Ügyszám: NAIH-1904-6/2014/T
Készítette: dr. Bíró János o.v.

Jelentés
a kémprogramok magyar nemzetbiztonsági célú alkalmazásáról

Egy állampolgár amiatt fordult bejelentéssel a Nemzeti Adatvédelmi és Információszabadság Hatósághoz (a továbbiakban Hatóság), mert a sajtóban megjelent hírek alapján véleménye szerint „*a magyarországi nemzetbiztonsági szolgálatok olyan kémprogramot használtak, illetve vásároltak, mely minden magyar állampolgár internetes levelezését ellenőrzi és számítógépére telepített*".

A sajtóban valóban megjelentek híradások, amelyek szerint egy számítógépes betörés során nyilvánosságra került egy kémprogram fejlesztő cég elektronikus levelezése, amelyben arra vonatkozó utalások szerepeltek, hogy a magyar Nemzetbiztonsági Szakszolgálat számára is értékesítették a cég termékeit. A szóban forgó kémprogramok tulajdonságairól rendelkezésre álló információk azt valószínűsítették, hogy ezek a kémprogramok alkalmasak az állampolgárok tömeges, titkos elektronikus megfigyelésére. A kémprogram alkalmazásával kapcsolatos aggodalmakat felerősítették azok a hírek, amelyek szerint az Egyesült Államok, azaz egy fejlett demokratikus jogállam világméretű, kiterjedt, titkos elektronikus megfigyelési programokat működtet, amelyek keretében az USA kormányának nemzetbiztonsági szolgálatai készletező jelleggel sok millió emberről gyűjtenek információkat.

Ha a magyar nemzetbiztonsági szolgálatok hasonló adatgyűjtést folytatnának, az a magyar adatvédelmi szabályok értelmében sértené az érintettek személyes adatainak védelméhez való jog érvényesülését, ezért a Hatóság vizsgálatot indított annak megállapítására, hogy a magyar nemzetbiztonsági szolgálatok alkalmaznak-e kémprogramot, és ha igen, e tevékenységük összhangban van-e a személyes adatok kezelésére és védelmére vonatkozó jogszabályi előírásokkal.

Kimondottan a kémprogram nemzetbiztonsági célú alkalmazásának szabályozására vonatkozó jogi normaanyag jelenleg nincs hatályban, ezért a kémprogram alkalmazására vonatkozó jogi követelményrendszer tisztázása a személyes adatok védelmére, valamint a nemzetbiztonsági szolgálatok tevékenységére, így különösen a titkos információgyűjtésre vonatkozó törvényi előírások értelmezése útján lehetséges. A vonatkozó jogszabályok nem tartalmaznak a kémprogram meghatározására vonatkozó értelmező rendelkezést, ezért a kémprogram definiálása is jogértelmezést igényel. Ezért a vizsgálat során az első feladat a kémprogram alkalmazás jogi hátterének feltárása, majd ennek alapján a titkos információgyűjtés céljából alkalmazott kémprogram jogi ismérveinek meghatározása, valamint a kémprogram alkalmazás adatvédelmi jogi modelljének megalkotása volt. Ezek ismeretében kerülhetett sor a kémprogram alkalmazás vizsgálatára a Nemzetbiztonsági Szakszolgálatnál.

I. A kémprogram alkalmazás jogi háttere

- Az Alaptörvény I. cikk (1) - (3) bekezdései szerint az ember sérthetetlen és elidegeníthetetlen alapvető jogait tiszteletben kell tartani. Védelmük az állam elsőrendű kötelezettsége. Magyarország elismeri az ember alapvető egyéni és közösségi jogait. 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. Az Alaptörvény VI. cikk (1) - (2) bekezdései szerint mindenkinek joga van ahhoz, hogy magán- és családi életét, otthonát, kapcsolattartását és jó hírnevét tiszteletben tartsák. Mindenkinek joga van személyes adatai védelméhez, valamint a közérdekű adatok megismeréséhez és terjesztéséhez.

- Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.) az információs önrendelkezési jog és az információszabadság biztosítása érdekében meghatározza a személyes adatok védelmét, valamint a közérdekű és a közérdekből nyilvános adatok megismeréséhez és terjesztéséhez való jog érvényesülését szolgáló alapvető szabályokat. Az Infotv. 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 szerint az adatkezelő köteles az adatkezelési műveleteket úgy megtervezni és végrehajtani, hogy az e törvény 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 e törvény, 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.

- A magyar 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 (Nbtv.) határozza meg. Az Nbtv. 53. § (2) bekezdése szerint a nemzetbiztonsági szolgálatok a titkos információgyűjtés speciális eszközeit és módszereit csak akkor használhatják, ha az e törvényben meghatározott feladatok ellátásához szükséges adatok más módon nem szerezhetők meg.

- A titkos információgyűjtés alkotmányosságát illetően fontos iránymutatással szolgál 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 szabályozza. Minthogy a titkos eszközök és módszerek igénybevétele súlyos beavatkozást jelent az egyén életébe, alkalmazásuknak csupán kivételesen, átmeneti, végső megoldásként lehet helye."

A nevezett AB határozat hivatkozik az Emberi Jogok Európai Bírósága ítélkezési gyakorlatára: „*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. A kémprogram meghatározása és a kémprogram alkalmazás adatvédelmi jogi modellje

A „kémprogram" a számítógépes kártevők egyik fajtájaként közismert fogalom. Azonban a jelen vizsgálat tárgyát nem ezek a kémprogramok képezik, hanem a magyar nemzetbiztonsági szolgálatok titkos információgyűjtő tevékenységének egyik jogilag szabályozott eszköze, ezért a kémprogram meghatározásának kiindulópontja az Nbtv. kell, hogy legyen. Minthogy az eszközalkalmazás titkos jellege folytán az érintettek jogérvényesítési lehetősége kizárt, jogvédelmi garanciális szempontból elengedhetetlen a titkos információgyűjtés világos, teljes és kellően részletes jogi szabályozása. Ezért a jogi szabályozás megfelelőségének kritériuma, hogy abból a technikai realitások figyelembe vételével meghatározható legyen a kémprogramnak, mint a titkos információgyűjtés jogilag szabályozott eszközének a funkcionalitása, valamint az eszközalkalmazás adatvédelmi jogi modellje.

A kémprogram alkalmazása feltételezi egy számítástechnikai eszköz vagy rendszer (a továbbiakban: célrendszer) létét, melynek adatait a kémprogram megismerhetővé és rögzíthetővé

teszi az eszközt alkalmazó nemzetbiztonsági szolgálat számára. Ezért a kémprogram alkalmazás statikus modelljének elemei:

- a kémprogram,
- a célrendszer és
- az alkalmazást végző nemzetbiztonsági szolgálat, illetve annak a kémprogrammal kommunikáló informatikai rendszere.

A kémprogram alkalmazása egyszersmind egy folyamat, ezért a kémprogram alkalmazás modelljének másik – dinamikus - nézetében az eszközalkalmazás egymás után következő, egymással oksági, logikai kapcsolatban álló szakaszai találhatók, amelyek az elemek között kapcsolatokat reprezentálják. Az alkalmazás szakaszai:

- az eszközalkalmazás feltételeinek létrehozása,
- az eszközalkalmazás: az adatok megismerése, illetve rögzítése,
- az eszközalkalmazás megszüntetése.

Az alábbi modell nem a nemzetbiztonsági szolgálatok titkos információgyűjtő tevékenységének általános modellje, hanem csak egy területre, a kémprogram alkalmazás sajátosságaira és adatvédelmi kereteire fókuszál.

Statikus modell – a kémprogram és a környezete

A kémprogram

Az Nbtv. teljeskörűen felsorolja a titkos információgyűjtés nemzetbiztonsági szolgálatok által alkalmazható eszközeit és módszereit (Nbtv. 54. § (1) bekezdés a)(-e) pontok, 55. § (1) bekezdés, 56. § a)-e) pontok). A felsorolás elemei gyűjtőfogalmak, amelyekbe esetenként több eszköz és módszer is beletartozhat. Az Nbtv. 56. § e) pontja szerint a nemzetbiztonsági szolgálatok „*külső engedély alapján „számítástechnikai eszköz vagy rendszer útján továbbított, vagy azon tárolt adatokat megismerhetik és azok tartalmát technikai eszközzel rögzíthetik, továbbá felhasználhatják*”. A kémprogram alkalmazása megfelel az Nbtv. idézett pontjának, de nem meríti ki az abban foglaltakat, ezért az Nbtv. 56. § e) pontja alapján más eszköz és módszer alkalmazására is sor kerülhet. Ez a Jelentés a kémprogram alkalmazását tárgyalja, ezért az egyéb eszközök és módszerek taglalása csak olyan mélységben szükséges, amennyire az a kémprogram meghatározása, valamint az egyéb eszközöktől és módszerektől való elhatárolása érdekében indokolt.

A kémprogram ismérvei:

1. A kémprogram számítástechnikai program, azaz számítástechnikai műveleteket leíró utasítások sorozata. Emellett tartalmazhat még az alkalmazáshoz szükséges adatokat, például változókat, paramétereket. A kémprogram nem tartalmaz hardver összetevőt. Ez megkülönbözteti a titkos információgyűjtés olyan eszközeitől, amelyek hardver és szoftver összetevőt egyaránt tartalmaznak, például egy digitális hangrögzítő eszköztől. A kémprogram szoftver jellege nem zárja ki azt, hogy a telepítéséhez adattároló hardvert használjanak, amilyen például a pendrive.

2. A titkos információgyűjtés során a kémprogram telepítésére és alkalmazására titokban, a célrendszer felhasználójának tudta és együttműködése nélkül kerül sor. Ez a kritérium elhatárolja azoktól az eszközöktől és módszerektől, amelyek

esetében a törvény együttműködésre kötelezi az adatkezelőt. (L. az elektronikus hírközlésről szóló 2003. évi C. törvény (Eht.) 92. §)

3. A kémprogram a célrendszeren fut. Ennél pontosabban nem szükséges meghatározni a telepítés célpontját, ami lehet például a célrendszer operációs rendszere, valamely alkalmazása, az alkalmazáshoz tartozó plugin, a rendszer valamelyik eszközének beépített adattárolója (pl. firmware) és a háttértárak teljes területe. Tehát a szóban forgó eszközt nem szükséges és nem is lehetséges egyértelműen megfeleltetni a számítógépes kártevők valamelyik ismert kategóriájának. Így a telepítés helyétől és a működés módjától függően például a „rootkitek", a „trójai programok" és a „hálózati férgek" tulajdonságaival rendelkezhet a célrendszerben. (A számítógépes kártevőkkel való összehasonlítás nem arra utal, hogy az olyan kémprogram, amelyet magyar nemzetbiztonsági szolgálatok alkalmazhatnak, bármilyen értelemben kártevő lenne.)

4. A kémprogram alkalmazása a célrendszer útján továbbított vagy tárolt adatok alkalmazást végző szerv számára megismerhetővé és rögzíthetővé tételére irányul. Ez a kritérium elhatárolja azoktól a szoftveres eszközöktől, amelyeket a nemzetbiztonsági szolgálat feladatainak ellátása során egyéb célból telepíthet a célrendszeren. A kémprogramétól eltérő egyéb funkció lehet például egy elektronikai vagyonvédelmi rendszer működésének rejtett módosítása az észrevétlen élőerős bejutás érdekében. Az ehhez hasonló, a megfigyelésen, adatgyűjtésen kívül eső célokra szolgáló szoftveres eszközök műveleti alkalmazását az Nbtv. jelenleg nem szabályozza. A jogi szabályozás hiánya az „egyéb célú" eszközalkalmazást nem zárja ki, feltéve hogy az alapvető jog érvényesülését még csekély mértékben és közvetve sem érinti. A törvényi szabályozás a jövőben akkor és annyiban válik szükségessé, amennyiben az ilyen egyéb célra szolgáló eszközök alkalmazása alapvető jogot, például az emberi méltóságot, a magánélet tiszteletben tartásához fűződő jogot érintheti.

5. A kémprogram alkalmazása a lakásban történtek megfigyelésére és rögzítésére is irányulhat. Erre az ad technikai lehetőséget, hogy a lehetséges célrendszerek nagy részében megtalálhatók azok az érzékelők – például kamera, mikrofon - amelyek alkalmasak a célrendszer környezetére vonatkozó különféle adatok gyűjtésére. A lakásban történtek kémprogram segítségével történő megfigyelése és rögzítése esetén azért kell a tevékenység jogi megítélését differenciálni, mert az Nbtv. 56. § b) pontja külön nevesíti az eszközök és módszerek között azt, hogy a nemzetbiztonsági szolgálatok külső engedély alapján a lakásban történteket technikai eszközök segítségével megfigyelhetik és rögzíthetik. Ebben az esetben is az Nbtv. 56. § e) pont szerinti eszközalkalmazás történik, ami azonban az Nbtv. 56. § b) pontjában meghatározottakra irányul.

E két alkalmazási funkció összefüggései, a tevékenység jogi megfeleltetése elvileg kérdéseket vet fel. Ugyanis a célrendszerből történő adatgyűjtés során óhatatlanul keletkeznek olyan információk is, amelyek a célrendszer környezetére – adott esetben a lakásban történtekre – vonatkoznak. Ha például egy otthoni személyi számítógépre telepítették a kémprogramot, akkor a működésének tényéből az a következtetés vonható le, hogy a számítógépet bekapcsolták. Ha a kémprogram keyloggere billentyűleütésekről küld információt, akkor feltehetőleg valaki éppen használja a billentyűzetet. Ha a kémprogram rögzít egy Skype-hoz hasonló

alkalmazás által továbbított beszélgetést, akkor a hangfolyamba bekerülhetnek olyan háttérzajok (például ajtócsapódás, a televízió hangja, az egyéb jelenlévő egyéb személyek beszélgetésének foszlányai stb.), amelyek a lakásban történtekre utalnak. Vajon ezek az Nbtv. 56. § b) pontja alá tartoznak? A válasz az, hogy a felsoroltak csak esetleges körülmények. A választóvonal ott húzódik, hogy olyan-e az eszközalkalmazás módja, amely elsődlegesen az Nbtv. 56. § b) pontja szerinti adatgyűjtést tesz lehetővé. Ha például a kémprogram az adatgyűjtés során titokban bekapcsolja a célrendszer mikrofonját és rögzíti a célrendszer környezetében elhangzottakat, vagy pillanatfelvételeket készíttet a célrendszer képfelvevőjével, akkor ez amellett, hogy megfelel az Nbtv. 56. § e) pontjának, egyúttal már az Nbtv. 56. § b) pont szerinti eszköz funkcionalitásának is megfeleltethető. Ha azonban az eszközalkalmazás során csak esetlegesen, mellékesen keletkeznek olyan, a fenti példákban bemutatottakhoz hasonló információk, amelyekből a célrendszer környezetére lehet következtetni, az még nem alapozza meg a tevékenység Nbtv. 56. § b) pontjának megfeleltetését.

6. Az Nbtv. szabályozási rendszere lehetővé teszi a következők elhatárolását az Nbtv. 56. § e) pontjában meghatározott eszközöktől és módszerektől:

- Az Nbtv. 54. § (1) bekezdése szerint a titkos információgyűjtés keretében a nemzetbiztonsági szolgálatok
d) az információgyűjtést elősegítő információs rendszereket hozhatnak létre és alkalmazhatnak;
i) az 56. §-ban foglaltakon kívül beszélgetést lehallgathatnak, az észlelteket technikai eszközökkel rögzíthetik;
j) hírközlési rendszerekből és egyéb adattároló eszközökből információkat gyűjthetnek.

- Az Nbtv. 56. § d) pontja szerint a nemzetbiztonsági szolgálatok külső engedély alapján „*elektronikus hírközlési szolgáltatás útján továbbított kommunikáció tartalmát megismerhetik, az észlelteket technikai eszközzel rögzíthetik*”.

A célrendszer

Célrendszer alatt az a számítástechnikai eszköz vagy rendszer értendő, melynek továbbított vagy tárolt adatai megismerésére, illetve rögzítésére a kémprogramot alkalmazzák. A célrendszer a kémprogram alkalmazási környezetéhez tartozik, ezért a célrendszerek milyensége alapvetően meghatározza a kémprogram alkalmazásának technikai lehetőségeit. Részletes elemzés nélkül elég e helyütt utalni azokra a változásokra, amelyek a kémprogramok alkalmazási lehetőségeit, valamint az eszközalkalmazás adatvédelmi jogi megítélését az Nbtv. 56. § e) pontjának törvénybe iktatása óta is befolyásolhatták:

1. A mindennapi elektronikai cikkek körébe tartozó a számítástechnikai rendszerek diverzitása nő. Elterjedtek a különféle mobil számítógépek, játékkonzolok, táblagépek. Megjelennek az „intelligens” mobiltelefonok, használati eszközök (szemüvegek, órák stb.) és háztartási gépek, melyeket vezetékes vagy vezeték

nélküli helyi hálózat köt össze. Az előbb említettek a kémprogram alkalmazása szempontjából potenciális célrendszerek.

2. Az érzékelők elterjedésének jelentősége: az elektronikai fogyasztási cikkek új generációja (táblagépek, okostelefonok, egyéb „okos”-eszközök, játékkonzolok) stb. különféle érzékelőket tartalmaz, mint például a mikrofon, a kamera, a gyorsulásmérő, a hőérzékelő, a GPS modul. Ezek révén a korábbinál többféle adat gyűjthető a célrendszer felhasználójáról és a környezetéről. Például helymeghatározási adatok elárulják a célszemély hollétét és lehetővé teszik a helyváltoztatásának követését, amiből következtetni lehet életritmusára, szokásaira is. Az okos eszközök nagy felbontású kamerájának képe biometrikus személyazonosításra ad lehetőséget.

3. Az intelligens eszközök mobillá válása, személyes használata és a kommunikációban betöltött szerepük: az újfajta intelligens elektronikai fogyasztási cikkek között sok olyan van, amelyet arra terveztek, hogy a felhasználó magánál tartsa táskában, zsebben, vagy a testén viselve. Egyre inkább teret nyernek az olyanok, amelyek nem adott helyszínhez (gépteremhez, irodához, lakáshoz) rendelhetők, hanem a felhasználójuk személyes használatára szántak, beleértve ebbe a mobil telefonálást, az e-mail küldést és a közösségi portálok használatát is, tehát az elektronikus kommunikáció különféle módozatait is. E számítástechnikai rendszerek erősebb, közvetlenebb kapcsolatban vannak a felhasználóval, mint pl. a személyi számítógép.

4. Az elektronikus hírközlés és az informatika konvergens technológiai fejlődése, csak címszavakban: a hang továbbítására kifejlesztett vezetékes vagy mobil telefon hálózatok egyre inkább adatkommunikációra szolgálnak. Ugyanakkor az internetes informatikai rendszerekben hozzáférhetők olyan szolgáltatások, amelyek jellegükben hasonlók a telefonáláshoz, levelezéshez. Az informatikai fejlődés a kommunikációval kapcsolatos szolgáltatások sokszínű, gyorsan bővülő kínálatát hozta létre, amelyek mind nagyobb szerepet töltenek be a kommunikáció hagyományos módozataival (elsősorban a telefonálással) szemben.

A technikai fejlődés, különösen a személyes használatú számítástechnikai rendszerek új, különféle érzékelőkkel ellátott kategóriáinak létrejötte, továbbá az új elektronikus kommunikációs formák és szolgáltatások elterjedése elvileg megnöveli az e rendszerekből történő titkos információgyűjtés lehetőségeit és ez felértékeli más, hagyományosnak tekinthető eszközökkel és módszerekkel (például a „telefonlehallgatással”) összehasonlítva. Ugyanakkor a jelzett változások azt is jelzik, hogy a technikai fejlődés a korábbiaknál jobban átláthatóvá teszi a titkos információgyűjtéssel érintett személyek magánéletét és kommunikációját az eszközt alkalmazó számára.

<u>A kémprogram alkalmazását végző szerv informatikai rendszere (a továbbiakban: irányító szerver)</u>

Az irányító szerver nem szükségszerű eleme a kémprogram alkalmazás modelljének. Ugyanis elképzelhető olyan eszközalkalmazási mód, amelyben a nemzetbiztonsági szolgálat a kémprogram által összegyűjtött adatokhoz közvetlenül, emberi erővel fér hozzá. Ez az alkalmazási mód azonban kivételesnek tekinthető. Akárcsak a hétköznapi

számítógépes kártevők esetében, az a tipikus, hogy a kémprogram kommunikál az irányító szerverrel. Az irányító szerver utasításokat küld az adatgyűjtés megkezdésére és leállítására, továbbá az adatgyűjtés módjára, a kémprogram pedig továbbítja az összegyűjtött adatokat.

Dinamikus modell – a kémprogram alkalmazás folyamata

Az eszközalkalmazás feltételeinek megteremtése

Az eszközalkalmazás feltételeinek megteremtése szigorúan véve nem része az alkalmazás folyamatának, azonban logikailag elválaszthatatlan attól, ugyanis kémprogram alkalmazására csak akkor kerülhet sor, ha annak a jogi és a technikai feltételei fennállnak. Ami törvényi feltételeket illeti, a nemzetbiztonsági szolgálatok tevékenységének egésze törvényi szabályozásnak van alávetve. Ebből a Jelentés a kémprogram alkalmazásának közvetlen jogi előfeltételét, a külső engedélyt emeli ki. A technikai feltételek között pedig a kémprogram telepítéséről indokolt szót ejteni.

A kémprogram alkalmazás jogi feltételei - a külső engedély

Az Ntbv. szabályozási rendszerében a titkos információgyűjtés azon eszközei és módszerei igényelnek külső engedélyt, amelyek legerősebben és legközvetlenebbül érinthetik a magán- és családi élet, az otthon és a kapcsolattartás tiszteletben tartásához, valamint a személyes adatok védelméhez fűződő jogot. Az Nbtv. 56. § e) és b) pontjaiban foglaltak a külső engedélyhez kötött eszközök és módszerek közé tartoznak, így megállapítható, hogy a kémprogram alkalmazás külső engedélyhez kötött.

A külső engedély tárgyában történő határozathozatal időben megelőzi az eszközalkalmazást és a külső engedély a titkos információgyűjtés megkezdésének előfeltétele. (Ez alól kivétel az Nbtv. 59. § szerinti eljárás, ám az eszközalkalmazás folytatása és az adatok felhasználása az Nbtv. 60. § (2) bekezdése szerint ebben az esetben is a külső engedély megadásához van kötve.)

Az eljárás a külső engedély iránti előterjesztés benyújtásával indul. Az Nbtv. egységesen szabályozza a külső engedély iránti előterjesztés adattartalmát, ezért a kémprogram alkalmazására vonatkozó előterjesztést illetően elég csak a kémprogrammal összefüggésben értelmezést igénylő kérdéseket tárgyalni:

- A titkos információgyűjtés megnevezése: a titkos információgyűjtés eszközeinek és módszereinek kategóriáit az Nbtv. határozza meg, ezért minimumkövetelmény az Nbtv. által használt megnevezés használata. Ez a kémprogram esetében az Nbtv. 56. § e) pontja szerinti megnevezés. Ha a tervezett eszközalkalmazás a lakásban történtek megfigyelését és rögzítését is magába foglalja, akkor az előterjesztésnek az Nbtv. 56. § b) pontja szerinti megnevezést is tartalmaznia kell. Véleményünk szerint a helyes gyakorlat az, ha az előterjesztés ezeken túl egyértelművé teszi, hogy a titkos információgyűjtés ténylegesen kémprogram alkalmazásával történik, ugyanis ez az információ is hozzájárul ahhoz, hogy az engedélyező megalapozott döntést hozzon a titkos információgyűjtés szükségességéről és a cél elérésére

alkalmas voltáról. (Erről a kémprogram alkalmazás adatvédelmi hatásprofiljáról szóló részben még lesz szó.)

- A titkos információgyűjtés helye: annak az objektumnak (lakásnak, irodának, helyiségnek stb.) a pontos címe, elhelyezkedése, ahol a kémprogram célrendszere található. Ha célrendszer mobil eszköz (például laptop, táblagép), akkor a titkos információgyűjtés földrajzi helyének pontos megadására nincs mód, mert az az eszközalkalmazás időszakában változhat. Mobil célrendszerek esetén az eszközalkalmazás helye jobb híján úgy adható meg, ha az előterjesztés a titkos információgyűjtés helyeként a mobil célrendszert azonosítja. Például így: „*az X. Y. által használt, Z. típusú, W. gyártási számú notebook*".

Az engedélyező arról dönt, hogy a külső engedély iránti előterjesztés megalapozott-e. A döntési folyamat teljes rekonstruálása nélkül az előterjesztés megalapozottságának mibenlétét illetően kiemelendők a következők:

- A titkos információgyűjtés csak a nemzetbiztonsági szolgálat Nbtv.-ben meghatározott feladatának teljesítése érdekében történhet, de nem vonatkozhat az Nbtv. 4. § h) pontjában és a 8. § (1) bekezdés d)-e) pontjaiban meghatározott feladatok ellátására (Nbtv. 53. § (1) bekezdés).

- az Nbtv. 53. § (2) bekezdése szerint a nemzetbiztonsági szolgálatok a titkos információgyűjtés speciális eszközeit és módszereit csak akkor használhatják, ha az e törvényben meghatározott feladatok ellátásához szükséges adatok más módon nem szerezhetők meg;

- Az előterjesztésnek az Nbtv. szerint az előterjesztés benyújtására jogosult személytől kell származnia. Az Nbtv. 57. § (2) bekezdése szerint az előterjesztésnek tartalmaznia kell a

> „*a) a titkos információgyűjtés helyét, az érintett vagy érintettek nevét vagy körét, illetőleg az azonosításra alkalmas - rendelkezésre álló - adatokat;*
> *b) a titkos információgyűjtés megnevezését és szükségességének indokolását;*
> *c) a tevékenység kezdetét és végét napban meghatározva;*
> *d) az 59. §-ban meghatározott engedély iránti előterjesztés esetén annak indokolását, hogy adott ügyben arra a nemzetbiztonsági szolgálat eredményes működéséhez feltétlenül szükség volt*"

Az ismertetett szabályok értelmében az engedélyező dönt arról, hogy az előterjesztésben foglaltak alátámasztják-e a titkos információgyűjtés szükségességét, továbbá konkretizálja az alkalmazható eszközt, illetve módszert, az alkalmazás helyét, időbeli kezdetét és végét, és (egyedileg vagy csoportismérv szerint) az érintetteket. Ennek során úgy kell meghatározni a titkos információgyűjtés kereteit, hogy az a személyes adatok célhoz kötött kezelésének követelményével (Infotv. 4. § (1) és (2) bekezdések) összhangban az információgyűjtés céljának eléréséhez szükséges legkisebb mértékben korlátozza a magánélet tiszteletben tartásához, valamint a személyes adatok védelméhez való jog érvényesülését. A szükségesség követelménye tehát nem csak arra vonatkozik, hogy a titkos információgyűjtés szükséges-e, hanem arra is, hogy hol, mettől, meddig, milyen módon és kivel szemben szükséges.

A hatályos törvényi szabályozás nem tartalmaz arra vonatkozó előírást, miszerint a külső engedély iránti előterjesztésben feltüntetésre kerüljön az adatkezelés célja, például annak az Nbtv.-ben meghatározott feladatkörnek a megjelölésével, melyek teljesítése érdekében a titkos információgyűjtés szükséges. Emiatt a jogi szabályozás nem garantálja azt, hogy az engedélyező a döntés során minden esetben megvizsgálhassa a következő kérdéseket:

- A titkos információgyűjtés nemzetbiztonsági szolgálat feladatkörébe tartozó feladat ellátásához szükséges?

- A titkos információgyűjtés annak a nemzetbiztonsági szolgálatnak a feladatkörébe tartozó feladatnak az ellátásához szükséges, amely a külső engedély iránt előterjesztéssel élt?

- A titkos információgyűjtés szükségességének indokai összhangban vannak azzal a feladattal, melynek teljesítésére a titkos információgyűjtés szolgál?

- Az előterjesztésben meghatározott eszköz, illetve módszer alkalmas az eszközalkalmazás céljának elérésére?

Lehetséges, hogy adott esetben az előterjesztésben az alkalmazás szükségességét megalapozó indokolás tartalmaz a fenti kérdések megválaszolásához szükséges információkat, de a célmeghatározás közlésére vonatkozó törvényi előírás hiányában ez esetleges, ezért e tekintetben az Nbtv. kiegészítése indokolt lenne.

A kémprogram alkalmazás technikai feltételei - a kémprogram telepítése

A kémprogram telepítése azaz a célrendszerbe juttatása és működőképessé tétele nélkül nem lehetséges annak alkalmazása, azonban a telepítés még nem része az eszközalkalmazásnak, mert a telepítés során még nem kezdődik meg a titkos információgyűjtés. Emiatt a kémprogram telepítésére általában nem vonatkoztathatók a személyes adatok kezelésére vonatkozó elvek és szabályok. Azonban a kémprogram telepítése közvetve befolyásolhatja a magánélet tiszteletben tartásához és a személyes adatok védelméhez való jog érvényesülésének feltételeit, ezért a következőket szükséges figyelembe venni a telepítést illetően:

- Mind a személyes adatok védelme, mind az eszközalkalmazás eredményessége szempontjából lényeges, hogy a kémprogramot az előzetesen kiválasztott és meghatározott célrendszerre telepítsék. Ha nem így történik, akkor a kémprogram alkalmazása olyan személyes adatok megszerzését eredményezheti, amelyek kezelése nem felel meg a célhoz kötött adatkezelés követelményének. Ezért a telepítés módjának meghatározása és a telepítés végrehajtása során a kellő gondossággal kell eljárni.

- A kémprogram rejtettsége a telepítéstől kezdve egészen az eszközalkalmazás megszüntetéséig a titkos információgyűjtés eredményességének feltétele. Ugyanakkor a titkosság azért is fontos, hogy illetéktelen személy ne szerezhessen tudomást arról, hogy a célrendszer felhasználója titkos információgyűjtés érintettje. A nemzetbiztonsági szolgálat az érintett érdekében is köteles megóvni őt attól, hogy

illetéktelenek tudomást szerezhessenek a vele szemben folytatott titkos információgyűjtés tényéről.

- A kémprogram telepítése és alkalmazása során a kémprogram és az irányító szerverrel való kommunikáció elrejtése céljából a célrendszer bizonyos elemeinek – például a tűzfal, az operációs rendszer stb. - módosítására is sor kerülhet. Azonban e módosítások nem érinthetik a célrendszer működésének biztonságát. Nem fogadható el „mellékhatásként" az, hogy a célrendszeren tárolt adatokat illetéktelen megszerezhesse, vagy az adatok hozzáférhetetlenné váljanak a célrendszer felhasználója számára. Ezért még ideiglenesen sem engedhető meg például a célrendszer tűzfalának vagy vírusvédelmének kikapcsolása, vagy az operációs rendszer működésének olyan módosítása, amely mások számára is könnyen hozzáférhető távfelügyeleti funkciókat aktivizál a felhasználó tudta nélkül.

- A kémprogram működésének biztonsága is alapkövetelmény. Azon túl, hogy illetéktelen nem fedezheti fel a kémprogramot, arról is gondoskodni kell, hogy ha mégis felfedezik, akkor illetéktelen személy ne használhassa azt a célrendszerből történő titkos információgyűjtésre.

A kémprogram alkalmazása

A kémprogram alkalmazása a célrendszer útján továbbított, vagy azon tárolt adatok megismerése és azok tartalmának rögzítése. Adatvédelmi szempontból az vizsgálandó, hogy ez milyen hatással járhat a titkos információgyűjtés érintettje információs önrendelkezési jogának érvényesülésére. Konkrét nemzetbiztonsági feladat ellátása során a titkos információgyűjtés tervezésekor az alkalmazó nemzetbiztonsági szolgálatnak, illetve a külső engedélyezés folyamán az engedélyezőnek arra a kérdésre is választ kell találnia, hogy a titkos információgyűjtés adott célra alkalmas eszközei és módszerei közül melyik az, amely az érintett információs önrendelkezési jogát a legkevésbé korlátozza. A legkevésbé jogkorlátozó eszköz kiválasztásához tudni kell azt, hogy a kémprogram alkalmazás információs alapjogi hatása miben tér el a többi szóba jöhető eszköz és módszer hatásától. Ezért figyelembe kell venni az eszköz adatvédelmi hatásprofilját.

A kémprogram alkalmazás adatvédelmi hatásprofiljának összetevői

1. A kémprogram alkalmazása révén a számítógépes hálózati adatforgalom megfigyelésére szolgáló passzív eszközök és módszerek (a továbbiakban passzív eszközök) alkalmazásánál nagyobb mértékben képes beavatkozni az érintettek magánéletébe, mert többféle adat megismerését és az adatok többféle felhasználást teszi lehetővé.

- Ami az adatokat illeti, a kémprogram a passzív eszközöktől eltérően a célrendszer útján továbbított adatokon kívül a célrendszerben tárolt adatokhoz, valamint a célrendszer érzékelőinek jeleihez is hozzáférhet. Az Nbtv. nem korlátozza általános érvénnyel, hogy a titkos információgyűjtés milyen adatfajtákra vonatkozhat. Az, hogy a kémprogram alkalmazása során megszerzett és rögzített információk összhangban vannak-e a titkos információgyűjtés céljával, csak konkrét titkos információgyűjtéssel összefüggésben vizsgálható. Általános érvénnyel csak az a

megállapítás tehető, hogy bármely adat, amely a számítógépen hozzáférhető, a kémprogrammal végzett titkos információgyűjtés potenciális tárgya lehet.

- A kémprogram törvényes felhasználási lehetőségei az Nbtv. 56. § e) pontjában meghatározott tevékenység révén:

a) a célrendszerben tárolt adatok megismerése, rögzítése,

b) a célrendszer felhasználója kommunikációjának és magatartásának megfigyelése, valamint

c) a célrendszer környezetének megfigyelése (de lakás esetében csak az Nbtv. 56. § b) pontjában foglaltakra vonatkozó jogi és technikai feltételek fennállása esetén).

2. A kémprogram alkalmazása irányított adatgyűjtést tesz lehetővé

Az alkalmazást végző nemzetbiztonsági szolgálat az eszköz működésének előzetes beállításai révén, illetve az alkalmazás folyamán irányító szerver útján irányítja az adatgyűjtést. Ez a kémprogram működésének megindításán, időzítésén és leállításán túl az adatforrások (célrendszeren tárolt vagy továbbított adatok, a célrendszer érzékelőinek jelei) és az adatgyűjtés részleteinek (például bizonyos alkalmazás működése során keletkezett adatok, meghatározott típusú adatállományok, a megadott keresési kulcsnak megfelelő adatok) meghatározására is kiterjedhet. A kémprogram például

* megnyithat és beolvashat adatállományokat,
* az alkalmazó által meghatározott szempontok szerint adatfeldolgozást végezhet, például kereshet a célrendszerben tárolt adatok között,
* módosíthatja a célrendszer működését, például bekapcsolhat érzékelőket,
* az adatokat az alkalmazóhoz továbbítja.

A kémprogram alkalmazás e sajátossága azért lényeges a személyes adatok védelme szempontjából, mert a lehetővé teszi, hogy az alkalmazást végző szerv a célhoz kötött adatkezelés követelményének megfelelően a cél eléréséhez szükséges adatokra korlátozza a titkos információgyűjtést. Ez fejlett eszközalkalmazási kultúrát igényel a kémprogramot alkalmazó nemzetbiztonsági szolgálat részéről.

A kémprogram alkalmazásának irányított jellegével szembeállítható a passzív eszközök alkalmazása. Minthogy ez utóbbiak esetében elsősorban a megfigyelt adatforgalom szűrésével válogathatók ki az alkalmazás céljának eléréséhez szükséges információk, a passzív eszközök alkalmazására inkább jellemző a szűrő-kutató jellegű adatkezelés, továbbá sokkal inkább fennáll a célhoz kötött adatkezelés követelményét sértő, készletező jellegű adatgyűjtés veszélye.

3. A képprogram kevéssé alkalmas tömeges alkalmazásra

- A képprogram alkalmazási környezete a célrendszer, amely a célrendszer felhasználója számára hozzáférhető, ezért a távoli, passzív eszközökénél több lehetőség van a képprogram felhasználó általi felfedezésére. Minél több célrendszerre telepítenek egyidejűleg képprogramot, annál nagyobb a valószínűsége annak, hogy valamelyik célrendszer felhasználó azonosítja.

- A képprogram működése hasonlít a számítógépes kártevőkére, ezért fennáll a lehetőség arra, hogy felfigyel rá valamelyik számítógépes kártevők elleni programot fejlesztő cég. Tömeges alkalmazás esetén arra is számítani lehetne, hogy a képprogram előfordulási gyakorisága eléri azt a szintet, hogy valamelyik informatikai biztonsági fejlesztő cég számára kifizetődővé válik védelmet fejleszteni ellene. Emiatt a gyakorlatban a képprogram tömeges alkalmazására ténylegesen akkor sem lenne lehetőség, ha az adatvédelmi szempontból megengedhető lenne. E technikai alkalmazási korlát adatvédelmi szempontból tulajdonképpen kedvező, mert az eszközalkalmazási kapacitás behatárolt volta arra készteti a lehetséges képprogram alkalmazókat, hogy minden esetben gondosan mérlegeljék az alkalmazás szükségességét.

A képprogram alkalmazás időtartama és az alkalmazás megszüntetése

A képprogram alkalmazás kezdőnapját és végét az engedélyező határozza meg. Az Nbtv. 58. § (4) bekezdése szerint az engedélyező a titkos információgyűjtést e törvény eltérő rendelkezése hiányában esetenként legfeljebb 90 napra engedélyezi. Ezt a határidőt az engedélyező indokolt esetben - a főigazgatók előterjesztése alapján - e törvény eltérő rendelkezése hiányában további 90 nappal meghosszabbíthatja. Azonban az Nbtv. 60. § (1) bekezdése értelmében a törvényes és célhoz kötött adatkezelés követelményének megfelelően a titkos információgyűjtést ezen az időtartamon belül is haladéktalanul meg kell szüntetni, ha

a) az engedélyben meghatározott célját elérte;
b) a további alkalmazásától eredmény nem várható;
d) a titkos információgyűjtés bármely okból törvénysértő.

Az idézett szabályok alapján a képprogram alkalmazás megkezdésekor még nem tudható biztosan, hogy mikor kell megszüntetni az eszköz alkalmazását. Ezért az irányító szervernek képesnek kell lennie képprogram működésének haladéktalan megszüntetésére, ha az alkalmazás jogi feltételi megszűntek. A működés megszüntetése azt jelenti, hogy a képprogram többé nem rögzít adatot a célrendszeren és nem tesz hozzáférhetővé a célrendszeren tárolt, vagy továbbított adatot.

Ha a képprogram alkalmazásának megszüntetésével egyidejűleg nem kerül sor a képprogram célrendszerből való törlésére (például azért, hogy ha később ismét megteremtődnek az alkalmazás jogi feltételei, akkor ismételt telepítés nélkül rendelkezésre álljon), úgy a következő adatvédelmi követelmények fogalmazódnak meg:

- Az inaktív kémprogramnak rejtve kell maradnia. A nemzetbiztonsági szolgálat az érintett személy érdekében is köteles megóvni őt attól, hogy illetéktelenek tudomást szerezhessenek a vele szemben folytatott titkos információgyűjtés tényéről.

- Gondoskodni kell arról, hogy ha egy illetéktelen harmadik személy mégis felfedezi az inaktív kémprogramot, akkor ne használhassa azt a célrendszerből történő titkos információgyűjtésre.

III. A vizsgálat

A vizsgálat körülményei

A Hatóság eljárását kezdeményező bejelentés a magyar nemzetbiztonsági szolgálatok kémprogram használatára vonatkozott, ezért Hatóságunk e szervezetek adatkezelését illetően folytatott vizsgálatot, mellőzve a további, a törvény szerint titkos információgyűjtésre és titkos adatszerzésre jogosult szervezetek tevékenységének vizsgálatát. Az Infotv. 2. § (1) bekezdése szerint az Infotv. hatálya a Magyarország területén folytatott, személyes adatra vonatkozó adatkezelésekre és adatfeldolgozásokra vonatkozik, ezért a vizsgálat nem terjedhetett ki az Információs Hivatal országhatáron kívül történő adatkezelésére. Az Infotv. 71. § (3) bekezdése szerint a Hatóság az alapvető jogok biztosáról szóló 2011. évi CXI. törvény 23. § (2) bekezdésében meghatározott adatokat az alapvető jogok biztosáról szóló 2011. évi CXI. törvény 23. § (7) bekezdésében 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.

A kémprogram alkalmazása speciális technikai eszközt igényel, ezért Hatóságunk az Nbtv. 8. § (1) bekezdés a) pontjára tekintettel az NBSZ-nél végezte a titkos információgyűjtő tevékenység adatvédelmi vizsgálatát.

Hatóságunk a vizsgálat során a tényállás tisztázása érdekében a következő vizsgálati cselekményeket foganatosította:

- A Hatóság elnöke részt vett az Országgyűlés Nemzetbiztonsági bizottságának zárt ülésén, amelyen a vizsgálatunk tárgyára vonatkozó tájékoztató hangzott el.

- Egy másik alkalommal a Hatóság munkatársa részt vett az Országgyűlés Nemzetbiztonsági bizottságának kihelyezett zárt ülésén, ahol az NBSZ titkos információgyűjtő tevékenységére vonatkozó tájékoztató hangzott el.

- A Hatóság munkatársa helyszíni vizsgálat során részt vett egy bemutatón, amelyen az adatkezelést végző szerv a titkos információgyűjtés eszközeinek és módszereinek alkalmazását demonstrálta.

- A Hatóság részletes írásbeli felvilágosítást kért az NBSZ főigazgatójától a kémprogramok titkos információgyűjtés keretében történő alkalmazásáról. Az információigény a következő főbb tárgykörökre terjedt ki:

* az alkalmazott kémprogram azonosítása,
* a kémprogram funkcionalitása (honnan, milyen szenzorokból, adatforrásokból, eszközökből, milyen jellegű adatokat képes gyűjteni),
* alkalmazás statisztika (alkalmazás száma/év),
* a szolgáltatást megrendelő szervezetek megnevezése,
* a kémprogram alkalmazásának biztonsága (telepítés esetén nem jelzi a titkos információgyűjtést harmadik személy számára, illetve nem teszi hozzáférhetővé a számítógépet harmadik személy számára),
* az alkalmazás feltételeit meghatározó törvényi előírások NBSZ általi értelmezése és alkalmazása, különös tekintettel a titkos információgyűjtés külső engedélyezésére.

IV. Megállapítások

- 2011. január 1-jén lépett hatályba az Nbtv. 56. § e) pontja, amely alapján a nemzetbiztonsági szolgálatok a törvényben meghatározott feladataik ellátása során kémprogramot alkalmazhatnak. A törvény a kémprogram alkalmazását nem nevesíti külön a titkos információgyűjtés eszközei és módszerei között, azonban jogértelmezés útján egyértelműen meghatározhatók a kémprogram alkalmazásra vonatkozó szabályok az Nbtv. szabályozási rendszerében. A kémprogram alkalmazása külső engedélyhez kötött titkos információgyűjtés. A törvényi szabályozás kellő garanciát nyújt a titkos információgyűjtéssel érintettek magánszférájának tiszteletben tartásához és személyes adataik védelméhez való joguk érvényesülése érdekében.

- A törvényi szabályozás áttekintése során egy „nem kémprogram specifikus" kérdésben merült fel, hogy indokolt lenne az Nbtv.-t pontosítani: a külső engedélyezési eljárás során célszerű lenne egyértelművé tenni, hogy az előterjesztésnek tartalmaznia kell annak a feladatnak a megjelölését, amelyre tekintettel a titkos információgyűjtés szükséges, hogy az engedélyező minden esetben a cél-eszköz viszonylatában is vizsgálhassa a titkos információgyűjtés szükségességét.

- A gyors infokommunikációs technikai fejlődés az Nbtv. hivatkozott módosításának hatályba lépése óta eltelt néhány év alatt is változtatta a kémprogram alkalmazási környezetét. Például olyan számítástechnikai rendszerek térnyerése tapasztalható, amelyek mobilisak, használatunk nem helyhez, hanem kifejezetten személyhez kötött és újfajta érzékelőkkel rendelkeznek, amelyek révén a titkos információgyűjtés során újfajta lehetőségek nyílnak a felhasználók és környezetük megfigyelésére. E változások megnövelik a számítástechnikai rendszerekből történő titkos információgyűjtés lehetőségeit és felértékelik a titkos információgyűjtés hagyományos módozataival szemben. Ez egyelőre nem igényli a törvényi szabályozás adatvédelmi garanciarendszerének felülvizsgálatát, azonban a technikai környezet változásának gyorsasága indokolttá teszi, hogy a Hatóság a jövőben időről időre visszatérően vizsgálja, hogy a törvényi szabályozás képes-e fenntartani az egyensúlyt a titkos megfigyelés lehetőségei és az érintettek információs jogainak érvényesülése között. Ez annál is inkább fontos, mert a titkos információgyűjtés szükségképpen az érintettek tudomása nélkül történik, így ők nem képesek a jogaik védelme érdekében fellépni és a titkosság folytán a közvélemény sem képes ítéletet alkotni arról, hogy az állami szervek titkos információgyűjtő tevékenysége megfelel-e a demokratikus jogállami normáknak.

- A vizsgálat során megismert tényekből az a következtetés adódik, hogy a Nemzetbiztonsági Szakszolgálat a a kémprogram alkalmazásával kapcsolatban a törvényi előírásokat maradéktalanul betartva hajtja végre az Nbtv. 8. § (1) bekezdés a) pontjában meghatározott feladatait. A vizsgálat során jogsértésre vonatkozó információ nem merült fel.

- A megismert tények alapján alaptalanok azok a sajtóban megjelent aggodalmak, melyek szerint a magyar nemzetbiztonsági szolgálatok kémprogram alkalmazásával tömeges megfigyelést végeznek.

Köszönettel tartozom az Országgyűlés Nemzetbiztonsági bizottságának a vizsgálathoz nyújtott értékes segítségéért. Nagyra értékelem a Nemzetbiztonsági Szakszolgálat vezetőinek és munkatársainak korrekt együttműködését a vizsgálat folyamán.

Budapest, 2014. december „ „

Dr. Pérterfalvi Attila
elnök
c. egyetemi tanár