Az elektronikus kommunikáció titkos megismerésével kapcsolatos jogszabályi garanciák Magyarországon

Parti Katalin*

1. Bevezetés

Az elmúlt évek adatvédelemmel összefüggő fejleményei, amelyek hatására szigorított feltételekkel gyűjthetők, hallgathatók le, rögzíthetők és adhatók át a felhasználók adatai, mind a belföldi nyomozó hatóságok számára, mind pedig az egyes tagállamok nyomozó hatóságai között, új kihívások elé állította a jogalkotót. Ezekre a kihívásokra válaszol részben a 2018. július 1-jétől hatályos új büntetőeljárási törvény, amely az állampolgári alapjogok védelme, valamint azok szükséges és arányos korlátozhatósága érdekében megszünteti a titkos információgyűjtés és a titkos adatszerzés közötti különbséget, és bevezeti a leplezett eszköz jogintézményét. Ugyanakkor a telekommunikációs (internet) szolgáltatók továbbra is – adatgyűjtésben és átadásban megnyilvánuló – együttműködésre kötelesek, hiszen közreműködésük nélkül nem lenne adat, azaz bizonyíték az igazságszolgáltatás kezében. A nyomozó hatóság és a titkos információgyűjtésre (összefoglalóan: megfigyelésre) feljogosított szervek pedig az adatvédelmi rendelkezéseket szem előtt tartva abszolválhatják feladataikat. Az elektronikus adatok megismerésének a büntetőeljárási törvényben, valamint a rendészeti és a nemzetbiztonsági célú titkos információgyűjtést szabályozó ágazati törvényekben lefektetett szabályait a tanulmány a magánélethez fűződő alapvető jogok szemszögéből vizsgálja.

2. Az új Be. szabályai a leplezett eszközökről

A 2017. évi XC. törvény a büntetőeljárásról (a továbbiakban új Be.) kimondja, hogy minden tevékenység, amelyet az ügyészség/nyomozó hatóság korábban a titkos információgyűjtés vagy a titkos adatszerzés keretében végzett[1], a büntetőeljárás

* Assistant professor, Department of Sociology, Virginia Tech

[1] FARKAS Ákos – RÓTH Erika: *A büntetőeljárás*. Negyedik, átdolgozott kiadás. Wolters Kluwer, Budapest, 2018. 293.

leplezett eszközének minősül. Leplezett eszköz alkalmazható a büntetőeljárásban bírói vagy ügyészi engedéllyel, illetve engedély nélkül – a szükségesség és az arányosság feltételei mellett.

Nem szükséges külön engedély ahhoz, hogy a leplezett eszközök alkalmazására feljogosított szerv a bűncselekményre vonatkozó információ megszerzése érdekében titkosan együttműködő személyt vegyen igénybe (*leplezett eszköz alkalmazása külső engedély nélkül:* új Be. 215. §), a leplezett eszközök alkalmazására feljogosított szerv tagja a bűncselekményre vonatkozó információt gyűjtsön, ellenőrizzen, sérülést vagy egészségkárosdást nem okozó csapdát állítson, vagy a sértett helyettesítésére dublőrt állítson a bűncselekmény megszakítása, elkövetőjének felderítése és a bizonyítás érdekében, továbbá a sértett életének és testi épségének megóvása céljából.

Az *ügyészi engedélyhez kötött leplezett eszközök* [új Be. 214–260. §] közül a tanulmányban a *sértett írásbeli hozzájárulásával alkalmazott megfigyelést* szükséges megemlíteni [új Be. 220. §], hiszen ebben az esetben a sértett önként mond le a magánéletének védelmét biztosító jogokról az őt érintő bűncselekmény felderítése, folytatásának megakadályozása, illetve bizonyítékok gyűjtése érdekében. Ilyen bűncselekmény különösen a kapcsolati erőszak, a zaklatás, illetve a fenyegetéssel megvalósuló bűncselekmények. Ilyenkor a leplezett eszköz alkalmazására feljogosított szerv a sértett, illetve a bűncselekmény elkövetésére felhívás vagy rábírás címzettje által használt elektronikus hírközlő hálózaton vagy más információs rendszeren folytatott kommunikáció tartalmát megismerheti, technikai eszközzel rögzítheti, és a kommunikációban részt vevők személyes adatait megismerheti. Mivel a zaklatás és a kapcsolati erőszak sokszor elektronikus eszközön keresztül valósul meg, a jogintézményt valószínűleg gyakran fogják alkalmazni. A törvény ezen kívül külön kitételt tartalmaz az elektronikus hírközlési szolgáltatás útján való kommunikáció megismerésére [új Be. 220. § (4) bek.].

Az *információs rendszer titkos megfigyelése* – ide tartozik az elektronikus hírközlési szolgáltató rendszerében az elektronikus kommunikáció megfigyelése és rögzítése – és a telekommunikációs eszközökön folytatott kommunikáció megismerése, azaz a klasszikus értelemben vett *lehallgatás* – bírói engedélyhez kötött [új Be. 232. § (5) bek.]. A bíró az ügyész indítványa alapján határoz [új Be. 236. § (1) bek.).] Ha *az engedélyezés olyan késedelemmel járna*, amely az elérni kívánt célt jelentősen veszélyeztetné, az ügyészség „titkos kutatást" rendelhet el, illetve a bíróság döntéséig, de legfeljebb 120 órára elrendelheti a leplezett eszköz alkalmazását [új Be. 238. § (1) bek.]. De az ügyészség ilyenkor is, az elrendelést követő 72 órán belül indítványt tesz a bíróságnak az utólagos engedélyezés érdekében, amelyről a bíróság 120 órán belül dönt. Ha a bíróság az engedélyt nem adja meg, úgy a leplezett eszközzel szerzett információ bizonyítékként nem használható fel, és az adatokat haladéktalanul törölni kell [új Be. 238. § (5) bek.].

Az új Be. ugyan nem jut el addig, hogy kimondaná: a nemzetbiztonsági szolgálatok nem végezhetnek bűnügyi felderítést, jóllehet azt eléri, hogy minden titkos felderítési eszköz alkalmazására rálát az ügyész: az ügyész felügyelete alatt olyan adatok és úgy kerülnek bekérésre és rögzítésre a nyomozás során, amely

lehetővé teszi a leplezett eszközök által megszerzett adatok büntetőügyben való felhasználását.[2]

Az elektronikus kommunikáció megismerhető a fentieken kívül bűnüldözési és a nemzetbiztonsági célú titkos információgyűjtéssel is; ez a büntetőeljárási törvényen kívüli, ágazati jogszabályok alapján lehetséges.

3. Az elektronikus kommunikáció megfigyelésének alkotmányos és jogszabályi biztosítékai

3.1. A megfigyelés módszere, eszköze. A leplezett eszközök alkalmazásakor és a titkos információgyűjtéskor bármilyen módszer megfelelhet a jogi előírásoknak, ami nem valósít meg tömeges (cél nélküli) és készletező jellegű adatgyűjtést. A Zakharov v. Oroszország-ügyben[3] és a Szabó és Vissy v. Magyarország-ügyben[4] az EJEB joggyakorlata úgy összegezte az elvárásokat, hogy mindig legyen egyértelmű időintervallumra korlátozva a lehallgatás. Ezt az új Be. úgy rendezi, hogy eszközalapúvá teszi a titkos adatgyűjtés szabályozását: egy személlyel szemben bármennyi eszközt használható (eszközmultiplikáció), de a megfigyelés alkalmanként 90 napig tarthat, és mindösszesen 360 nap áll rendelkezésre a megfigyelésre [új Be. 239. §]. Egy személy lehallgatására egyetlen engedélyt kell kérni és azt az eljárás adatai alapján lehetséges módosítani például akkor, ha a lehallgatást más eszközökre is ki kell terjeszteni. Az egyes titkos információgyűjtési módszereket együttesen, egymást kiegészítően is alkalmazhatják az arra feljogosított szervek. Az elrendelés ügyészi indítványhoz kötött és nyomozási bíró rendeli el. Az új Be. tehát a régi Be.-hez képest erős garanciákat ad.

3.2. Garanciák a készletező jellegű adatgyűjtés ellen. A magánszférához, a magán- és családi élet tiszteletben tartásához való jogot és az ezzel szoros összefüggésben álló információs önrendelkezési jogot Magyarország Alaptörvényének VI. cikke biztosítja. Ezek az emberi méltósággal szoros kapcsolatban álló jogok együttesen hivatottak biztosítani azt, hogy az érintett akarata ellenére mások ne hatolhassanak be a magánszférájába. Ugyanakkor alkotmányos demokráciákban is elfogadott a magánszférához való jog korlátozása olyan legitim célok érdekében, mint a nemzet- és közbiztonság, a bűncselekmények megelőzése és felderítése, valamint az állam büntetőjogi igényének érvényesítése, azaz ezen jogok megsértésének tilalma nem ius cogens.[5] A magánszférához való jog korlátozásának azonban ki kell állnia az alapjogsérelem alkotmányos megengedhetőségének megítélésére irányadó, háromlépcsős alapjogi teszt próbáját. Így 1) a korlátozásnak alkalmasnak kell lennie a kívánt cél elérésére (alkalmasság-teszt). 2) A szükségesség követelménye csakis akkor teljesülhet, ha a tervezett jogkorlátozásokat az említett célok elérése kényszerítően megkívánja,

[2] Az ügyészi ellenőrzés közvetlenségéről és problémáiról lásd részletesen: FARKAS– RÓTH: i.m. 315–318.
[3] *Roman Zakharov v. Russia*, judgement of 4 December 2015, no. 47143/06
[4] *Szabó and Vissy v. Hungary*, judgement of 1 December 2016, no. 37138/14
[5] BAKONYI Mária: A leplezett eszközök megítélése az EJEB joggyakorlatában. *Ügyészek Lapja,* 2019/1. 87–97.

azaz olyan kvalifikált fenyegetettség áll fenn, amelyek esetében a rendelkezésre álló eszközök alkalmazása nem vezetne eredményre (szükségesség-teszt). 3) A tervezett korlátozások arányossága pedig annak függvénye, hogy milyen alkotmányos garanciák érvényesülnek (arányosság-teszt). Jogkorlátozásra azok alkalmasságát és szükségességét megalapozó körülmények fennállása esetén is csak törvényben rögzített, szigorú és átlátható eljárási rendben, a magánszférába való beavatkozás minden részletkörülményére kiterjedő, adekvát intézményes garanciák mellett kerülhet sor.

Magyarország Alaptörvénye deklarálja az említett magánélet tiszteletben tartásához való jogot [VI. Cikk (1) bek.], a személyes adatok védelméhez és a közérdekű adatok nyilvánosságához való jogot [VI. Cikk (2) bek.], valamint azt, hogy a személyes adatok védelméhez és a közérdekű adatok megismeréséhez való jog érvényesülését sarkalatos törvénnyel létrehozott, független hatóság ellenőrzi [VI. Cikk (3) bek.]. Ezen túl a célhoz kötöttség követelménye az adott szerv hatáskörét meghatározó ágazati jogszabályokban van lefektetve. Az ágazati jogszabályok meghatározzák, hogy milyen szűk körben és milyen lépcsőzetes szabályok betartásával lehet ilyen eszközöket alkalmazni. Ilyen az 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról (a továbbiakban Nbtv.), amely kimondja, hogy *„A nemzetbiztonsági szolgálatok az adatkezelés során kötelesek az adott cél eléréséhez feltétlenül szükséges, ugyanakkor az érintett személyiségi jogait legkevésbé korlátozó eszközt igénybe venni.”* [Nbtv. 39. § (2) bek.]. A nemzetbiztonsági célú titkos információgyűjtést határozott időre szóló engedélyhez köti, amelyben meg kell jelölni a titkos információgyűjtés szükségességének indokolását is [Nbtv. 57. § (2) bek.]. A külső engedélyhez kötött titkos információgyűjtést haladéktalanul meg kell szüntetni egyebek mellett akkor, ha az engedélyben meghatározott célját elérte, vagy bármely okból törvénysértő [Nbtv. 60. § (1) bek.]. Ez utóbbi esetben az információgyűjtés során nyert adatokat haladéktalanul meg kell semmisíteni [Nbtv. 59. § (2) bek.].

A rendőrségről szóló 1994. évi XXXIV. törvény a nyomozási cselekményekre és az adatkezelésre vonatkozóan állapít meg szükségességi és célhoz kötöttségi kritériumot – beleértve a bűnmegelőzési, felderítési, bűnüldözési feladatok ellátását is [Rtv. 77. § (1)–(2) bek.]. A rendőrségi feladatok ellátásához szükséges, azaz a „kezelhető adatok” körét a 81–91/T. §-ok határozzák meg. A rendőrségi adatkezelő szerv vezetője köteles gondoskodni arról, hogy a személyes adatok védelme érdekében az érintett – az információs önrendelkezési jogról és az információszabadságról szóló törvényben (2011. évi CXII. törvény, a továbbiakban Infotv.) meghatározott módon – kezelt adatai köréről tájékoztatást kapjon, valamint gyakorolhassa a helyesbítéshez, a törléshez és a zároláshoz való jogát. Az érintett kérheti, hogy a tárolt adatait töröljék, ha azok kezelése jogellenes, az adatok tárolásának törvényben meghatározott határideje lejárt, illetve a törlést a bíróság vagy a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) elrendelte [Rtv. 80. § (2) bek.]. Jogsérelem esetén az érintett bírósághoz vagy a NAIH-hoz fordulhat – erről tájékoztatni kell [Rtv. 80. § (4) bek.]. Akinek a rendőrség valamilyen intézkedése alapvető jogát sértette, panasszal fordulhat az intézkedést foganatosító rendőri szervhez is, és kérheti, hogy a panaszt az

intézkedést lefolytató, a panasszal érintett rendőri szerv felett felügyeleti jogkört gyakorló szervezet élén álló személy (pl. az országos rendőr-főkapitány, a terrorizmust elhárító szerv főigazgatója stb.) közvetlenül bírálja el [Rtv. 92. § (1) bek.].

A NAV nyomozó hatósága bűnüldözési, bűnmegelőzési, felderítési és nyomozási tevékenységet folytat (2010. évi CXXII. törvény a Nemzeti Adó- és Vámhivatalról, a továbbiakban NAVtv. 35. §). A kényszerintézkedések végrehajtására a szükségességi és arányossági követelmények betartásával kerülhet sor [NAVtv. 36/E. §]. A NAV engedélyhez nem kötött és bírói engedélyhez kötött titkos információgyűjtést végezhet bűnüldözési célból, a súlyos bűncselekmények (pénzmosás és terrorizmus finanszírozása) esetében, valamint a NAV nyomozó hatósági hatáskörébe utalt egyéb, üzletszerűen vagy bűnszövetségben elkövetett, három évig terjedő szabadságvesztéssel büntetendő, az adózás rendjét sértő bűncselekmények esetében [NAVtv. 63. § (1) bek.]. A bírói engedélyhez kötött titkos információgyűjtési tevékenysége körében, egyebek mellett, elektronikus hírközlési szolgáltatás útján továbbított kommunikáció tartalmát megismerheti, az észlelteket technikai eszközzel rögzítheti, valamint számítástechnikai eszköz vagy rendszer útján továbbított vagy azon tárolt adatokat megismerheti, rögzítheti és felhasználhatja [NAVtv. 63. § (1) bek. d)–e) pont]. Az eljárás során megszerzett, az eljárásban nem érintett személyekre vonatkozó adatokat haladéktalanul meg kell semmisíteni [NAVtv. 63. § (2) bek]. Mint minden – a bírói engedélyhez kötött titkos információgyűjtésre feljogosított – hatóság, a NAV az ún. különleges eszközök alkalmazását a Nemzetbiztonsági Szakszolgálattól (NBSZ) rendeli meg [NAVtv. 63. § (5) bek.]. Az eszközök alkalmazását legfeljebb 90 napra lehet elrendelni, alkalmazásuk kérelemre legfeljebb egyszer 90 nappal meghosszabbítható [NAVtv. 63. § (6) bek.]. Ha a különleges eszköz alkalmazásának engedélyezése olyan késedelemmel járna, amely az ügyben sértené a bűnüldözés eredményességéhez fűződő érdeket, a NAV titkos információgyűjtés folytatására feljogosított szervének vezetője legfeljebb a bírói döntésig engedélyezheti a különleges eszköz alkalmazását azzal, hogy haladéktalanul meg kell szüntetni az eszköz alkalmazását, ha azt a bíró nem engedélyezte vagy az engedélyben meghatározott célját elérte (NAVtv. 65. §). A különleges eszközzel szerzett adatokat a megfigyelés befejezését követő 8 napon belül meg kell semmisíteni, ha a megfigyelés célja szempontjából érdektelen vagy az ügyben nem érintett személlyel kapcsolatos. Az adatkezelésre, nyilvántartásra, szolgáltatásra, adatátadásra és átvételre vonatkozó rendelkezéseket a törvény 66–80/A. §-ai tartalmazzák. Ezen belül a bűnügyi adatkezelésre külön rendelkezések irányadók. Az ilyen adatokat csak bűnüldözés céljára lehet felhasználni (célhoz kötöttség) [NAVtv. 69. § (1) bek.]. A NAV nyomozó hatósága adatokat gyűjthet a bűnüldözési rendszerekből (pl. a rendőrség és ügyészség közös elektronikus adatbázisa, a Robotzsaru), továbbá saját, bűnüldözési és egyéb adatbázisait is összekapcsolhatja [NAVtv. 73. § (5) bek.]. A célhoz kötöttség itt is érvényesül. Adótitoknak, vámtitoknak minősülő adat azonban csak ügyészi jóváhagyással vehető át más adatbázisokból.

A NAV nyomozó hatósága az Európai Unió tagállamai, valamint az Európai Unió jogi aktusával létrehozott nemzetközi szervezetek és adatkezelési rendszerek részére bűnüldözési célból személyes és bűnüldözési adatokat továbbíthat vagy vehet át az Európai Unió jogi aktusa, illetve két- vagy többoldalú nemzetközi szerződés alapján az ott meghatározott adatkörben és időtartamban. A NAV nyomozó hatósága által kezelt személyes és bűnüldözési adat harmadik ország, valamint nemzetközi szervezet részére bűnüldözési célból nemzetközi szerződés alapján az ott meghatározott adatkörben és időtartamban az információs önrendelkezési jogról és az információszabadságról szóló törvényben meghatározott feltételek fennállása esetén is csak akkor továbbítható, ha a harmadik ország átvevő hatósága vagy az átvevő nemzetközi szerv feladata bűncselekmények megelőzése, nyomozása, felderítése, büntetőeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása [NAVtv. 77. § (1)–(2) bek.]. Amennyiben utólag megállapítják, hogy hibás adatokat továbbítottak vagy adatokat jogellenesen továbbítottak, erről a címzettet haladéktalanul értesíteni kell. A nemzetközi bűnügyi együttműködés keretében végzett adatátadásokról az információs önrendelkezési jogról és az információszabadságról szóló törvényben meghatározottak szerint adattovábbítási nyilvántartást kell vezetni [NAVtv. 77. § (4) bek.]. Ez a nyilvántartás azonban sem az állampolgár, sem a kutató számára nem nyilvános, így onnan statisztikai adatokat nem lehetséges lekérni.

Az internet- és a telekommunikációs szolgáltatásokra vonatkozó szabályok is tartalmaznak célhoz kötöttségi klauzulát. Az elektronikus kereskedelmi szolgáltatásokról szóló (2001. évi CVIII. törvény, a továbbiakban Ekertv.) szerint a szerződések létrehozása, tartalmának meghatározása, módosítása, teljesítésének figyelemmel kísérése, az abból származó díjak számlázása, valamint az azzal kapcsolatos követelések érvényesítése, illetve a szolgáltatás nyújtása céljából a szolgáltató kezelheti az igénybe vevő azonosításához szükséges és elégséges – tehát az elengedhetetlenül szükséges – azonosító adatokat (Ekertv. 13/A. §). Az „adattakarékosság elve" az elektronikus szolgáltatók esetében azt a kötelezettséget jelenti, hogy úgy kell megválasztani az információs társadalommal összefüggő szolgáltatás nyújtása során alkalmazott eszközöket, hogy személyes adatok kezelésére csak akkor kerüljön sor, ha ez a szolgáltatás nyújtásához feltétlenül szükséges, de ebben az esetben is csak a szükséges mértékben és ideig.[6] A szolgáltatás nyújtása céljából kezelt adatokat haladéktalanul törölni kell a szerződés létrejöttének elmaradása, a szerződés megszűnése, valamint a számlázás megszűnése után. Az információs önrendelkezési jogról és az információszabadságról szóló törvényben meghatározott tájékoztatáson kívül (Infotv. 14–19.§) a szolgáltatónak biztosítania kell, hogy az igénybe vevő a szolgáltatás igénybevétele előtt és közben is megismerhesse, hogy a szolgáltató mely adatfajtákat milyen célból kezel, ideértve a vevővel közvetlenül kapcsolatba nem hozható adatok kezelését is.[7]

[6] MEZŐ István: *Személyes adatok védelme az Európai Unió jogában és Magyarországon.* PhD értekezés. Miskolci Egyetem Deák Ferenc Állam- és Jogtudományi Doktori Iskola, Miskolc, 2009. 286. Elérhető: http://midra.uni-miskolc.hu/document/5522 (2018.06.15.)

[7] MEZŐ: i.m. 287.

Végül a Polgári Törvénykönyv (2013. évi V. törvény, a továbbiakban Ptk.) a személyiségi jogok körében a képmáshoz, hangfelvételhez, adathoz való jog körében fekteti le a magánélethez és az információszabadsághoz való jogokat [Ptk. 2:43. §].

Milyen konzekvenciával jár ezeknek a biztosítékoknak a megsértése? Ha az előírások megszegésével történik az adatgyűjtés, akkor az így megszerzett adat bizonyítékként nem használható fel a büntetőeljárásban vagy olyan más eljárás során, amelyben a megszerzésére sor került. Ezen túl az adatok jogosulatlan kezelője tipikusan a következő bűncselekményeket valósíthatja meg: jogosulatlan titkos információgyűjtés vagy adatszerzés bűntette (kifejezetten a titkos információgyűjtés szabályainak megsértése esetén valósul meg; Btk. 307. §), a tiltott adatszerzés bűncselekménye (ha pl. valaki magánemberként, magáncélból helyez el lehallgatókészüléket egy magánlakásban, magántitkot jogosulatlanul ismer meg; Btk. 422. §), az információs rendszer vagy adat megsértése (ha például a titkos megfigyelésre jogosult személy jogosultsága kereteit – így a célját, idejét stb. – túllépi és a megfigyelt információs rendszerben tovább bent marad; Btk. 423. §).

3.3. A megfigyelés anyagi jogi kellékei és feltételei. Farkas Ákos az új Be. rendelkezéseit értékelve kiemeli, hogy nem tudjuk, hol húzódik a gyanú határa.[8] Az új Be. szerint az információgyűjtésnek három szakasza lehetséges: az előkészítő eljárás, a felderítés, és a vizsgálat. Ennek megfelelően az egyes szakaszok által megkövetelt gyanú szintje is más-más: az előkészítő eljárásban az „egyszerű gyanút megelőző gyanú", a felderítésben az „egyszerű gyanú", a vizsgálat során pedig „alapos vagy megalapozott gyanú" szükséges. Az új büntetőeljárási kódex ezzel megteremti annak lehetőségét, hogy a nyomozó hatóság akár engedély nélkül, bármennyi ideig megfigyelhessen valakit, a büntetőeljárást megelőző „előkészítő eljárás" keretében.[9] Az előkészítő eljárás céljaként [új Be. 340. § (1) bek.] ugyanis annak megállapítását jelöli ki, hogy a bűncselekmény gyanúja fennáll-e. Jogértelmezések szerint a gyanú hiánya értelmezhetetlenné teszi mind a szükségesség, mind az arányosság követelményét; így Finszter Géza és Korinek László szerint *„a gyanú hiánya a bűnüldöző hatóságokat, de végső soron az igazságszolgáltatást is védtelenné teszi a hatalom önkényes alkalmazásával szemben, megszünteti annak ellenőrizhetőségét, hogy a bűnüldözést jogállamban kizárólag a büntetőjogi igény legitimálhatja"*[10]. Farkas Ákos és Róth Erika hasonló állásponton van: a hatóság előbb feltételezi, hogy ki lehet az elkövető, mint hogy tudná, bűncselekmény történt-e vagy sem. De az elkövető személye csak akkor határozható meg, ha nyilvánvaló, hogy bűncselekmény történt.[11] Az új Be. tehát logikai tautológiával teszi legitimmé az előkészítő eljárásban a megfigyelést bárki ellen, aki az elkövetőként szóba jöhető személlyel közvetlenül vagy közvetetten

[8] HANCZ Patrik: Nem vagyok híve, hogy kivették az ülnököket – Interjú Farkas Ákossal az új Be-ről. *Ars Boni,* 2017. szeptember 6. https://arsboni.hu/nem-vagyok-hive-hogy-kivettek-az-ulnokoket-interju-az-uj-rol/ (2018.06.15.)

[9] FARKAS– RÓTH: i.m. 321.

[10] FINSZTER Géza – KORINEK László: Az eltűnt gyanú nyomában. *Belügyi Szemle,* 2018/3. 121.

[11] FARKAS– RÓTH: i.m. 322.

kapcsolatot tart. Tovább menve, a rendőrségi törvény értelmében a rendészeti célú titkos információgyűjtés keretében (tehát a felderítésnek az előkészítő eljárást megelőző szakaszában) a büntetőeljárásról szóló törvényben meghatározottak szerint lehetséges leplezett eszközök alkalmazása [Rtv. 63.§ (4) bek.]. A rendészeti célú titkos információgyűjtéshez egy negyedik fajta, még az előkészítő eljárást megelőző, annál is absztraktabb gyanúfogalom kapcsolódik. A gyanúfogalom ilyen módon való kiterjesztése azonban sem a normavilágosság, sem az átláthatóság, sem a kiszámíthatóság követelményének nem tesz eleget.[12]

3.4. Az elektronikus kommunikáció *tartalmának* megismerése. Az új Be. értelmében nemcsak nyílt eljárásban, hanem az „információs rendszer titkos megfigyelése" keretében is beszerezhető az elektronikus adat, amely a büntetőeljárásban bizonyítékként felhasználható (új Be. XXXIII. Fejezet: Tárgyi bizonyítási eszköz, elektronikus adat). A lehallgatás tárgya tehát az „információs rendszer titkos megfigyelése" [új Be. 231. § a) pont], amely minden esetben bírói engedéllyel lehetséges.

Az ágazati törvények [Rtv. 69. § (1) bek. d)–e) pont; Nbtv. 56. § d)–e) pont] keretszabályként fogalmazzák meg a hírközlő hálózatban továbbított közlés tartalmának megismerhetőségét. Bármilyen típusú elektronikus kommunikáció lehallgatható. Az elektronikus hírközlési szolgáltató a rendészeti és nemzetbiztonsági célú titkos adatgyűjtés (lehallgatás) céljára köteles biztosítani az elektronikus hírközlő hálózatban továbbított küldemények, közlések, továbbá a szolgáltató által kezelt adatok titkos információgyűjtéssel, illetve titkos adatszerzéssel történő megismeréséhez szükséges eszközök és módszerek alkalmazási feltételeit [2003. évi C. törvény az elektronikus hírközlésről, a továbbiakban Eht., 92. § (4) bek.], valamint monitoring alrendszert köteles kiépíteni, amelyhez a műszaki specifikáció leírását a lehallgatás végrehajtója, a Nemzetbiztonsági Szakszolgálat adja meg [Eht. 92. § (5) bek.]. Az így megadott műszaki specifikáció bármiyen típusú adatra és bármilyen típusú szolgáltatásra, illetve bármilyen típusú kommunikációra vonatkozhat. Ami jelenleg még nem működik a gyakorlatban, az az ún. ötödik generációs számítástechnikai adatok lehallgatása.[13] Az ilyen típusú adatok lehallgatására szolgáló műszaki specifikáció kidolgozása még tart. Ameddig azt az NBSZ nem fejezi be, és nem utasítja a szolgáltatót az erre szolgáló monitoring alrendszer kiépítésére, addig az ilyen típusú adatokat jelenleg nem lehetséges lehallgatni.

Az Eht. 159/A. §-a meghatározza, hogy az elektronikus hírközlési szolgáltató a bűnüldözési, nemzetbiztonsági és honvédelmi célú adatmegőrzési kötelezettsége keretében mely adatokat köteles átadni. A szolgáltató a kommunikáció *tartalmi* adatainak átadására nem köteles, hiszen annak kezelésére sem jogosult [Eht. 157. §], így a kommunikáció tartalma csak jelenidejű lehallgatással, titkos információgyűjtés keretében valósulhat meg. A kommunikáció tartalmát a szolgáltató csak addig tárolhatja, ameddig arra – a szolgáltatás nyújtásához, illetve

[12] FINSZTER– KORINEK: i.m. 121.

[13] Ilyen például az optikai számítógép, aminek lényege az, hogy nem elektromos, hanem sokkal gyorsabb fényimpulzusok hordozzák az információt. Zajlik a kvantumszámítógép kutatása is.

a számlázáshoz – elengedhetetlenül szükség van [Eht. 157. § (2) bek.]. Specifikus esetek a telefonszolgáltatáshoz tartozó SMS- és hangpostafiók, valamint az e-mail-fiók, amelyekhez a szolgáltató tárhelyet biztosít. Ezekben az esetekben a szolgáltatás sajátosságaiból adódóan bizonyos ideig meg kell őrizni a kommunikáció tartalmát a szolgáltatás teljesítése érdekében. A kézbesített és megnyitott e-mailek tartalma nyílt nyomozás keretében, a nem kézbesített e-mailek tartalma titkos információgyűjtés keretében (lehallgatással), a kézbesített, de nem megnyitott e-mailek tartalma csak ügyész engedélyével ismerhető meg.

3.5. Online (azaz távolról történő) házkutatás megengedhetősége a büntetőeljárásban. A régi Be. (1998. évi XIX. tv.) meghatározása szerint a házkutatás a ház, lakás, egyéb helyiség, az azokhoz tartozó bekerített hely, vagy jármű átkutatása, továbbá az ott elhelyezett információs rendszer vagy ilyen rendszerben tárolt adatokat tartalmazó adathordozó átvizsgálása az eljárás eredményessége érdekében (régi Be. 149. §). Az 1998-as Be. hatálybalépése előtt a felsorolás nem tartalmazta az elektronikus adatokra vonatkozó kitételt, így vita folyt azzal kapcsolatban, hogy egy számítástechnikai rendszer vagy adathordozó átvizsgálása házkutatásnak minősül-e.[14]

A német szövetségi alkotmánybírósági határozata[15] (2009) kimondta az online házkutatás alkotmányellenességét és új alapjogként fogalmazta meg az információs rendszer bizalmasságához és integritásához való jogot. Megállapította, hogy ugyanazokat a garanciákat kell az online házkutatás esetén biztosítani, mint a titkos megfigyelés esetében, ami nem volt adott. Magyarországon sem a régi, sem az új Be. nem nevesíti külön az online házkutatás lehetőségét, de lehetőséget ad erre, mint bírói engedélyhez kötött titkos megfigyelésre. Erre olyan esetekben kerül sor, amikor az adatok vizsgálata később már nem lehetséges, illetve nem biztos, hogy az adatok később változatlan formában megismerhetők, pl. felhőszolgáltatásban tárolt adatok esetén.[16]

Az új Be. immár „kutatásként" hivatkozik erre a kényszerintézkedésre, amely jobban illeszkedik annak tartalmához, hiszen nemcsak ház, hanem jármű és információs rendszer is a tárgya lehet [új Be. 302. §]. A kutatás köre az új Be.-ben kibővül a régi Be.-hez képest, hiszen akkor is alkalmazható, ha elkobozható, illetve vagyonelkobzás alá eső dolog megtalálására, vagy információs rendszer, illetve adathordozó átvizsgálására vezet. Az ilyen eszközökön tárolt elektronikus adat bizonyítási eszköznek tekinthető.

Ami a nemzetbiztonsági szolgálatok által végzett titkos információgyűjtő tevékenységet illeti, már 2009-ben született adatvédelmi biztosi ajánlás az NBSZ által alkalmazott FinFisher kémprogram alkalmazásának problémáiról.[17] Az

[14] LACZI Beáta: A számítógépes környezetben elkövetett bűncselekmények nyomozásának és a nyomozás felügyeletének speciális kérdései. *Magyar Jog,* 2001/12. 726–738.

[15] BVerfG, 1 BvR 370/07

[16] DORNFELD László: A kibertérben elkövetett bűncselekményekkel összefüggésben alkalmazható kényszerintézkedések. *Belügyi Szemle,* 2018/2. 115–135.

[17] *A nemzetbiztonsági szolgálatok külső engedélyhez kötött titkos információgyűjtéséről szóló adatvédelmi biztosi ajánlás.* Adatvédelmi biztos, 2008. Ügyszám: 1813/T/2008-4. Elérhető:

adatvédelmi biztos nevesíti, hogy az akkor hatályos törvényben a célszemélyek körét pontatlanul (személyek körére való utalással) határozták meg, valamint a törvény nem tartalmazott kifejezett előírást a szükségtelen adatok törlésére. A miniszteri és a bírói engedélyezés elhatárolása sem volt egyértelmű.[18] Az Nbtv. az osztott engedélyezési rendszert ugyan nem küszöbölte ki (a jelenleg hatályos szabályozás szerint is a miniszter vagy a bíró engedélyezi a megfigyelést), de pontosította a szabályozást. Az adatvédelmi biztos ugyanakkor felrótta, hogy az akkori szabályozás szerint a megfigyeléshez (titkos információgyűjtéshez) külső engedélyt csak „a közcélú telefonvezetéken vagy az azt helyettesítő távközlési szolgáltatás útján továbbított közlemény" megfigyeléséhez kellett kérni, és nem volt egyértelmű, hogy a számítógépek távolról, hálózaton történő elérésére és átkutatására milyen szabályok alkalmazandók, továbbá hogy kell-e egyáltalán külső engedély ilyen esetben.[19] A szabályozás 2011. január 1-jével megváltozott és immár követelmény, hogy a nemzetbiztonsági szolgálatok csak külső engedély birtokában ismerhetik meg és használhatják fel a „számítástechnikai eszköz vagy rendszer útján továbbított, vagy azon tárolt adatokat" [Nbtv. 56. § e) pont].

Hazánkban a magánélet tiszteletben tartásához való alkotmányos alapjog és az állam büntetőjogi jogérvényesítéséhez fűződő joga összeütközését tárgyalva a német szövetségi alkotmánybíróság ún. *Online Durchsuchung*-ügyben hozott döntésére[20] szokás hivatkozni.[21] A hivatkozott ügyben büntetőeljárásban zárt kommunkációs hálózatok (információs-technikai, azaz IT-rendszerek) integritásához és bizalmasságához fűződő alapjogot deklarált a német szövetségi alkotmánybíróság, és ebből levezetve tiltotta meg a tartományi alkotmányvédelmi hatóság számára azt, hogy kémprogram (mint tipikus leplezett eszköz) segítségével ezen hálózatokban az online kommunikációt monitorozza és a program segítségével személyi számítógépek tartalmát is átvizsgálja. A büntetőügyben született, ún. „IT-határozat" az általános személyiségi jogból kiindulva vezette le az IT-rendszerek bizalmasságához és integritásához fűződő alapjogot (Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme). A német szövetségi alkotmánybíróság a védelmet a Grundgesetz 1., 2., és 10. (magánszféra védelmét kimondó) cikkeiből vezette le és értelmezésével az e-mailes kommunikáció számára is biztosította a bizalmasság védelmét. Sulyok Márton szerint *„Ezen alapjog, mint az IT-rendszerek bizalmasságát és integritását megalapozó jogátvétel egyik lehetséges útja hazánk, de más európai ország alapjogvédelmi keretrendszerét (pl. az erre tekintettel megalkotott kizárási szabályok tekintetében) és jogalkalmazási vagy alkotmányértelmezési gyakorlatát is finomíthatja az információs jogokkal és az*

http://abi.atlatszo.hu/index.php?menu=aktualis/ajanlasok&dok=1813_T_2008-4; JÓRI András: Az internetes házkutatásokról a FinFisher-ügy apropóján. *Átlátszó.hu,* 2014. 09. 13. Elérhető: https://atlatszo.hu/2014/09/13/jori-andras-az-internetes-hazkutatasokrol-a-finfisher-ugy-apropojan/ (2018.06.15.)

[18] Adatvédelmi biztos (2009): i.m.

[19] Uo.

[20] BVerfG, 1 BvR 370/07

[21] SULYOK Márton: A bizalmi kapcsolattartás bizonyítási védelme a magyar polgári eljárásban – alkotmányjogi szempontok. *Eljárásjogi Szemle,* 2017/2. 1–30.

elektronikus magánszférával összefüggésben".[22] A német IT-határozat egybecseng a magyar Alkotmánybíróság alaphatározataiban tett megállapításokkal[23], amelyek szerint *„a modern alkotmányos gyakorlat az általános személyiségi jogot – mint anyajogot – különféle aspektusain keresztül (pl. magánszférához való jog) nevezi meg, amely mindig hivatkozható, ha nincs az adott szegmens védelmére nevesített alapjog".*[24]

3.6. Az állampolgár értesítése a megfigyelés tényéről és a megfigyelés elleni jogorvoslat. Az érintettet a nemzetbiztonsági célú titkos információgyűjtés tényéről az engedélyező utólag, a megfigyelés befejeződésével *sem* tájékoztatja [Nbtv. 58. § (6) bek.]. Egyéb esetekben, a nyomozó hatóság és a rendőrség titkos információgyűjtése megszűnésekor az érintettet tájékoztatni kell. A büntetőeljárást megelőző, ún. előkészítő eljárás esetében azonban a megfigyelt személy nem tudja, hogy ellene megfigyelés folyik, ezért nincs neki lehetősége panaszra vagy kártalanításra. Ennek a jogsérelemnek az orvoslása akkor lehetséges, amikor nyílttá teszik az információgyűjtést, azaz amikor a bíróság előtt bizonyítékként felhasználják, akkor vitatható az elrendelés törvényessége, jogszerűsége, felhasználhatósága, az adat megszerzésének a jogszerűsége. Fontos, hogy az ügyvéd vagy jogi képviselő az utólag nyílttá tett minősített adathoz hozzáférhet. Ilyenkor is zárt tárgyalást kell tartani a minősített adat miatt, de a védő megismerheti és kérheti, hogy a bizonyítékok köréből zárják ki a szóban forgó adatot, például azon az alapon, hogy nem voltak meg a feltételei a titkos megfigyelésnek, hogy nem a jogszabályban előírt bűncselekmény esetén alkalmazták, vagy hogy nem készítették el határidőben a jelentést.

Ha azonban az előkészítő eljárás nem járt sikerrel, tehát az előzetes eljárásban gyűjtött információ nem vezetett büntetőeljárás megindítására, akkor a megfigyelt személy az előzetes eljárás lezárásával sem szerez tudomást arról, hogy megfigyelték és valaha is adatot gyűjtöttek róla.

3.7. A telekommunikációs szolgáltató titoktartási kötelezettsége. Az elektronikus hírközlési szolgáltatóknak adatmegőrzési és átadási kötelezettsége van az Eht., az Rtv., és az Nbtv. alapján. Tehát a szolgáltatót együttműködési kötelezettség terheli az e törvényekben meghatározott célból. Az elektronikus hírközlő hálózat üzemeltetője, illetve az elektronikus hírközlési szolgáltató a bíróság, ügyészség, nyomozó hatóság, az előkészítő eljárást folytató szerv, valamint a nemzetbiztonsági szolgálat kérelmére megőrzi az előfizetőivel kapcsolatos, a szolgáltatás nyújtásával összefüggésben előállított vagy kezelt adatokat [Eht. 159/A. § (1) bek.]. E kötelezettség törvénybe iktatásával a jogalkotó alapvetően az Európai Unió adatmegőrzési irányelve[25] végrehajthatóságának tett eleget. Ám annak ellenére, hogy az Európai Unió Bírósága érvénytelenné

[22] SULYOK: i.m. 14.
[23] 8/1990. (IV. 23.) AB határozat
[24] 17/2014. (V. 30.) AB határozat indokolása; idézi SULYOK: i.m. 15.
[25] Az Európai Parlament és a Tanács 2006/24/EK irányelve (2006. március 15.) a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtása, illetve a nyilvános hírközlő hálózatok szolgáltatása keretében előállított vagy feldolgozott adatok megőrzéséről és a 2002/58/EK irányelv módosításáról. (Európai Unió Hivatalos Lapja, L 105/54, 2006. 04. 13.)

nyilvánította az adatmegőrzési irányelvet, az annak alapján törvénybe iktatott magyar adatmegőrzési kötelezettségek[26] jelenleg is hatályban vannak és kötelezőek az elektronikus hírközlési szolgáltatókra nézve.

Az elektronikus hírközlési szolgáltatókat titoktartási kötelezettség terheli a titkos információgyűjtéshez nyújtott, törvényben meghatározott közreműködésük mivoltát illetően. Ezt két jogszabály határozza meg: az elektronikus hírközlési szolgáltatóknak a titkos információgyűjtésben való közreműködését előíró 180/2004. (V. 26.) Korm. rendelet és a 2009. évi CLV. törvény a minősített adat védelméről (a továbbiakban Mavtv). *„A titkos információgyűjtéssel összefüggő tevékenység végzésében, valamint a monitoring alrendszer, berendezés telepítésében, üzemeltetésében, rendszerfelügyeletében, javításában, karbantartásában az a személy vehet részt, aki az Nbtv.-ben meghatározott nemzetbiztonsági ellenőrzésen megfelelt és rendelkezik az elektronikus hírközlési szolgáltató vezető tisztségviselője által az NBSZ egyetértésével kiadott megbízással"* (180/2004. Korm. rendelet 13. §). A biztonsági feltételekről a Mavtv. rendelkezik: *„Elektronikus biztonsági intézkedéseket kell tenni az elektronikus rendszeren kezelt minősített adat és az elektronikus rendszer bizalmassága, sérthetetlensége és rendelkezésre állása érdekében"* [Mavtv. 10. § (7) bek.]. Az adathoz hozzáférő együttműködő személy „személyi biztonsági tanúsítványt" kap, amelyet a Nemzeti Biztonsági Felügyelet bocsát ki [Mavtv. 17. § (2) bek. a) pont].

4. Dilemmák és epilógus

Ha nemzetbiztonsági célú titkos felderítés során a megfigyelt személyről bűncselekményre utaló adatok merültek fel, azokat a régi Be. szerint csak komplikált módon lehetett a büntetőeljárásban felhasználhatóvá tenni. Ennek indoka, hogy azokat nem valamely büntetőeljárás alapjául szolgáló eljárásban szerezték be, és nem is bírói, hanem igazságügyi miniszteri engedéllyel. Egyes vélemények szerint a titkos felderítést ilyen esetekben is csak bírói engedély birtokában lenne jogszerű elrendelni.[27] Más hangok szerint azonban, ha a titkosszolgálat alkotmányvédelmi célból felderítést végez, azért büntetőbíró nem vállalhat felelősséget, ugyanis ilyenkor a titkosszolgálatok per definitionem bűncselekményt valósítanak meg. Ehhez pedig bíró nem adhat engedélyt, hiszen nem szolgál bűnüldözési érdeket, hanem a politikai felelősség körébe tartozik.

[26] Beiktatta a 2007. évi CLXXIV. törvény 13.§, hatályos 2008. III. 15-től. A szakaszt legutóbb a 2017. évi CXCVII. törvény 188. § g) pontja módosította.

[27] SZABÓ Máté Dániel – HIDVÉGI Fanny: Két ítélet és végrehajtásuk. Az Európai Bíróságnak az adatvédelmi biztosról és az adatmegőrzésről szóló ítéletei és azok utóélete Magyarországon. *Fundamentum,* 2014/4. 72-74.; A Társaság a Szabadságjogokért álláspontja a terrorizmus elleni fellépéssel összefüggő egyes törvények módosításáról szóló törvény tervezetéről. Társaság a Szabadságjogokért, 2016. https://tasz.hu/files/tasz/imce/a_tasz_allaspontja_a_terrorizmus_elleni_fellepessel_osszefuggo_egyes_torvenyek_modositasarol_szolo_torveny_tervezeterol.pdf; *Vélemény a Belügyminisztérium nemzetbiztonsági szolgálatokról szóló törvény és az információs jogi törvény módosításával kapcsolatos, BM/8652/2017. számú előterjesztéséről.* Társaság a Szabadságjogokért, 2016. https://tasz.hu/files/tasz/imce/2015/nbtv_velemeny.pdf (2018.06.15.)

Ezért a mindenkori kormánynak kell felelősséget vállalnia, tehát az igazságügyért felelős miniszternek kellene engedélyeznie.[28]

A büntetőeljárást érintő törvényekben (régi Be., új Be., valamint az Nbtv. szerint) a nemzetbiztonsági és a bűnüldözési hatáskörök továbbra is összecsúsznak, amennyiben a törvények kimondják, hogy az ügyész nemcsak bűnüldözési érdekből, hanem nemzetbiztonsági érdekből is köthet vádalkut.[29] Ennek akkor lehet jelentősége, ha például egy Magyarország elleni összehangolt kibertámadást kell megelőzni, kifürkészni, leleplezni, tehát egy politikai támadás van készülőben a magyar kormány érdekei ellen, akkor vádalku köthető és a kevésbé súlyos cselekményt – pl. online pedofília, online szerencsejáték tiltott szervezése – el lehet engedni, hogy a nemzetbiztonsági szempontok érvényesülhessenek.

Az új büntetőeljárási törvényben nem valósul meg teljes mértékben a titkos felderítés szabályrendszerének jogállamiság és hatékonyság követelményét egyaránt érvényre juttató megújítása. Ha a nyomozás részeként rendelik el a titkos információgyűjtést, akkor a nyomozás elrendeléséhez az egyszerű gyanú elegendő. A nyomozás elrendelése előtt még ennél is kevesebb, azaz absztrakt veszély szükséges a titkos információgyűjtéshez. Az egyetlen elhatároló ismérv, hogy kutató-szűrő jellegű, tehát meghatározott cél nélküli megfigyelés a nyomozás során már nem rendelhető el. Az új Be. *„[e] tekintetben [...] nemhogy előrelépésként, hanem egyenesen visszalépésként értékelhető. Ez még akkor is igaz, ha a legsúlyosabb jogkorlátozással járó, bírói engedélyhez kötött eszközöket csak a szervezett bűnözéssel összefüggő információk beszerzése érdekében lehet majd folytatni"* – fejti ki Bárándy és Enyedi.[30]

Annak ellenére, hogy az Európai Unió adatmegőrzési irányelvét hatályon kívül helyezték, a magyar jogszabályok még mindig az irányelvben foglaltaknak megfelelően szabályozzák az adatmegőrzést, ami tömeges és készletező jellegű adatgyűjtésnek (legalábbis ami a forgalmi adatokat illeti) felel meg.

[28] A szerző saját interjúja a Transparency International munkatársaival.

[29] ZSÍROS Bettina: Valóságos-e, ami igazságos? Gondolatok a perbeli egyezségkötés új Be.-ben szabályozott intézményéről. *Büntetőjogi Szemle,* 2018/1. 93–96.

[30] BÁRÁNDY Gergely – ENYEDI Krisztián: Leplezett eszközök és titkos információgyűjtés, avagy az új büntetőeljárási törvény margójára. *Büntetőjogi Szemle,* 2018/1. 104.