Pázmány Péter Katolikus Egyetem
Jog- és Államtudományi Kar

Péterfalvi Attila:

A magánszféra védelme a nemzetbiztonsági célú titkos információgyűjtés során

habilitációs tézisek

Budapest, 2022

A magánszféra védelme a nemzetbiztonsági célú titkos információgyűjtés során[1]

1. Témaválasztás indoka

Az utóbbi időben az érdeklődés fókuszába kerültek a „Pegasus" kémszoftver kapcsán a titkos információgyűjtéssel kapcsolatos kérdések: az ügy újra nyitotta azt a vitát, hogy a magánszféra megvédhető-e a titkos információgyűjtés során, mivel ezekben az esetekben maga az érintett sem tud a megfigyelésről, tehát érintetti jogainak gyakorlásában korlátozva van.
A témát aktualitása és a Nemzeti Adatvédelmi és Információszabadság Hatóság által lefolytatott vizsgálat eredményeinek fontossága okán választottam.

2. A magyar szabályozás átalakulása a rendszerváltozás óta

2.1. Az 1990. évi X. törvény a különleges titkosszolgálati eszközök és módszerek engedélyezésének átmeneti szabályozásáról

Az Országgyűlés 1990. január 25-i ülésén elfogadta a különleges titkosszolgálati eszközök és módszerek engedélyezésének átmeneti szabályozásáról szóló 1990. évi X. törvényt.

A szabályozás különleges eszköznek minősítette minden olyan eszköz és módszer alkalmazását, amelyet az érintett személy tudta nélkül alkalmaznak, és amelynek

[1] A „Pegasus" kémszoftver Magyarországon történő alkalmazásával összefüggésben a Nemzeti Adatvédelmi és Információszabadság Hatóság által hivatalból indított vizsgálatának megállapításai alapján

használata a magánlakás sérthetetlenségéhez, valamint a magántitok, a levéltitok és a személyes adatok védelméhez fűződő jogokat sértheti. Már ez a törvény úgy rendelkezett, hogy különleges eszköz alkalmazására csak abban az esetben kerülhet sor, ha az adatok más módon nem szerezhetők be.

A szabályozás a különleges eszközök alkalmazásának esetei között különbséget tesz aszerint, hogy az bűncselekmények esetén alkalmazható vagy nemzetbiztonsági célból - bár nem használja ezt a kifejezést - de tartalmi szempontból a nemzetbiztonsági érdeknek megfelelő esetköröket sorol fel. Az információgyűjtés engedélyezése az igazságügy miniszter hatáskörébe tartozott. Garanciális szabályként tartalmazta a törvény, hogy amennyiben "a különleges eszközök alkalmazása nem alapozza meg az ellenőrzött személlyel szemben büntető eljárás elrendelését, az ellenőrzött személyt az alkalmazott intézkedésről az engedélyt kérő tájékoztatja, és ezt követően az ellenőrzés során szerzett adatokat meg kell semmisíteni".[2]

2.2. Az 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról

Az 1990. évi X. törvényt a nemzetbiztonsági szolgálatokról szóló 1995. CXXV. törvény helyezte (továbbiakban: Nbtv.) hatályon kívül.

A hatályos szabályozás különbséget tesz a bíró által, valamint az igazságügyi miniszter által engedélyezett titkos információgyűjtés között. A magánszféra vonatkozásában a miniszteri engedéllyel kapcsolatban merül fel kérdésként, hogy a végrehajtó hatalmon belüli engedélyezés megfelelő-e a magánszféra védelme szempontjából. Amennyiben bíró engedélyezi az információgyűjtést – mivel a bíró elkülönül a végrehajtó hatalomtól -, ez a kérdés ebben az esetben nem merül fel.

A magánszféra védelme vonatkozásában egyaránt fontos figyelembe venni a tagállami alkotmányos, polgári jogi és büntető jogi védelem mellett nemzetközi jogi kötelezettségként az Emberi jogok és alapvető szabadságok védelméről szóló egyezményt[3] is. Az Egyezmény 8. cikke szerint „mindenkinek joga van arra, hogy

[2] A különleges titkosszolgálati eszközök és módszerek engedélyezésének átmeneti szabályozásáról szóló 1990. évi X. törvény 5.§ (2) bekezdés

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

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".

A 32/2013. (XI.22.) Alkotmánybírósági határozat - figyelembe véve az Emberi Jogok Európai Bírósága ítélkezési gyakorlatát – kimondja: „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".

A titkos információgyűjtés alkotmányosságát vizsgáló 2/2007. (I. 24.) sz. határozat indoklásában az Alkotmánybíróság kifejtette, hogy „a titkos információgyűjtés és a titkos adatszerzés büntető jogi eszközként való igénybevételét a demokratikus jogállamban megalapozza az a körülmény, hogy egyes, a társadalom rendjét súlyosan sértő vagy veszélyeztető a bűncselekmények elleni eredményes fellépéshez a hagyományos eszközök nem bizonyulnak elegendőnek. 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 szabályozza. Minthogy a titkos eszközök és módszerek igénybevétele súlyos beavatkozást jelent az egyén életébe, alkalmazásuknak csupán kivételesen, átmeneti, végső megoldásként lehet helye."

Az Emberi Jogok Európai Bírósága szerint „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 nyújtanak az egyén jogainak érvényesülésére”.[4]

2.3 Törvénymódosítási javaslat

Tekintettel arra, hogy a nemzetbiztonsági célú titkos információgyűjtés külső engedélyezési rendszerét az Emberi Jogok Európai Bíróságának (EJEB) 2016. január 12-én meghozott ítélete (továbbiakban: Ítélet) nem tartotta megfelelőnek és megállapította, hogy Magyarország megsértette az Európai Emberi Jogi Egyezmény (továbbiakban: Egyezmény) magán- és családi élet tiszteletben tartásához való jogról szóló cikkét, a Belügyminisztérium elkészített és nyilvános vitára bocsátott egy törvénymódosítási javaslatot, amely az igazságügyi miniszteri engedély fölé intézményesítette volna a Nemzeti Adatvédelmi és Információszabadság Hatóság felülbírálati jogkörét. A tervezet szerint újságírót, képviselőt és egyházi személyt a jövőben csak úgy lehetett volna lehallgatni, ha ezt a Nemzeti Adatvédelmi és Információszabadság Hatóság (továbbiakban: Hatóság) jóváhagyja. A Hatóság ellenőrizhette volna a külső engedélyhez kötött adatgyűjtés jogszerűségét is. Az igazságügyért felelős miniszternek az engedélyező döntését az aláírást követően 48 órán belül kellett volna megküldenie a Hatóságnak, melynek 72 órán belül lett volna lehetősége dönteni a kérdésben. Amennyiben a Hatóság úgy ítélte volna meg, hogy az információgyűjtés törvénytelen, akkor leállíthatta volna azt és az addig összegyűjtött adatok törlésére utasíthatta volna az adott szervet. Aki tudomást szerezett volna arról, illetve azt gyanította volna, hogy valamelyik szerv jogosulatlanul folytatott ellene titkos adatgyűjtést, ebben az esetben is a Hatósághoz lehetett volna fordulni, melynek 3 hónap állt volna rendelkezésre, hogy kivizsgálja a panaszt. Ha törvénytelenül figyeltek volna meg valakit, akkor leállíthatta volna az akciót (ha az még folyamatban volt), de bűncselekmény gyanúja esetén feljelentést is tehetett volna.

[4] Dr. Vissy Beatrix és Dr. Szabó Máté Dániel indított ügyben az Emberi Jogok Európai Bíróságának (EJEB) 2016. január 12-én meghozott ítélete

2.3.1. A Hatóság álláspontja a tervezett szabályozással kapcsolatban

A Hatóság javaslatait a nemzetbiztonsági célú titkos információgyűjtés külső engedélyezési rendszerének továbbfejlesztését illetően megküldtem az Országgyűlés Törvényalkotási bizottsága számára.

Az EJEB fentiekben hivatkozott ítélete, amely kimondta, hogy Magyarország megsértette az Egyezmény magán- és családi élet tiszteletben tartásáról szóló cikkét „tágabb összefüggésben arra hívja fel a figyelmet, hogy az infokommunikációs technika gyors fejlődése a számtalan kedvező hatás mellett veszélyekkel is jár: egyre könnyebbé teszi a titkos megfigyelés tömeges alkalmazását, ami a polgárok magánéletébe való beavatkozáson túl hosszabb távon egyéb kedvezőtlen társadalmi hatásokkal is járhat. A fejlett demokratikus jogállamok közvéleményének figyelmét elsősorban az Edward Snowden által nyilvánosságra hozott dokumentumok irányították e problémákra. A szivárogtatás közvetve a személyes adatok transzatlanti továbbítását és felhasználását szabályozó Safe Harbor egyezmény megsemmisítéséhez vezetett.

A Safe Harbor helyébe lépő Privacy Shield erősítette az európai polgárok személyes adatainak védelmét az Egyesült Államok hírszerző ügynökségei által végzett titkos megfigyelésekkel szemben és felhatalmazta az Európai Unió tagállamai adatvédelmi hatóságait arra, hogy az ezekkel a titkosszolgálati adatgyűjtésekkel kapcsolatos jogorvoslati eljárásokban közreműködjenek az állampolgárok jogainak védelme érdekében.

A [5]Privacy Shield ezen túl azért is lényeges tárgyunk szempontjából, mert az Egyesült Államokkal kapcsolatban támasztott adatvédelmi elvárások olyan közös európai alapértékeket fejeztek ki, amelyek természetszerűleg az európai államok számára is irányadók, amikor a tagállami törvényhozások arról döntenek, hogy milyen feltételekkel

[5] Az Európai Unió Bírósága Schrems II ügyben hozott C311/18. számú ítélete érvénytelennek nyilvánította a 95/46/EK európai parlamenti és tanácsi irányelv alapján az EU–USA adatvédelmi pajzs által biztosított védelem megfelelőségéről szóló, 2016. július 12i (EU) 2016/1250 bizottsági végrehajtási határozatot.

lehetséges a titkos megfigyelés és milyen garanciákra van szükség az állampolgárok jogaik védelme érdekében."

A bírósági eljárás nem terjedt ki a Hatóság véleményének beszerzésére, ami ahhoz vezetett, hogy a magyar szabályozással kapcsolatban, különösen a miniszteri engedély feletti külső kontroll vonatkozásában számos jogilag és ténybelileg téves állítás reflektálatlanul maradt a per folyamán. Így nem kerülhetett sor arra, hogy az EJEB megismerje a Hatóságnak a nemzetbiztonsági szolgálatok titkos információgyűjtő tevékenységének független külső ellenőrzése során megszerzett tapasztalatait.

„Az Alaptörvény VI. cikk. (3) bekezdés szerinti, a személyes adatok védelméhez és a közérdekű adatok megismeréséhez való jog érvényesülését ellenőrző, sarkalatos törvénnyel létrehozott, független hatóság a Nemzeti Adatvédelmi és Információszabadság Hatóság, melynek feladatait és hatáskörét az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.) határozza meg.

Az Infotv.-t - amint azt a preambuluma kinyilvánítja - az Országgyűlés az információs önrendelkezési jog és az információszabadság biztosítása érdekében, az Alaptörvény végrehajtására, az Alaptörvény VI. cikke alapján alkotta meg. Az Infotv. releváns rendelkezései:

> *„1. § E törvény célja az adatok kezelésére vonatkozó alapvető szabályok meghatározása annak érdekében, hogy a természetes személyek magánszféráját az adatkezelők tiszteletben tartsák [...].*
> *2. § (1) E törvény hatálya a Magyarország területén folytatott minden olyan adatkezelésre és adatfeldolgozásra kiterjed, amely természetes személy adataira, valamint közérdekű adatra vagy közérdekből nyilvános adatra vonatkozik.*
> *38. § (2) A Hatóság feladata a személyes adatok védelméhez, valamint a közérdekű és a közérdekből nyilvános adatok megismeréséhez való jog érvényesülésének ellenőrzése és elősegítése.*
> *38. § (5) A Hatóság független, csak a törvénynek van alárendelve, feladatkörében*

nem utasítható, a feladatát más szervektől elkülönülten, befolyásolástól mentesen látja el. A Hatóság számára feladatot csak törvény állapíthat meg.

52. § (1) A Hatóságnál bejelentéssel bárki vizsgálatot kezdeményezhet arra hivatkozással, hogy személyes adatok kezelésével, illetve a közérdekű adatok vagy a közérdekből nyilvános adatok megismeréséhez fűződő jogok gyakorlásával kapcsolatban jogsérelem következett be, vagy annak közvetlen veszélye fennáll.

Az ismertetett szabályok alapján a Hatóság a személyes adatok védelméért felelős, független ellenőrző szerv. Az Infotv. hatálya a nemzetbiztonsági szolgálatok által Magyarország területén végzett valamennyi titkos információgyűjtő tevékenységre kiterjed és a Hatóság jogosult ellenőrizni e tevékenységeket. Az 52. § (1) bekezdése alapján bárki a Hatósághoz fordulhat, ha véleménye szerint valamelyik (bármelyik) magyar nemzetbiztonsági szolgálat jogsértő titkos információgyűjtést folytat vagy folytatott vele szemben, vagy a jogsértő titkos információgyűjtés közvetlen veszélye fennáll.

Az Infotv. megfelelő eszközöket biztosít a Hatóság számára az esetlegesen jogsértő titkos információgyűjtés feltárására és a jogsértéssel szembeni fellépésre. A vizsgálati eljárás (Infotv. 52. - 58. §§) szabályai az ombudsmani eljáráshoz hasonlóan erőteljes betekintési, másolatkérési, adatmegismerési, belépési, felvilágosításkérési és vizsgálat kezdeményezési jogosultságokat biztosít. Az Infotv. 71. § olyan szabályokat tartalmaz, amelyek kifejezetten a nemzetbiztonsági szolgálatokat érintő eljárások esetén is biztosítják a Hatóság számára a szükséges adatok megismerését.

A Hatóság ezen túl a vizsgálati eljárásban megismert adatokat – beleértve a nemzeti minősített adatokat is – felhasználhatja adatvédelmi hatósági eljárásban. Ennek eredményeként például megtilthatja a személyes adatok jogellenes kezelését, elrendelheti a jogellenesen kezelt személyes adatok megsemmisítését, elrendelheti az érintett tájékoztatását, ha azt az adatkezelő jogellenesen tagadta meg, valamint bírságot szabhat ki. Ez sokkal erőteljesebb jogkör, mint ami az Ítéletben szóba jöhető független

külső kontrollként hivatkozott ombudsmani eljárásé.

A Hatóság a jogalkalmazási gyakorlatában abból indul ki, hogy a titkos megfigyelés jellegénél fogva megfosztja az adatalanyt a közvetlen jogorvoslat lehetőségétől, ezért e területen a független külső adatvédelmi ellenőrzés az információs magánszféravédelem kulcseleme. Ennek megfelelően a Hatóság minden, az állampolgároktól érkező, titkos megfigyelésre vonatkozó panaszt, bejelentést kivizsgál, attól függetlenül, hogy a beadványban leírt körülmények utalnak-e titkos információgyűjtésre, illetve az érintett az eljárás eredményéről tájékoztatható-e. Évente hozzávetőleg 10-20 ilyen tárgyú bejelentés érkezik a Hatósághoz."

A nemzetbiztonsági célú titkos információgyűjtés külső engedélyezési rendszerének átalakítása szempontjából az Alaptörvényben és az Infotv.-ben foglaltakon túl figyelembe kell venni az Alkotmánybíróság 2/2007. (I. 24.) AB határozatában, valamint a 32/2013. (XI. 22.) AB határozatában foglaltakat is.

„A 32/2013. (XI. 22.) AB határozat és az Ítélet a titkos információgyűjtés előzetes ellenőrzésére, vagyis a külső engedélyezésre fókuszál. Az előzetes külső engedélyezés az egyik eleme az információs magánszféra védelmi garanciarendszernek, amely fontos, de önmagában nem elégséges. Ugyanis az előzetes külső engedélyezés eljárásrendjére a szűk időkeretek, a meglehetősen kötött bizonyítás (az előterjesztő által válogatott, szerkesztett, megfogalmazott dokumentáció alapján kell dönteni), valamint a nyilvánosság teljes kizárása és a kontradiktorius eljárás hiánya jellemző. Ezért a 2/2007. (I. 24.) AB határozat útmutatásának megfelelően célszerű együttesen, összefüggéseiben szemlélni a titkos információgyűjtés teljes kontrollrendszerét és olyan jogi szabályozási megoldásra törekedni, amely összességében tesz lehetővé megfelelő védelmet az állampolgárok jogsértő (szükségtelen, aránytalan) titkosszolgálati megfigyelésével szemben. Tehát egy több szakaszos (előzetes, közbenső és utólagos) és többszereplős (a nemzetbiztonsági szolgálatok belső kontrolljai, az országgyűlési bizottsági ellenőrzés, a külső engedélyezésre jogosult szerv, az adatvédelmi hatóság) kontrollrendszernek összességében kell megfelelően működnie az említett cél elérése érdekében."

A Hatóság feladata az Alaptörvényben rögzített rendeltetéséből és az Infotv.-ben meghatározott feladatköréből adódóan a titkos információgyűjtés utólagos ellenőrzése, így a panaszok és bejelentések kivizsgálása, valamint a szükséges intézkedések megtétele vagy kezdeményezése - a külső engedélyhez kötött és az azt nem igénylő titkos információgyűjtésekkel összefüggésben. A Hatóság álláspontja szerint ezért az utólagos adatvédelmi ellenőrzés rendszerének egységességét nem lehet megbontani, így a külső engedélyhez kötött titkos információgyűjtésre vonatkozó állampolgári panaszok kivizsgálása nem telepíthető más szervre. Az utólagos kontroll garanciális szerepének erősítését az Infotv. módosítása tette lehetővé, amely alapján a Hatóság a titkos információgyűjtésekkel kapcsolatban hivatalból is indíthat vizsgálatot.

A titkos információgyűjtés előzetes külső engedélyezési rendszerének átalakítása esetén többféle szabályozási modell érvényesülhet. A külső kontroll függetlensége és a közjogi–hatalommegosztási elvek szempontjából kifogástalan megoldást eredményezne, ha a jelenleg az igazságügyért felelős miniszterhez tartozó külső engedélyezési hatáskör a bírósághoz kerülne."

Az Ítélet megenged azonban olyan értelmezést is, amely szerint a miniszter előzetes engedélyezési jogköre megmarad. Ezzel kapcsolatban a Hatóság 2016-ban, az Országgyűlés Törvényalkotási bizottsága számára megküldött javaslatai a következőket hangsúlyozták:

- „Egy korábbi, a titkos információgyűjtés külső engedélyezési eljárások adatainak több évre kiterjedő statisztikai elemzésével végzett adatvédelmi vizsgálat eredményei arra utaltak, hogy az igazságügyi miniszter külső engedélyezési jogköre esetében az egyszemélyi döntési felhatalmazás ellentétbe kerülhet a megalapozott döntéshozatal követelményével. A nemzetbiztonsági szolgálatok főigazgatói évről-évre olyan nagyszámú előterjesztést nyújtanak be, amelyeket egy ember - a miniszter – nem képes kellő mélységgel áttekinteni az engedélyről hozandó döntése előtt. Ezért, ha

a jogkör továbbra is miniszteriális keretek között marad, úgy a Hatóság véleménye szerint megfontolandó lenne létrehozni egy olyan bizottságot, amelynek az lenne a feladata, hogy a miniszteri döntéshozatal előtt törvényességi és szükségességi szempontból szűrje az előterjesztéseket és javaslatot tegyen azok engedélyezhetősége tárgyában. E bizottságban a titkos információgyűjtés törvényességében érdekelt kormányzati szervezetek (például BM, nemzetbiztonsági szolgálatok) által delegált, a szükséges speciális nemzetbiztonsági ismeretekkel rendelkező szakértők vennének részt. E bizottság tehát nem független, külső kontrollt valósítana meg, hanem az lenne a szerepe, hogy elősegítse a külső engedély tárgyában hozandó miniszteri döntések jogszerűségét és megalapozottságát és ezáltal töltene be jogvédelmi szerepet. A bizottság létrehozásának szabályozási keretei a Nbtv. módosításával teremthető meg.

- Az Ítéletben foglaltakra tekintettel a miniszteri külső engedélyezési jogkör fenntartása esetén elengedhetetlenül szükséges azt független külső kontroll alá helyezni. Közjogi szempontból nincs akadálya annak, hogy e szerepkört a Hatóság töltse be, amely az Alaptörvényben meghatározott független adatvédelmi ellenőrző hatóság és amelynek feladatkörébe a titkos információgyűjtés jogszerűségének utólagos ellenőrzése egyébként is beletartozik. Az Infotv. megfelelő szabályozási keretet ad e feladat ellátásához, beleértve a tényállás megállapításához szükséges vizsgálati jogosultságokat, valamint az információs magánszférát sértő miniszteri döntés észlelése esetén a szükséges intézkedések megtételét. Lényegében elég lenne az Infotv.-t annyival kiegészíteni, hogy a Hatóság folyamatosan ellenőrzi a titkos információgyűjtés miniszteri engedélyezésének jogszerűségét.”[6]

[6] NAIH/2016/6396/3/J számú ügy

3. Nemzetbiztonsági szolgálatok titkos információgyűjtő tevékenységének átfogó, adatvédelmi szempontú auditja[7]

A Hatóság a nemzetbiztonsági szolgálatok speciális tevékenységéhez kapcsolódó adatkezelés jogszerűségének elősegítésére irányuló eljárásokat is folytat. 2016-ban az egyik nemzetbiztonsági szolgálat kezdeményezésére és együttműködésével egy adatvédelmi auditot végzett, amelynek keretében gyakorlati tesztekkel ellenőrizte a titkos információgyűjtés egyes eszközei és módszerei alkalmazásának jogszerűségét. A Hatóság e tevékenysége egy újszerű és nemzetközi összehasonlításban is példa nélküli adatvédelmi ellenőrzési módszeren alapult.

„A titkos információgyűjtés adatvédelmi auditálásához kidolgozott módszer lényege az, hogy az NBSZ a Hatóság által megtervezett kísérleti szituációkban, a valóságoshoz lehetőség szerint minél inkább hasonló körülmények között hajtsa végre a titkos információgyűjtéssel kapcsolatos szolgáltató tevékenységét.

A tesztek a titkos információgyűjtés valamennyi, az Nbtv. 56. §-ában felsorolt, külső engedélyhez kötött eszközére és módszerére kiterjedtek, valamint a külső engedélyt nem igénylő eszközök és módszerek közül azokra, amelyek a személyes adatok védelme szempontjából relevánsak. A teszt szituációk úgy lettek kialakítva, hogy az NBSZ a teszt végrehajtása során minden alkalommal valamilyen előre meghatározott, adatvédelmi szempontból lényeges kérdésben döntési helyzetbe kerüljön. Nem elégedtünk meg a titkos információgyűjtés során tipikusan előforduló helyzetek modellezésével, hanem valós körülmények között esetleg csak ritkán előadódó helyzetek tesztelését is felvettük az audit terv teszt katalógusába, ha az adott teszttel valamilyen adatvédelmi szempontból fontos követelmény érvényesítését lehetett ellenőrizni.

[7] Lásd részletesen: Péterfalvi Attila: 25 éves az NBSZ c. jubileumi kiadvány, pp. 79-86., Nemzetbiztonsági Szakszolgálat, Budapest, 2021,

A teszt terveket csak az NBSZ kijelölt kapcsolattartói ismerhették meg, akik titoktartási kötelezettséget vállaltak.
Általában a Hatóság biztosította a teszt szituációkban felhasznált eszközöket, felszereléseket, anyagokat. A Hatóság munkatársai alakították a teszt szituációkban a célszemélyeket, valamint a titkos információgyűjtés során képbe kerülő egyéb személyeket, továbbá a szolgáltatást megrendelő szervezet (rendszerint a fiktív Polgári Felderítő Szolgálat) tisztjeit.

A Hatóság a valóságoshoz hasonló körülmények között vizsgálta az NBSZ titkos információgyűjtéssel kapcsolatos eljárásainak teljes folyamatát. Minden teszt úgy indult, hogy a Hatóság a nem létező Polgári Felderítő Szolgálat nevében átadta az NBSZ-nek az adott teszt fiktív tényállásának megfelelő megrendelés dokumentációját, beleértve a fiktív adatokkal kitöltött szolgálati jegyeket és a külső engedélyhez kötött titkos információgyűjtés esetén a fiktív külső engedélyt is. A tesztek előkészítése és végrehajtása során az NBSZ mindenben úgy járt el, mint az Nbtv. 8. § (1) bekezdés a) pontja szerinti szolgáltató tevékenysége során.

A tesztek végrehajtását az NBSZ kijelölt munkatársa jegyzőkönyvben dokumentálta. (Ez egyébként a Hatóság feladata lenne, de csak így lehetett megoldani, hogy ne jusson a tudomásunkra olyan, a tesztek végrehajtáshoz egyébként sem szükséges információ, amelyet a Hatóság az Infotv. 71. §-ában foglaltak értelmében nem jogosult megismerni.) Ugyanakkor a Hatóság munkatársai az adott teszthez készített feljegyzésben dokumentálták azt, ha a Polgári Felderítő Szolgálat tisztjeként egyeztettek az NBSZ munkatársaival vagy például soron kívüli „műveleti tájékoztatást” kaptak a fiktív titkos információgyűjtésről. Ilyen módon az NBSZ és a megrendelő szervezet közötti kommunikáció és interakció is teljeskörűen ellenőrizhetővé vált.

Az NBSZ a tesztek során ugyanúgy gyűjtötte, rögzítette, és dolgozta fel az információkat, mint amikor „élesben” végzi a szolgáltató tevékenységet. A titkos információgyűjtés tesztek eredményeként Hatóságnak átadott dokumentációk jellegüket (például jegyzőkönyv, képfelvétel, hangfelvétel, szakértői vélemény stb.) az

információk feldolgozottságát, az adattartalmukat és formátumukat tekintve ugyanolyanok voltak, mint a tényleges titkos információgyűjtések esetében. A 2016 áprilisa és 2017 február közötti időszakban 34 titkos információgyűjtés teszt végrehajtására került sor.

Az audit messzemenően visszaigazolta az NBSZ elkötelezettségét az adatkezelés törvényességét illetően, ugyanakkor a tesztek a titkos információgyűjtéssel kapcsolatos tevékenységek néhány olyan részletét is feltárták, amelyekkel kapcsolatban a Hatóság az adatvédelmi követelmények magas szintű érvényesítése érdekében észrevételekkel és javaslatokkal élt”[8].

4. Hatályos magyar szabályozás értékelése a garanciák szempontjából - a „Pegasus” kémszoftver Magyarországon történő használatának vizsgálata

Ezek után vizsgáljuk meg, hogy a hatályos magyar szabályozásban a nemzetbiztonsági célú titkos információgyűjtés engedélyezése, megfelel-e a fenti kritériumoknak, kellő garanciát nyújt-e a megfigyelt személy magánszférájának védelmére!

A nemzetbiztonsági célú titkos információgyűjtésre vonatkozó hatályos szabályozás alapján megállapítható, hogy az igazságügyi miniszter engedélyezési jogkörét érintően nem történt jogszabály módosítás, így jelenleg is ugyanazok a szabályok vannak hatályban, mint amely miatt az Emberi Jogok Európai Bírósága elmarasztalta Magyarországot.

Fontosnak tartom azonban kihangsúlyozni, hogy az Infotv.-nek az Általános Adatvédelmi Rendelettel[9] (továbbiakban: GDPR) történő megfeleltetése során[10] a Hatóság jogkört kapott arra, hogy hivatalból is megindíthatja a vizsgálati vagy adatvédelmi hatósági eljárást. Ezáltal lehetővé vált, hogy a Hatóság a nemzetbiztonsági

[8] A Nemzeti Adatvédelmi és Információszabadság Hatóság Beszámolója a 2016. évi tevékenységéről
[9] 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)
[10] 2018.évi XXXVIII. törvény 20. és 23. §, hatályos 2018. VII. 26-tól

célú titkos információgyűjtés ellenőrzésére hivatalból indítson akár vizsgálati, akár adatvédelmi hatósági eljárást. Ez történt a „Pegasus" kémszoftver alkalmazása kapcsán is.

„A titkos információgyűjtés általános adatvédelmi jogi kereteit a személyes adatok kezelését illetően az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 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[11]) 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 a 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."

Arra nem vállalkoznék, hogy megjósoljam azt, hogy a 2016. óta bekövezett jogszabály módosítást az EJEB a végrehajtó hatalmon belüli (igazságügyi miniszteri) engedély feletti külső kontroll vonatkozásában hogyan értékelné, azt azonban fontosnak tartom bemutatni, hogy a „Pegasus" kémszoftver alkalmazásával összefüggésben történt

[11] 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 irányelv

ellenőrzés milyen mélységű volt, milyen iratokat ellenőrzött a Hatóság.
A Hatóság az Infotv. 54. § (1) bekezdése alapján folytatott 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. 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 – ideértve 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 e rendelkezés alapján kereste meg az Amnesty International Magyarország Egyesületet, valamint az Amnesty International Nemzetközi Titkárságát – sajnálatos módon együttműködésük hiányában – eredménytelenül.)

„A Hatóság feladat- és hatásköre a nemzetbiztonsági szolgálatok adatkezelése, valamint azon belül is a titkos információgyűjtés törvényességi ellenőrzése szempontjából meglehetősen széleskörű 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 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.
A Hatóság az igazságügyért felelős miniszter általi külső engedélyezés jogszerűségének ellenőrzése során minden egyes esetben megvizsgálta az előterjesztést, hogy az megfelelt-e a jogszabályban meghatározott formai és eljárási követelményeknek.

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

A külső engedélyezés jogszerűségének vizsgálata során a Hatóság azt is megvizsgálta, 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 megvizsgálta, 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 kell, hogy meghozza a határozatot hoz arról, hogy az előterjesztésnek helyt ad-e, vagy azt megalapozatlansága esetén elutasítja. A Hatóságnak tehát nem csak az előterjesztések formai és eljárási követelményeit kell ellenőriznie, 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.

A Hatóság a fenti jogszabályi rendelkezések alapján - közel száz előterjesztés, valamint ahhoz tartozó igazságügyi miniszteri határozat megfelelősége vonatkozásában – a külső engedélyezés jogszerűségére vonatkozó vizsgálatát – az alábbi kérdések mentén folytatta:

- 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 helyszíni eljárások során a Hatóság azt is megvizsgálta, hogy az alkalmazott minősítés dokumentálása megfelel-e a minősített adat védelméről szóló 2009. évi CLV. törvény (Mavtv.) rendelkezéseinek.

A Hatóság eljárása azért is kiemelkedő jelentőségű, mert az érintettek - tekintettel arra, hogy érintetti jogaikat a nemzetbiztonsági célú adatkezelés során csak korlátozottan tudják gyakorolni – helyett, nevükben az Infotv. szerinti jogaikat a Hatóság tudja gyakorolni. (A 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 Mavtv.-ben biztosított betekintési jogát a főigazgató nemzetbiztonsági érdekből korlátozhatja. Garanciaként megemlíthető, hogy a nemzetbiztonsági szolgálatok kötelezettsége, 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[12], 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[13], az Nbtv. 48. §. szerinti tájékoztatás megtagadása esetén az érintett a jogait az Infotv. fent ismertetett rendelkezései[14] szerint, a Hatóság közreműködésével tudja gyakorolni. Ezért a Hatóságnak a sajtóhírekben megjelent minden újabb érintett személy esetében a jövőben hivatalból kell vizsgálatot folytatnia akkor is, ha az érintettek nem élnek a részükre biztosított jogérvényesítési lehetőségekkel.

A Hatóság az eljárása során nem tárt fel arra vonatkozó információt, 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. A Hatóság vizsgálata során tudomására jutott és rendelkezésére álló információk alapján a Nemzetbiztonsági Szakszolgálat a

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

Hatóság vizsgálatának tárgyát képező technikai eszközt az információs rendszer titkos megfigyelése, illetve a hely titkos megfigyelése terén nyújtott szolgáltatásai teljesítése során alkalmazta.

A Hatóság azt is 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.

Fontos hangsúlyozni azt a tényt, hogy 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! E körben indokolt utalni a hatályos törvény szerinti nemzetbiztonsági érdek fogalmára[15]:
„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,

[15] Nbtv. 74. § a) pontja

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 Hatóságnak eljárása során azt is tisztáznia kellett, hogy hogyan fordulhatott elő az, hogy nyilvánosságra kerülhettek olyan személyes adtok, melyek arra utalnak, hogy az érintettekkel szemben titkos információgyűjtésre került sor. Sajnálatos módon azonban 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. Ugyanakkor az egyértelműn megállapítható, hogy ilyen adatok nem kerülhettek volna nyilvánosságra, hiszen 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 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.

Az Infotv. 3. § 26. pontja szerint adatvédelmi incidens: *„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”.*
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.

A Hatóság eljárása során igénybe vett információbiztonsági szakértőt, aki

szakvéleményében ugyancsak 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.

Amennyiben nem történt adatvédelmi incidens, hanem 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.

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

Az esetleges büntető eljárás kapcsán kétségeimet fogalmazom meg abban a vonatkozásban, hogy az eljárás egyértelműen meg tudja állapítani, hogy az „adatszivárgás” adatvédelmi incidens vagy jogellenes adatkezelés volt-e!

Melléklet

A „Pegasus” kémszoftver bemutatása a Nemzeti Adatvédelmi és Információszabadság Hatóság által felkért információbiztonsági szakértő elemzése alapján[16]

„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[17]. A lista körül nagy a bizonytalanság. A listával kapcsolatos megfogalmazások, félreértelmezhetők és nem feltétlenül egyeznek meg közvetlen vagy mögöttes jelentésükben.”

„Az NSO Group határozottan visszautasítja[18], hogy a tevékenységükkel vagy ügyfeleik

[16] A Nemzeti Adatvédelmi és Információszabadság Hatóság hivatalból indított vizsgálatának megállapításai a „Pegasus” kémszoftver Magyarországon történő alkalmazásával összefüggésben: file:///C:/Users/NAIH-204/Downloads/Adatved_jelentes_NAIH-423-2-2022%20(1).pdf

[17] Azerbajdzsán, Bahrein, Kazahsztán, Mexikó, Marokkó, Ruanda, Szaúd-Arábia, Magyarország, India és az Egyesült Arab Emírségek

[18] https://www.theguardian.com/news/2021/jul/18/response-from-nso-and-governments

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 adatokat, szolgáltatási jogosultságokat, aktuális tartózkodási helyet, az eszköz állapotát (ki- vagy bekapcsolt) vagy egyéb előfizetői adatokat."

„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."

„ 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, amely feltehetőleg 2013 időszakából származik, és amelyet az NSO termékfelelőse készített. A dokumentum alapján az ügyfelek a saját oldalukon működő rendszerben tevékenykednek, azaz a „célzás” az ügyfél oldalon történik.

A telefonszámokat tartalmazó lista kiszivárgásával kapcsolatban, több esetben is felmerült, hogy az adatok ciprusi szerverről kerültek ki.”

„Az NSO azt állítja, hogy nincsenek szerverei Cipruson, illetve több adatot is ellenőriztek a listáról és egyik sem kapcsolódik egyetlen ügyfelükhöz sem.”

„A Pegasus Project újságírói 1000 körüli telefonszámot azonosítottak, ezekhez képesek voltak a tulajdonosok személyét hozzárendelni.”

„A listán 300 magyar telefonszám szerepel. Az Amnesty International által kiadott digitális nyomelemzési riport mellékletében csak két magyar érintett tűnik fel, a Pegasus Project hazai partnereként a Direkt36 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 Direkt36 terminológiájában a listán szereplőket „célba vették”, azonban ez nem jelenti azt, hogy az érintett eszközét meg is fertőzték és/vagy lehallgatták.”

„A Direkt36 olyan személlyel kapcsolatban is megjelentetett anyagot, akinek a telefonszáma nem volt rajta a kiszivárgott listán, 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.”

„**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 használ egy chat alkalmazás végponttól végpontig terjedő titkosítást, a támadó képes hozzáférni a még titkosítatlan adatokhoz.”
„Az alkalmazás telepítéséhez a Pegasus az eszközök, illetve az eszközön futó alkalmazások sérülékenységeit használja ki.”

„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.”

„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.”

„A kompromittálási folyamat és a mögöttes infrastruktúra”

„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, 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."

„A 2015-ös szerződés ennél sokkal részletesebben határozza meg az elvárt eszközöket és ajánlatot is tartalmaz az eszközök beüzemelésére.

„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 működtetését lehetővé tévő operátori munkaállomások."

„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 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.
Az NSO által kiadott Transparency Report dokumentum tartalmaz egy olyan kijelentést, amely például a Darknet Diaries szakmai podcast 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."

„Anonimizer és proxy hálózat"

„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 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.

A digitális nyomelemzés egy összetett, dokumentált és hiteles vizsgálati módszertanon alapuló 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 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 és francia érintettekkel kapcsolatban.”