investigations/tree/master/2021-07-18_nso
[104] https://imazing.com/guides/detect-pegasus-and-other-spyware-on-iphone

Védelem a Pegasus ellen?

A Pegasus korábbi, 2016-2018 közötti evolúciós szakaszaiban felhasználói interakcióra volt szükség a fertőzéshez. Az SMS, email vagy más üzenetküldő alkalmazásokban megjelenő linkekre rá kellett kattintani ahhoz, hogy a felhasználó kapcsolatba kerüljön a Pegasus agentet telepítő szerverrel. A felhasználói biztonságtudatosság ebben az esetben még védelmet jelentett, ha a felhasználó nem kattintott az ismeretlen forrásból érkezett üzenet linkjére, a támadás meghiúsult. Azonban a jól felépített, megtévesztésen alapuló Social Engineering támadás képes úgy manipulálni az áldozatot, hogy az végül önként megszegje a biztonságtudatos magatartás normáit és rákattintson a kártékony linkre. Azoknál az eszközöknél, ahol az Amnesty International ki tudta mutatni a sikeres, „one-click" alapú támadás nyomait, a Social Engineering manipulációja erősebbnek bizonyult a felhasználók biztonságtudatosságánál.

Az eszközök operációs rendszerének naprakészen tartása nem jelentett védelmet a felhasználók számára, mivel hiába volt a legfrissebb az eszköz operációs rendszere, ha a sérülékenység abban is kihasználható. Az Apple azonban nagyon gyorsan kiadta a szükséges javításokat, azaz miután már kivizsgálták az esetet és elkészítették a javítást, a frissítés telepítése már védelmet nyújt a Pegasus fertőzés ellen.

Ha egy átlátszó táskában sokmillió forint kézpénzt hordozva sétál az állampolgár, előbb-utóbb lesz valaki, aki megpróbálja elvenni tőle a táskát. Minél feltűnőbb a táska és minél több pénz van benne, annál nagyobb a valószínűsége, hogy a támadás be fog következni. A kibertámadások elleni védekezés alapja, hogy a felhasználó vagy az érintett szervezet csökkenti a támadásokkal szembeni kitettségét és megpróbálja a lehetséges károk mértékét az elfogadható szintig csillapítani, azaz a kockázatokkal arányos védelmi intézkedéseket vezet be és alkalmaz.

Az Android mobileszközök esetében ilyen kockázatcsillapító védelmi intézkedés (a naprakészen tartás mellett) a mobileszközök kártékony kódok elleni védelme. Az Android eszközökön futtatott anti-vírus vagy anti-malware alkalmazások képesek lehetnek észlelni a Pegasus agent (mint fájl) szignatúráját, tehát képesek lehetnek megakadályozni, hogy a telepítő elinduljon és lefusson. Magát a konkrét támadást, a sérülékenység kihasználását és a távolról történő kódfuttatást nem feltétlenül észlelik, azonban a Pegasus agent kódjának le kell töltődnie és el kell indulnia, azaz fájlszinten az állományok a szignatúra adatbázissal felismerhetők lehetnek. Több vírusvédelmi gyártó is publikálta, hogy mobilbiztonsági alkalmazásaik védenek a Pegasus fertőzés ellen.

Az Android mobileszközök kártékony kód elleni védelme jelentős különbséget mutat a hagyományos, számítógépeken futó vírusvédelmi eszközöktől. A számítógép vírusvédelmi funkcionalitása sokkal szélesebb körű, azonban a mobileszközök rendelkezésre álló erőforrásai nem teszik lehetővé az erőforrás igényes és szofisztikált vizsgálatokat, így többnyire a szignatúra alapú felismerésre támaszkodnak. A szignatúra alapú felismerés hátránya, hogy a biztonsági alkalmazás csak akkor ismeri fel a kártékony fájlt, ha a gyártó már találkozott a fájlal és elkészítette róla a szignatúrát, azaz csak a már ismert Pegasus variációk ismerhetők fel ilyen módon. Ha a fájl akár csak kicsit is megváltozik, a szignatúrája nem fog

egyezni a gyártó által ismert szignatúrával és a vírusvédelem nem fogja felismerni a fájlt.
Az iOS platform esetében a klasszikus vírusvédelem nem megvalósítható. Ennek oka az Apple zárt ökoszisztémája, az iOS eszközökre csak az Apple Store-ból lehet alkalmazásokat telepíteni, oda pedig csak a gyártó által nagyon szigorúan megvizsgált, ezért az Apple által biztonságosnak tekintett alkalmazások kerülhetnek be[105]. A másik probléma, hogy az iOS esetében az alkalmazások egymástól teljesen elzárt homokozóban működnek, azaz egyik alkalmazás sem képes kilépni a saját környezetéből, ezért nem is tudják egymás működését ellenőrizni, vagy egymás szeparált homokozójában futó folyamatokba beavatkozni. Azonban, ha egy alkalmazás mégis képes kijutni a homokozóból, semmilyen védelem vagy kontroll nincs a tevékenysége felett. Ezt használta ki a Pegasus.

A Pegasus képességei alapján kimondható, hogy a felhasználók nagyon keveset tehetnek a „zeroday-zeroclick" támadások ellen. Érdemes két csoportra bontani a védekezési lehetőségeket.
Az első csoportba azok az általános kiber-higiéniás készségek tartoznak, amelyeket egy átlagos, hétköznapi mobileszköz felhasználónak egyébként is érdemes megtennie a személyes és egyéb fontos adatainak védelmére és az internetes jelenlétből, vagy a mobileszközök felhasználásából adódó kitettség csökkentésére - a Pegasustól függetlenül.

Ilyenek kitettséget csökkentő intézkedések lehetnek például:

- *A nem használt alkalmazások eltávolítása, mert a kevesebb alkalmazás kevesebb sérülékenységet jelent.*
- *Alkalmazásokat csak biztonságos forrásból szabad telepíteni (Android, Google Play).*
- *Az üzenettartalom és a linkek ellenőrzése. Ismeretlen forrásból érkező üzenetek figyelmen kívül hagyása.*
- *A rövidített URL címek ellenőrzése (például bemásolás az ExpandURL szolgáltatásba, amely felfedi a tényleges webhelyre mutató címet).*
- *Az ismerősöktől érkező furcsa, kéretlen jellegű üzenetekre érdemes egy másik kommunikációs csatornán rákérdezni, valóban az ismerős küldte-e.*
- *Az alapértelmezett, az operációs rendszer által preferált böngésző helyett másik böngésző használata. Sok esetben a webes támadókódokat az alapértelmezett böngészőre írják, ilyen esetekben a támadás meghiúsulhat, mert a felhasználó egy attól eltérő böngészőt használ[106].*
- *Az operációs rendszer és alkalmazások naprakészen tartása, a javítások telepítése.*
- *A telepített alkalmazások rendszeres ellenőrzése, az alkalmazásjogosultságok ellenőrzése és visszavonása.*
- *Az eszközhöz való fizikai hozzáférés korlátozása, képernyőzár, jelszóvédelem, PIN kód alkalmazása.*
- *Biztonsági másolatok készítése, a biztonsági másolatok külső ellenőrzése vírusvédelmi megoldásokkal.*
- *Időnként az eszköz gyári állapotra történő visszaállítása, adatok visszatöltése.*

---

[105] Ezért is kell a Pegasus agent telepítéséhez/indításához a távoli jailbreak, amely lehetővé teszi ennek a védelemnek a megkerülését és a kernel közeli működést.
[106] Erre például az NSO termékbemutató dokumentuma is kitér, ilyen esetben nem történik meg a fertőzés és a felhasználó hibaüzeneteket észlelhet.

- *Időnként az eszköz újraindítása, mert ezzel a nem perzisztens kártevők működése megszűnik.*
- *Mobileszközökre fejlesztett biztonsági megoldások használata (webes tartalom szűrés, vírusvédelem (Android), adatmegsemmisítés (wipe), SPAM és SCAM védelem, beállítás ellenőrző, csalásvédelem, adathalászat védelem, stb.).*
- *Adatforgalmi-statisztikák és jelentősebb kiugrások ellenőrzése.*
- *Ismeretlen, vagy ingyenes Wi-Fi hálózatok kerülése.*
- *Titkosított kommunikáció használata (HTTPS).*
- *Jelszó higiénia, biztonságos jelszavak használata, kétfaktoros hitelesítés használata, hozzáférésenként egyedi jelszó használata, jelszómenedzser alkalmazások használata.*

A Pegasust és más, hasonlóan fejlett kémprogramokat nem az „átlagos", hétköznapi felhasználók ellen vetik be. A Pegasus és a hasonló technológiák bekerülési költsége, és az eszközökre lebontott lehallgatások költsége rendkívül magas, ezért a felhasználók széles rétege bár kitett, de nem fenyegetett az ilyen fejlett technológiák által.

A második csoportba olyan felhasználók vagy szervezetek tartozhatnak, akiknek nem csak a kitettsége magas, de fenyegetve is érzik magukat. Az általános kiber-higiéniás készségek mellett számukra javasolt lehet például:

- *A mobileszközök központi menedzseléséért és biztonságos üzemeltetésért felelős Mobile Device Management (MDM) rendszer bevezetése. Konténerizált titkosítás, alkalmazások egyedi jelszóvédelmének beállítása, eszközfelügyelet, forgalomelemzés, stb.*
- *Eszközszétválasztás (kompartmentizáció), dedikált eszközök a különféle, bizalmas adatokat tároló vagy bizalmas kommunikációt folytató alkalmazásokhoz.*
- *Régi típusú „butatelefon" használata (csak hangkommunikációra) – bár a GSM-alapú lehallgatások ellen ez sem fog védeni.*
- *Eszközök napi újraindítása.*
- *A gyári beállítások visszaállítása például hetente, havonta.*
- *Tárolt adatok titkosítása.*
- *Kiemelten bizalmas adatok tárolásának elkerülése.*
- *Adatkommunikáció titkosítása VPN hálózaton keresztül.*
- *Elő- és hátlapi kamerák letakarására képes telefontokok használata, vagy külön kameratakarók használata.*
- *Mikrofonblokkoló használata*[107]
- *Csak töltést engedélyező USB adapter használata az eszközök feltöltéséhez*[108]*.*
- *Az eszközök GSM és egyéb rádiós kommunikációját leárnyékoló és blokkoló tárolók vagy tokok használata („Faraday Bag").*
- *Gyakori telefonszám- és eszközcsere.*
- *Az eszközök időszakos bevizsgáltatása digitális nyomelemző vagy igazságügyi szakértő segítségével.*

A magukat fenyegetve érző felhasználók számára javasolt lehet az MVT vagy egyéb Pegasus nyomokat észlelő eszközök használata, azonban az MVT csak a közelmúltig bezárólag

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

tartalmazza a Pegasus érintettség megállapításához szükséges indikátorokat. Az Amnesty International riportját követően például az Amazon leállította a platformjukhoz köthető NSO szervereket, azonban feltételezhető, hogy máshol és más címeken újra fog indulni a „szolgáltatás", az új címeket pedig az MVT (a jelenlegi indikátor adatbázissal) nem fogja tudni azonosítani az eszközökön. A Pegasusra jellemző volt korábban is, hogy sűrűn változtatta a publikus interneten működő PATN címeket, ezért a jövőben az MVT sem fog tudni megbízható információkkal szolgálni, csak ha az Amnesty International folyamatosan bővíti az indikátorok adatbázisát.

V. Megállapítások

V.1.
A titkos információgyűjtés alkalmazási köre

A Hatóság mindenekelőtt fontosnak tartja felhívni a figyelmet az alábbi, a sajtóban megjelent állítás kapcsán a vizsgálata során feltárt körülményekre és a hatályos magyar jogi helyzetre:

A Direkt36.hu 2021. július 19-én megjelent cikke szerint:

„A Pegasus annyira komoly kiberfegyvernek számít, hogy az NSO csak az izraeli védelmi minisztérium engedélyével adhatja el más országoknak. Hivatalosan csak terrorizmussal és szervezett bűnözéssel gyanúsított személyek ellen lehetne bevetni, de a tényfeltáró projekt kiderítette, hogy az NSO ügyfelei legalább 10 országban használják újságírók, jogvédők, ellenzéki politikusok, ügyvédek és üzletemberek ellen."[109]

A külső engedélyhez kötött titkos információgyűjtésre jogszabály alapján felhatalmazott szervek az Nbtv. által meghatározott feladataik ellátása érdekében használhatják a titkos információgyűjtés speciális eszközeit és módszereit. Az Nbtv. 53. § (2) bekezdése alapján azonban erre kizárólag abban az esetben van lehetőségük, ha az Nbtv.-ben meghatározott feladataik ellátásához szükséges adatok más módon nem szerezhetők meg. A külső engedélyhez kötött titkos információgyűjtésre jogszabály alapján felhatalmazott szervek feladatait az Nbtv. 4. § - 8. § részletezi, az Nbtv. 9. § b) pontja pedig rögzíti, hogy a nemzetbiztonsági szolgálatok ellátják – többek között – a terrorveszély-helyzettel összefüggő törvényben meghatározott feladatokat.

A hatályos magyar jog a külső engedélyhez kötött titkos információgyűjtés alkalmazásának feltételei tekintetében nem differenciál a hivatások, szakmai tevékenységek szerint, vagyis egyetlen hivatás (pl. „újságíró, jogvédő, ellenzéki politikus, ügyvéd és üzletember") vonatkozásában sem korlátozza a nemzetbiztonsági szolgálatoknak az Nbtv. 56. §-a keretében végzett tevékenysége végzésére való jogosultságát.

---

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

A Hatóság vizsgálata során nem merült fel arra vonatkozó információ, hogy az Nbtv. 56. §-a szerinti külső engedélyhez kötött titkos információgyűjtésre felhatalmazott szervek, a gyártó által meghatározott célokon (bűncselekmények és terrorcselekmények megelőzése és felderítése), valamint törvényben meghatározott feladataik ellátásán túl, egyéb célra használtak volna kémszoftvert.

V.2.
A Hatóság vizsgálatával érintett szervek adatkezelési műveletei

A Hatóság vizsgálatának tárgyát képező technikai eszköz egy olyan célszoftver, amely alkalmas a fertőzött eszközön lévő tartalom titokban történő megfigyelésére, valamint a perifériák (kamera, mikrofon) feletti távoli hozzáférés biztosítására. Az eszköz képes a titkos információgyűjtés keretében az információs rendszer, valamint a helyiség titkos megfigyelésére. A Hatóság rendelkezésére álló adatok alapján megállapítható, hogy a vizsgálat tárgyát képező eszköz alkalmazását Magyarországon a Nemzetbiztonsági Szakszolgálat hajtotta végre. A Nemzetbiztonsági Szakszolgálat törvényben meghatározott feladata a titkos információgyűjtés eszközeinek és módszereinek, illetve a leplezett eszközök alkalmazására feljogosított szervezetek munkájának támogatása speciális szolgáltatások biztosítása útján. A Nemzetbiztonsági Szakszolgálatnak a nemzetbiztonsági és rendvédelmi szervek központi szolgáltató szerveként nem csak joga, de kifejezett kötelessége is, hogy a szolgáltató feladatai ellátásához szükséges eszközök rendelkezésre állását biztosítsa.

A Hatóság vizsgálata során tudomására jutott és rendelkezésére álló információk alapján a Nemzetbiztonsági Szakszolgálat a Hatóság vizsgálatának tárgyát képező technikai eszközt az információs rendszer titkos megfigyelése, illetve a hely titkos megfigyelése terén nyújtott szolgáltatásai teljesítése során alkalmazta.

A Hatóság megállapította, hogy a technikai eszköz alkalmazásáról szóló szerződéses feltételek rögzítik, hogy a szerződő fél az alkalmazás során megteszi mindazokat az intézkedéseket, amelyek az eszköz alkalmazásával érintett személyes adatok illetéktelen külső fél általi megismerését megakadályozzák. A Hatóság álláspontja szerint a szerződés adatvédelemre vonatkozó rendelkezései ehhez az elvárható mértékű garanciákat biztosítják.

A Hatóság vizsgálata során nem merült fel arra vonatkozó adat, amely kétségessé tenné azt, hogy a technikai eszköz alkalmazása során a Nemzetbiztonsági Szakszolgálat a vonatkozó jogszabályok, közigazgatási szervezetszabályozó eszközök előírásainak, valamint szerződéses jogviszony esetén a szerződésben vállalt kötelezettségeknek a teljesítésével járt és jár el.

A Hatóság vizsgálata során feltárt körülmények és rendelkezésére álló információk szerint a technikai eszközt a Nemzetbiztonsági Szakszolgálat kizárólag a bűncselekmények és terrorcselekmények megelőzése és felderítése céljára, illetve a vonatkozó magyar jogszabályok által meghatározott feladatai ellátása érdekében használja és biztosítja, hogy azt nem használják alapvető jogok jogellenes korlátozására. A sajtóban megjelent hírekkel ellentétben, a Hatóság vizsgálata során nem merült fel arra vonatkozó információ, hogy a technikai eszköz használatát az izraeli védelmi minisztérium megtiltotta volna Magyarországnak.

A Hatóság az adatkezelőknél (megrendelő szervek) a vizsgált esetekben történt adatkezelések tekintetében nem tárt fel jogellenességet.
A Hatóság által megvizsgált igazságügyért felelős miniszteri engedélyek az Nbtv-ben meghatározott tartalmi elemeket – a titkos információgyűjtés helye, ideje, érintettje, az engedélyezett eszköz megnevezése – minden esetben tartalmazták.
A Hatóság által megvizsgált előterjesztések tartalmazták a titkos információgyűjtés elrendelésének jogalapját, valamint azt, hogy milyen tények és körülmények indokolják az Nbtv. 56. §-a szerinti eszköz alkalmazását. Az engedélyező az indokolási kötelezettségének – a vonatkozó törvényi előírásoknak megfelelően – a Hatóság által vizsgált valamennyi igazságügyi miniszteri határozatban eleget tett.

A Hatóság konkrét, egyedi esetek vizsgálatára vonatkozó megállapításai – valamint az egyes ügyekről készített feljegyzések – a minősített adat védelméről szóló 2009. évi CLV. törvény 7. § (1) bekezdés szerinti minősített adatokat tartalmaznak, így azok részletezésére jelen összefoglalóban nem kerül sor.

Tekintettel arra, hogy az előzőekben jelzettek szerint, a sajtóhírekben hivatkozott 300 telefonszámot tartalmazó listát az Amnesty International Nemzetközi Titkársága nem bocsátotta a Hatóság rendelkezésére a vizsgálat során így annak létezéséről, az abban foglalt érintettek köréről vizsgálata során a Hatóságnak nem állt módjában megbizonyosodnia.
Ebből fakadóan a Hatóság a vizsgálata során azon érintettek vonatkozásában végzett eljárási cselekményeket, akik érintettsége a szoftver alkalmazása során sajtónyilvánosságot kapott. A vizsgálat adatai alapján megállapítható, hogy a sajtóban, a „Pegasus” kémszoftver alkalmazásával érintettként azonosított személyek közül többek vonatkozásában is sor került az Nbtv. 56. §-a szerinti bírói vagy igazságügyért felelős miniszteri engedélyhez kötött titkos információgyűjtés végrehajtására.

V.3.
Az érintettek jogérvényesítési lehetőségei

Az érintett – személyes adatainak kezelésével összefüggő jogainak érvényesítése érdekében – bejelentéssel a Hatóság vizsgálatát kezdeményezheti az adatkezelő intézkedése jogszerűségének vizsgálata céljából, ha az adatkezelő az érintetti jogainak érvényesítését korlátozza, vagy e jogainak érvényesítésére irányuló kérelmét elutasítja, valamint a Hatóság adatvédelmi hatósági eljárásának lefolytatását kérelmezheti, ha megítélése szerint személyes adatainak kezelése során az adatkezelő megsérti a személyes adatok kezelésére vonatkozó, jogszabályban vagy az Európai Unió kötelező jogi aktusában meghatározott előírásokat. [Infotv. 22. §, 51/A. § (2) bekezdés, 60. § (1) bekezdés]

Noha a Hatósághoz egyetlen – a sajtóhírekben megjelent személyi körbe tartozó – érintett sem nyújtott be panaszt vagy kérelmet a Hatóság adatvédelmi hatósági eljárásának indítására, a Hatóság feladata a személyes adatok védelméhez való jog érvényesülésének ellenőrzése és elősegítése, ezért a Hatóság a hivatalból indított vizsgálat lefolytatása mellett döntött.

A Hatóság hivatalból indított eljárásának fontos szerepe van az érintettek jogainak gyakorlását elősegítendő, tekintettel arra, hogy a nemzetbiztonsági célú adatkezelés során az érintett csak korlátozottan, az Nbtv-ben meghatározottak szerint tudja gyakorolni az Infotv. alapján őt

megillető érintetti jogait. Az Nbtv. 48. § szerint ugyanis a nemzetbiztonsági szolgálatok által kezelt adatokról az érintett kérelmére történő tájékoztatást, vagy a személyes adatainak törlését a nemzetbiztonsági szolgálat főigazgatója nemzetbiztonsági érdekből vagy mások jogainak védelme érdekében megtagadhatja, valamint a nemzetbiztonsági szolgálatok minősített adataival kapcsolatban az érintettnek a minősített adat védelméről szóló 2009. évi CLV. törvényben biztosított betekintési jogát a főigazgató nemzetbiztonsági érdekből korlátozhatja. A nemzetbiztonsági szolgálatok kötelezettsége azonban, hogy az érintettektől érkező kérelmeket, azok elbírálásának módját és az elutasításuk indokát nyilvántartsák, és azokról évente tájékoztassák a Hatóságot.

A bűnüldözési célú adatkezelések tekintetében a Bűnügyi Irányelv 17. cikke arra kötelezi a tagállamokat, hogy ha a tagállami jog az érintett jogai gyakorlásának késleltetését, korlátozását vagy mellőzését rendeli el[110], olyan rendelkezéseket fogadjanak el, „*amelyek értelmében az érintett jogainak gyakorlására az illetékes felügyeleti hatóság közreműködésével is sor kerülhet*”.

Mivel a nemzetbiztonsági célú adatkezelések vonatkozásában – néhány, az Infotv.-ben kifejezetten meghatározott kivételtől eltekintve – a bűnüldözési célú adatkezelésekre vonatkozó, a Bűnügyi Irányelv alapján az Infotv.-ben rögzített szabályok alkalmazandóak[111], az Nbtv. 48. §. szerinti tájékoztatás megtagadása esetén az érintett a jogait az Infotv. fent ismertetett rendelkezései[112] szerint, a Hatóság közreműködésével tudja gyakorolni.

Tekintettel arra, hogy a Hatóság fenti ügyszámon folytatott vizsgálatának kezdete óta újabbnál újabb nevek jelentek meg a sajtóhírekben, jelenleg is több – hivatalból indított – vizsgálati eljárás van folyamatban, és a Hatóság a jövőben is hivatalból vizsgálatot fog folytatni a hasonló ügyekben, akkor is, ha az érintettek nem élnek a részükre biztosított jogérvényesítési lehetőségekkel.

V.4.
Az érintettek körének nyilvánossága mint adatvédelmi incidens

A Hatóság vizsgálata során nem sikerült tisztázni azt a kérdést, hogy a magyar személyekhez köthető telefonszámok – amelyek esetében az Amnesty International Security Lab elnevezésű egysége megállapította, hogy azok a kémszoftverrel megfertőződtek – miként kerülhettek nyilvánosságra az úgynevezett Pegasus Project nevű tényfeltáró vizsgálat során.

Az Infotv. 4. § (1)-(3) bekezdésében foglalt, a személyes adatok kezelésére vonatkozó alapelvek szerint személyes adat kizárólag egyértelműen meghatározott, jogszerű célból, jog gyakorlása és kötelezettség teljesítése érdekében kezelhető. Az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának, az adatok gyűjtésének és kezelésének tisztességesnek és törvényesnek kell lennie. Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas. A személyes adat csak a cél megvalósulásához szüksége mértékben és ideig kezelhető. A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható. Az érintettel akkor helyreállítható a kapcsolat, ha az adatkezelő

[110] Vö. Bűnügyi Irányelv 13. cikk (3) bekezdése, a 15. cikk (3) bekezdése és a 16. cikk (4) bekezdése.
[111] Infotv. 2. § (3) bekezdés
[112] Infotv. 22. §, 51/A. § (2) bekezdés, 60. § (1) bekezdés

rendelkezik azokkal a technikai feltételekkel, amelyek a helyreállításhoz szükségesek.

Az Infotv. 4. § (4a) bekezdése alapján az adatkezelőnek az adatkezelés során arra alkalmas műszaki vagy szervezési – így különösen az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisülésével vagy károsodásával szembeni védelmet kialakító – intézkedések alkalmazásával biztosítania kell a személyes adatok megfelelő biztonságát. Az adatkezelő a kezelt személyes adatok megfelelő szintű biztonságát és az érintettek alapvető jogainak érvényesülését az adatkezelés által fenyegető kockázatok mértékéhez igazodó műszaki és szervezési intézkedésekkel köteles biztosítani. Az adatkezelő a műszaki és szervezési intézkedések kialakítása és végrehajtása során figyelembe veszi az adatkezelés összes körülményét, így különösen a tudomány és technológia mindenkori állását, az intézkedések megvalósításának költségeit, az adatkezelés jellegét, hatókörét és célját, továbbá az érintettek jogainak érvényesülésére az adatkezelés által jelentett változó valószínűségű és súlyosságú kockázatokat.

A vizsgálat tárgyát képező technikai eszköz alkalmazása megköveteli az integritás és bizalmasság elvének szem előtt tartását, amely magában foglalja a jogosulatlan vagy jogszerűtlen kezeléssel, valamint a véletlen adatvesztéssel, megsemmisítéssel vagy károsodással szembeni védelmet a megfelelő technikai és szervezési intézkedések alkalmazásával.

Noha a nemzetbiztonsági célú adatkezelések tekintetében az uniós jog nem alkalmazandó, az adatkezelés alapelvei vonatkozásában figyelmet érdemel az Európai Adatvédelmi Testület 4/2019. számú iránymutatása[113], amely a beépített és alapértelmezett adatvédelem elvei között rögzíti, hogy a személyes adatok biztonságának biztosításához megfelelő intézkedések szükségesek, amelyekkel megelőzhetők és kezelhetők az adatvédelmi incidensek, garantálható az adatkezelési feladatok megfelelő végrehajtása és az egyéb elveknek való megfelelés, és amelyek elősegítik az egyén jogainak hatékony gyakorlását. Az iránymutatás követelményként rögzíti a személyes adatok védelmére szolgáló információbiztonsági intézkedések, valamint az adatvédelmi incidensek kezelésére szolgáló eljárásrend rendszeres felülvizsgálatát.

Az adatvédelmi incidens az Infotv. 3. § 26. pontja szerint: *„az adatbiztonság olyan sérelme, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisülését, elvesztését, módosulását, jogosulatlan továbbítását vagy nyilvánosságra hozatalát, vagy az azokhoz való jogosulatlan hozzáférést eredményezi”.*

Az információbiztonsági szakértő a fentiekben ismertetett szakvéleményében kifejtette, hogy az adatszivárgás körülményei nem ismertek, annyi azonban feltételezhető, hogy az adatbiztonság valamilyen módon sérült, hiszen a személyes adatokhoz való jogosulatlan hozzáférés vélelmezhető, így nem zárható ki, hogy adatvédelmi incidens történt.

A Hatóság vizsgálata ezért kiterjedt arra is, hogy a Hatóság által vizsgált adatkezelőknél történhetett-e adatvédelmi incidens a technikai eszköz alkalmazásával összefüggésben. A Hatóság vizsgálata ilyen adatvédelmi incidens bekövetkezésére utaló információt nem tárt fel.

---

[113] Az EDPB 4/2019. számú iránymutatása a GDPR 25. cikk szerinti beépített és alapértelmezett adatvédelemről, (Elfogadás időpontja: 2020. október 20.)

Az „*50 000 telefonszámot tartalmazó, kiszivárgott lista”* forrása és tartalma a Hatóság számára ismeretlen, azonban ha a „lista” a Pegasus Project szervezet, illetve az Amnesty International birtokába került, és az meghatározott természetes személyekhez köthető személyes adatokat tartalmaz, az a jogszabályi rendelkezésekből levezethetően feltehetően kizárólag a személyes adatok jogosulatlan továbbításával valósulhatott meg.

A magyar állampolgárok személyazonosító adatait és telefonszámait tartalmazó, állítólagos „300-as lista” – amelyet a sajtóhírek szerint az Amnesty International bocsátott a Direkt36 újságíróinak rendelkezésére[114] – és amely az eredetileg kiszivárgott 50 000 telefonszámot tartalmazó listából valamilyen, a Hatóság számára nem ismert szempontrendszer szerinti leválogatással jött létre – ugyancsak felveti ezen adatkezelési műveletek jogellenességét. A Hatóság rendelkezésére álló információk szerint nem tisztázott ugyanis, hogy az említett szervezetek (adatkezelők) milyen jogszabályi felhatalmazás alapján, milyen célból kezelik a kiszivárgott listán található érintettek személyes, egyes esetekben vélelmezhetően bűnügyi személyes adatnak minősülő adatait, ahogy az sem, hogy magyar állampolgárok személyes adatai milyen módon és jogi keretek között jutottak egy harmadik országbeli adatkezelő, a londoni székhelyű Amnesty International Nemzetközi Titkárságának birtokába.

Amennyiben harmadik fél jogosulatlanul jutott hozzá a kezelt személyes adatokhoz, úgy a Büntető Törvénykönyvről szóló 2012. évi C. törvény (a továbbiakban: Btk.) szerint büntetendő, több bűncselekmény (pl. Btk. 219. §: Személyes adattal visszaélés, Btk. 265. §: Minősített adattal visszaélés, Btk. 261. §: Kémkedés, Btk. 423. §: Információs rendszer vagy adat megsértése, Btk. 424. §: Információs rendszer védelmét biztosító technikai intézkedés kijátszása) tényállásának megvalósulására is sor kerülhetett.

A fentiekre tekintettel nem zárható ki, hogy bűncselekmény történt, ezért a Hatóság az Infotv. 70. § (1) bekezdése alapján büntetőeljárás megindítását kezdeményezi a nyomozó hatóságnál.

Noha a Hatóság a vizsgálat során nem tudta kétséget kizáróan bizonyítani, illetve kizárni, hogy adatvédelmi incidens történt-e az általa vizsgált adatkezelőknél, amennyiben a nyomozó hatóság eljárásának eredményeképpen bebizonyosodik, hogy történt adatszivárgás és annak oka adatvédelmi incidens volt, a Hatóság azt ki fogja vizsgálni.

Budapest, 2022. január 31.

Dr. Péterfalvi Attila
elnök
c. egyetemi tanár

[114] "Egy kémfilmbe illő sztori" – a két megfigyelt direkt36-os újságíró beszámolója | Direkt36

Jogszabályok:

- Magyarország Alaptörvénye
- 32/2013. (XI.22.) Alkotmánybírósági határozat
- 2/2007. (I. 24.) Alkotmánybírósági határozat
- 23/2018. (XII.28.) Alkotmánybírósági határozat
- Egyezmény az emberi jogok és alapvető szabadságok védelméről (Egyezmény)
- Szabó és Vissy kontra Magyarország ítélet, Emberi Jogok Európai Bírósága, Stasbourg, 2016. január 12.
- A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény (Nbtv.)
- Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.)
- 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról (Avtv.)
- A minősített adat védelméről szóló 2009. évi CLV. törvény (Mavtv.)
- Az Európai Parlament és a Tanács 2016. április 27-i (EU) 2016/680 Irányelve a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről (Bűnügyi Irányelv)
- A Rendőrségről szóló 1994. évi XXXIV. törvény (Rtv.)
- A büntetőeljárásról szóló 2017. évi XC. törvény (Be.)
- Az ügyészségről szóló 2011. évi CLXIII. törvény
- A Nemzeti Adó- és Vámhivatalról szóló 2010. évi CXXII. törvény
- Az alapvető jogok biztosáról szóló 2011. évi CXI. törvény (Ajbtv.)
- A haditechnikai tevékenység engedélyezésének és a vállalkozások tanúsításának részletes szabályairól szóló 156/2017. (VI. 16.) Korm. rendelet
- A központi államigazgatási szervekről, valamint a Kormány tagjai és az államtitkárok jogállásáról szóló 2010. évi XLIII. törvény
- Az Igazságügyi Minisztérium Szervezeti és Működési Szabályzatáról szóló 9/2019. (VIII.1) IM utasítás
- Az EDPB 4/2019. számú iránymutatása a GDPR 25. cikk szerinti beépített és alapértelmezett adatvédelemről, Elfogadás időpontja: 2020. október 20.
- 2012. évi C. törvény a Büntető Törvénykönyvről (Btk.)