



BELÜGYMINISZTERIUM

DR. PINTÉR SÁNDOR
miniszter

ALKOTMÁNYBÍRÓSÁG	
Ügyszám: <i>IV/1365-16/2016</i>	
Érkezett: 2022 JAN 17.	
Réldány: <i>1</i>	Kezelőiroda:
Melléklet: <i>1</i>	<i>4</i> db

Dr. Sulyok Tamás úrnak,
Elnök

Alkotmánybíróság

Budapest
Donáti u. 35-45.
1015

Tárgy: Állásfoglalás megküldése a
IV/1365/2026. számú alkotmányjogi panasz
tárgyában

Iktatószám: BM/503-4/2021.

Hivatkozási szám: IV/1365-16/2016.

Tisztelt Elnök Úr!

Az Alkotmánybíróságon IV/1365/2016. számon folyamatban lévő, az elektronikus hírközlésről szóló 2003. évi C. törvény 159/A. §-a elleni alkotmányjogi panasszal kapcsolatos álláspontomról a mellékletben foglaltak szerint tájékoztatom.

Budapest, 2022. január „*13.*”

Üdvözlettel:


Dr. Pintér Sándor


Belügyminisztérium
Miniszter
*

MELLÉKLET

Az Alkotmánybírósághoz a IV/1365/2016. számon benyújtott alkotmányjogi panasszal kapcsolatos belügyminiszteri álláspont:

ALKOTMÁNYBÍRÓSÁG	
Ügyszám:	IV/1365-24/2016
Álláspont:	2022 JAN 17.
Példány:	1
Melléklet:	db
Kezelőiroda:	2

1. Az indítvány tartalma

Az indítványban a panaszos és képviselője (a továbbiakban: panaszos) **az elektronikus hírközlésről szóló 2003. évi C. törvény** (a továbbiakban: Eht.) **159/A. §-a alaptörvényellenességének megállapítását kezdeményezte, figyelemmel arra, hogy álláspontja szerint az ellentétes Magyarország Alaptörvényének** (a továbbiakban: Alaptörvény) – az indítvány benyújtásakor hatályos – **VI. cikk (1) és (2) bekezdésével**, továbbá kérte e vitatott rendelkezésnek az eljárásra okot adó ügyben történő alkalmazásának tilalmát.

Az Eht. 159/A. §-a a bűnüldözési, nemzetbiztonsági és honvédelmi célú adatmegőrzési kötelezettségre vonatkozó szabályokat rögzíti. A rendelkezés meghatározza azt elektronikus hírközlési szolgáltatás nyújtásával összefüggésben a szolgáltató által előállított vagy kezelt adatokat, amelyeket az elektronikus hírközlő hálózat üzemeltetője, illetve az elektronikus hírközlési szolgáltatás szolgáltatója – a törvényben meghatározott szervek kérelmére történő adatszolgáltatás biztosíthatósága érdekében – köteles megőrizni. (Az Eht. hivatkozott rendelkezése az indítvány benyújtása óta a megőrzendő adatok tekintetében nem módosult, azonban bekerült az előkészítő eljárást folytató szerv, mint adatkérésre jogosult.)

Az Alaptörvény hivatkozott VI. cikk (1) és (2) bekezdésének az indítvány benyújtásakor hatályos szövege meghatározta, hogy „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 Alaptörvény VI. cikke és annak számozása az indítvány benyújtásának időpontja óta módosult, azonban a hivatkozott tartalom ma is megtalálható benne.)

A panaszos kiemeli, hogy a személyes adatokhoz való jog védelme alapjog, amely ugyan korlátozható, de a korlátozásnak alkalmasnak, szükségesnek és arányosnak kell lennie a kitűzött jogszerű célok elérése tekintetében és nem haladhatja meg az e célok eléréséhez szükséges mértéket. Ezen követelmények azonban álláspontja szerint nem valósulnak meg maradéktalanul, ebből pedig az következik, hogy a támadott rendelkezéssel megvalósuló alapjog-korlátozás esetében nem biztosított, hogy a korlátozás ténylegesen a feltétlenül szükséges mértékre korlátozódjon, illetve arányos legyen.

2. Az indítvánnyal kapcsolatos álláspont

Az Alaptörvény I. cikk (3) bekezdése az alapjogok korlátozása tekintetében rögzíti, hogy **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.** Ennek megfelelően a magyar alkotmánybírói gyakorlat a szükségesség, alkalmasság és arányosság tesztjét alkalmazza az alapvető jogok korlátozhatósága tekintetében.

A személyes adatok kezelésére vonatkozó alapvető rendelkezéseket az *információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény* (a továbbiakban: Infotv.) rögzíti. Az Infotv. 4. § (1) bekezdése értelmében: „*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.*” Az Infotv. 5. § (1) bekezdése a) pontja pedig akként rendelkezik, hogy: „*Személyes adat akkor kezelhető, ha azt törvény vagy - törvény felhatalmazása alapján, az abban meghatározott körben, különleges adatnak vagy bűnügyi személyes adatnak nem minősülő adat esetén - helyi önkormányzat rendelete közérdeken alapuló célból elrendeli.*”

Fentiekre figyelemmel a **személyes adatokhoz való jog korlátozható, törvény elrendelheti a személyes adatok kötelező szolgáltatását**, illetve előírhatja a felhasználás módját, célját is, ezekben az esetekben nem szükséges az érintettek hozzájárulása. E logikát követi az Eht. 159/A. §-a, amikor rögzíti az elektronikus hírközlési szolgáltatás előfizető, illetve felhasználó általi igénybevételével kapcsolatos adatok megőrzésére vonatkozó kötelezettséget.

Az Infotv. 14. §-a határozza meg az érintettet megillető jogosultságokat azzal, hogy azok a 16. § (3) bekezdés a)-f) pontjaiban meghatározott valamely érdek, így különösen bűnüldözési, nemzetbiztonsági vagy honvédelmi érdekből korlátozhatók.

Az Eht. 159/A. §-a alapján az elektronikus hírközlő hálózat üzemeltetője, illetve az elektronikus hírközlési szolgáltatás szolgáltatója bűnüldözési, nemzetbiztonsági és honvédelmi célból köteles megőrizni az Eht.-ban meghatározott adatokat. Az Eht.-ban alkalmazott szabályozási megoldás tehát az Infotv. szerinti, jogkorlátozást lehetővé tévő okokkal megegyezik.

Tekintettel arra, hogy a jogalkotó meghatározta a kötelezően megőrzendő adatok pontos megőrzési idejét, valamint azok felhasználását megfelelő garanciákhoz köti, így kellő egyensúlyt teremt az érintett alapvető jogok és társadalmi érdekek érvényesítése között.

Az elektronikus hírközlési szolgáltató bűnüldözési célú adatmegőrzési kötelezettségét a rendőrség vonatkozásában a rendőrségnek a *Rendőrségről szóló 1994. évi XXXIV. törvényben* (a továbbiakban: Rtv.) szerinti feladatai ellátásának biztosítása céljából az Eht. 159/A. §-a szabályozza. A megőrzött adatokhoz való hozzáférést a *büntetőeljárásról szóló 2017. évi XC. törvény* (a továbbiakban: Be.) 261. § (1) bekezdése biztosítja, amelynek értelmében a büntetőeljárások során a bíróság, az ügyészség és a nyomozó hatóság, illetve – törvényben meghatározott esetben – az előkészítő eljárást folytató szerv bármely szervtől, jogi személytől vagy jogi személyiséggel nem rendelkező szervezettől adatszolgáltatást kérhet. A fenti adatok bűnüldözési célú kezelésével összefüggésben további garanciális jellegű szabályokat rögzít a bűnüldözési célú adatkezelés szabályainak meghatározásával az Rtv. 90–91/I. §-a.

A nemzetbiztonsági szolgálatok a *nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvényben* (a továbbiakban: Nbtv.) rögzített feladataik teljesítése érdekében vannak felhatalmazva titkos információgyűjtésre, amelynek keretében jogosultak hírközlési rendszerekből és egyéb adattároló eszközökből információk gyűjtésére. Az Nbtv.-ben meghatározott nemzetbiztonsági érdek fogalmköre, illetve a nemzetbiztonsági szolgálatok feladatai törvényben rögzített objektív kritériumrendszernek tekinthetők: az Nbtv. 31. § (3) bekezdése szerint a nemzetbiztonsági szolgálatok a feladataik ellátása során a személyes szabadsághoz, a magánlakás, a magántitok és a levéltitok sérthetlenségéhez, a személyes adatok védelméhez, a közérdekű adatok nyilvánosságához, valamint a birtokvédelemhez fűződő jogokat e törvényben foglaltak szerint korlátozhatják.

A **szükségesség** követelményét illetően elmondható, hogy az alapjog korlátozásának oka a közösségek, más állampolgárok élethez, testi épséghez való joga (pl. egy tervezett támadás megakadályozása esetén), amelynek védelme például ezen adatok rendelkezésre állásával, feldolgozásával, az azokból történő információkinyeréssel megvalósítható. Figyelemmel arra, hogy az elektronikus hírközlési szolgáltatók általános adatmegőrzése olyan adatokat tesz elérhetővé, amelyek máshol nem szerezhetők be, mással nem helyettesíthetők, ezért nélkülözhetetlen értéket jelentenek mind a nemzetbiztonsági szolgálatok, mind a rendőrség munkájában.

Az Eht. 159/A. §-ában foglalt rendelkezések alkalmasak a meghatározott cél elérésére, a hivatkozott rendelkezés alapján biztosított adatkezelés alkalmas a bűnüldözéshez és a nemzetbiztonság védelméhez történő hatékonyan hozzájárulásra, hiszen ezen adatok kezelésével jutnak hozzá az arra jogosult szervek olyan információkhoz, amelyek hatékony és eredményes feladatellátásukhoz feltétlenül szükségesek.

Az alkotmányjogi gyakorlat – és a 30/1992. (V. 26.) AB határozatban foglaltak – szerint az **arányosság** tekintetében korlátozásra csak akkor és annyiban kerülhet sor, ha az ténylegesen az általános érdekű célkitűzéseket vagy mások jogainak és szabadságának védelmét szolgálja. Az arányosság követelménye megköveteli, hogy az elérni kívánt cél fontossága és az ennek érdekében okozott alapjogsérelem súlya összhangban legyen egymással. **Álláspontom szerint ezen feltételek megvalósulnak, hiszen az elérendő cél az olyan súlyos bűncselekmények megelőzése, felderítése, szankcionálása, amelyek elkövetése esetén mások jogai sérülhetnének, így az egyén személyes adatok védelméhez való joga áll szemben a közösségek jogával, a rendvédelmi szervek megfelelő feladatellátásának érdekeivel.**

Kiemelendő, hogy az **Alaptörvény 46. cikke** (A rendőrség és a nemzetbiztonsági szolgálatok) meghatározza, hogy **a rendőrség alapvető feladata a bűncselekmények megakadályozása, felderítése, a közbiztonság, a közrend és az államhatár rendjének védelme.**

A rendőrség és a nemzetbiztonsági szolgálatok feladat- és hatáskörére figyelemmel megállapítható, hogy az Eht. 159/A. §-ában meghatározott adatok nagyban hozzájárulnak a felderítési, megelőzési és elhárítási feladatainak megfelelő végrehajtásához. A megelőzés szempontjából kiemelt jelentőségű az esetleges elkövető személyes adatainak, mobiltelefonja cellainformációinak, tartózkodási helyének és mozgásának ismerete, az interneten, illetve a telefonon folytatott tevékenysége, valamint a vele kapcsolatban álló további személyek adatainak megismerése, hiszen sok esetben az elkövető beazonosítását, megfigyelését, mozgásának feltérképezését csak így lehet végrehajtani. Ezzel kapcsolatosan kiemelendő, hogy ezen adatok feltétlenül szükségesek, azok nem helyettesíthetők, nem pótolhatók, más forrásból nem beszerezhetők, ha azok a személyiségi jogok védelme érdekében idő előtt törésre kerülnek, nem tudják segíteni a hatóságok további (bűnmegelőzési, felderítési, nyomozati, életvédelmi, stb.) feladatellátását.

Fentiekre tekintettel az Eht. 159/A. §-ának hatályon kívül helyezése veszélyeztetné a rendőrség és a nemzetbiztonsági szolgálatok alapvető feladatainak ellátását, hiszen nem állnának rendelkezésre az ahhoz feltétlenül szükséges adatok. Erre figyelemmel álláspontom szerint a személyes adatok védelméhez fűződő alapjog-korlátozás szükségessége fennáll.

Az Nbtv. 53. § (2) bekezdése értelmében a nemzetbiztonsági szolgálatok a titkos információgyűjtés speciális eszközeit és módszereit csak akkor használhatják, ha az Nbtv.-ben

meghatározott feladatok ellátásához szükséges adatok más módon nem szerezhetők meg, amely szabályozás is megjeleníti az **arányosság követelményét**.

Megítélésem szerint az Eht. szerinti adatmegőrzési kötelezettség nem valósítja meg a személyes adatok védelmének lényeges és súlyos korlátozását, hanem csupán egy kockázatot jelent. Maga a jogsérelem akkor következik be, amikor ezen adatokat valaki megismeri. Nagy mennyiségű adat rögzítésénél valóban jelentős a jogsérelem kockázata, ezt a kockázatot azonban nem elsősorban a kevesebb adat rögzítésével vagy annak mellőzésével lehet csökkenteni. A visszaélést csakis az adatok biztonságos tárolását lehetővé tevő és a jogosulatlan hozzáférést megakadályozó megfelelő műszaki, szervezeti, biztonsági-védelmi intézkedések képesek kizárni.

Az adatmegőréssel kapcsolatban fontos hangsúlyozni továbbá, hogy az adatok rögzítésének pillanatában csak egy általános cél határozható meg: a biztonságra súlyos veszélyt jelentő cselekmények megelőzése, elhárítása és felderítése. A digitális társadalomban a hírközlési adatok megőrzésének és utólagos megismerhetőségének döntő jelentősége van, amely nem pótolható a fenyegetés, illetve gyanú azonosításának időpontjától kezdődő adatgyűjtéssel. Ha az általános adatmegőrzési kötelezettséget mint olyat minden további vizsgálat nélkül automatikusan jogellenesnek kellene tekinteni, a nemzetbiztonsági és bűnüldöző szervek munkájának eredményessége, és ennek következtében a biztonsághoz való jog komoly csorbát szenvedne. E megközelítés elfogadása valamennyi informatikai rendszernél alkalmazott eseménynaplózás gyakorlatát is ellehetetlenítené, hiszen a naplózott adat felhasználására, megszerzésére itt is csak utólag kerül sor; a rögzítés pillanatában nem bizonyos, hogy az adott adatra a későbbiekben ténylegesen szükség lesz. A helyes megközelítés az adat megismerhetőségének megfelelő garanciákkal való alátámasztása.

Az általános, minden szolgáltatóra, felhasználóra és hírközlési eszközre kiterjedő, megelőző jellegű adatmegőrzés ésszerűen nem korlátozható, hiszen itt az eszköz természetéből fakadóan abban a helyzetben vagyunk, hogy még nem került sor a bűncselekmény elkövetésére, vagy a hatóságoknak még nincs tudomása erről. Később, ha már egy adott cselekménnyel kapcsolatban a nemzetbiztonsági vagy bűnüldöző hatóságok beazonosítottak valamely személyt, személyeket, földrajzi helyszínt, akkor a hírközlési adatok szolgáltató általi gyűjtésén túl más eszközök használata (így a közlések tartalmára is kiterjedő nyomozás) válhat indokolttá.

A hozzáférés az a pillanat, amikor az adatokat valaki ténylegesen megismeri, így, míg az adat pusztán rögzítése csupán a visszaélés kockázatát hordozza, a hozzáférés pillanatában valósulhat meg ténylegesen a személyes adatokkal való visszaélés. Ez az a pont, ahol a megfelelő garanciák, a célhoz kötöttség, a szükségesség, arányosság, jogorvoslat lehetősége érvényesíthető és érvényesítendő.

A hírközlési adatok általános megőrzésének nincsen alternatívája a közrend és a közbiztonság fenntartásának, mint a rendőrség Alaptörvényben meghatározott közfeladatának érvényesítése körében. Az uniós jog helyes értelmezése nem vezethet olyan eredményre, amely a tagállamokat megfosztaná attól a lehetőségtől, hogy – megfelelő garanciális szabályok mellett – általános kötelezettségként előírják az elektronikus hírközlési szolgáltatók számára az e szolgáltatások nyújtása során keletkezett forgalmi és helymeghatározó adatok megőrzését, és ezáltal lehetővé tegyék az ezen adatokhoz nemzetbiztonsági, bűnüldözési és más hasonlóan kiemelt közérdekű célból való későbbi hozzáférést.

Minél kevesebb adat áll a hatóságok rendelkezésére, annál kisebb az esély, hogy érdemi döntésüket valóságghú tényállásra alapíthatják. Mind az elkövetők, mind az áldozatok szempontjából garanciális követelmény tehát, hogy az eljáró hatóságok megállapításait a lehető

legteljesebb mértékben felderített történeti tényállásra alapítsák. Megteelő nyomok és bizonyítékok hiányában az állampolgárok biztonságához és a tisztességes eljáráshoz való joga is sérül: a felderítetlen tényállás – amellet, hogy megghiúsítja az állam büntetőigényének érvényesítését – a terheltre és a sértetre nézve is hátrányos következményekkel jár. A magánélethez és a személyes adatok védelméhez való jog nem értékelhető a személyek biztonságához és a tisztességes eljáráshoz való jog, továbbá a közbiztonsághoz fűződő általános érdekű célkitűzések rovására.

A panaszban felhozott érvek nem az Eht. 159/A. § (1) bekezdésében előírt adatmegőrzési kötelezettséggel kapcsolatosak, hanem a megőrzött adatokhoz való későbbi hozzáférés lehetőségének alkotmányosságát vitatják. A hozzáférés lehetőségének szabályait nem az Eht. 159/A. §-a tartalmazza, hanem a különböző hatóságok eljárásaira irányadó jogszabályok (pl. Be., Nbtv.) Mindezek miatt a panaszban feltételezett alapjogsérelmek bekövetkezésének lehetősége nem az Eht. 159/A. §-ával áll összefüggésben, hanem a hivatkozott eljárási szabályokkal. A személyes adatok védelméhez fűződő alapjog tényleges sérelme akkor következhetne be, ha a megőrzött adatokhoz szükségtelenül és aránytalanul széles hozzáférési jogosultságot biztosítanának az eljárási jogszabályok (Be., Nbtv.) Az eljárási szabályok vizsgálatát azonban a panaszos sem az alapul fekvő polgári perben, sem az alkotmányjogi panaszban nem kezdeményezte, ezért azok alkotmányossága felől a IV/1365/2016. számú eljárásában nem lehet döntést hozni.

Mindezek alapján álláspontom szerint az Eht., valamint az adatmegismerést lehetővé tévő törvényi szabályozás mind a megőrzés, mind pedig a hozzáférés tekintetében megfelelő garanciákat tartalmaz, különös tekintettel arra, hogy a hozzáférés kérésére utólagosan, tehát a cselekménye elkövetését, vagy gyanújának felmerülését követően, és konkrét esetben kerülhet sor. A hozzáférésre vonatkozó előírások megfelelően biztosítják az intézkedés szükségességét és arányosságát, valamint a személyes adatok megfelelő, hatékony védelmét.

3. A támadott adatmegőrzési szabály indokoltsága

Álláspontom szerint az Eht. 159/A. §-ában szabályozott általános adatmegőrzés szabályozása büntetőjogi szempontból elengedhetetlen, alternatíva nélküli eszköz a hatékony bűnüldözés szempontjából. Az adatmegőrzés számtalan bűncselekmény, illetve bűncselekmény-típus esetében gyakorlatilag az egyetlen eszköz az eljáró szervek kezében, amely egyáltalán reális lehetőséget nyújt számukra, hogy az adott bűncselekmény elkövetőjét felderítsék, a vád megalapozottságát alátámasszák. Ilyen módon az adatmegőrzés sok esetben az egyedüli hatékony eszköz az állam számára, hogy az adott bűncselekmények sértettjeinek alapvető jogait sértő cselekmények esetén fellépjen. Az Alaptörvény 46. cikkében a rendőrség feladataként is rögzített, a bűncselekmények megelőzésére, kivizsgálására, felderítésére és üldözésére irányuló állami feladat ellátása, illetve a másik oldalról a sértett személyek változatos alapvető jogainak védelméhez kapcsolódó intézményvédelmi kötelezettség megfelelő indokot képeznek a személyes adatok védelméhez fűződő alapvető jog korlátozásához. A hatályos szabályozás továbbá megfelelő garanciákat tartalmaz, ezért álláspontom szerint a személyes adatok védelméhez fűződő jog és az információs önrendelkezési jog szükséges és arányos korlátozásának tekinthető az általános adatmegőrzés előírása.

3.1. Az adatgyűjtéssel, megőrzéssel kapcsolatban elvi szempontból mindenekelőtt azt fontos hangsúlyozni, hogy az adatok rögzítésének pillanatában csak egy általános cél határozható meg: a biztonságra súlyos veszélyt jelentő cselekmények megelőzése, elhárítása és felderítése. A digitális társadalomban a metaadatok megőrzésének és utólagos megismerhetőségének döntő

jelentősége van, amely nem pótolható a fenyegetés, illetve gyanú azonosításának időpontjától kezdődő ex post adatgyűjtéssel. Ha az általános adatmegőrzési kötelezettség, mint olyan meg nem engedettnek minősülne, a nemzetbiztonsági és bűnüldöző szervek munkájának eredményessége, és ennek következtében a biztonsághoz való jog komoly csorbát szenvedne. Álláspontom szerint a metaadatok általános megőrzésének nincsen alternatívája a közrend fenntartására irányuló államcél érvényesítése, illetve a sértettek alapvető jogainak védelméhez kapcsolódó intézményvédelmi kötelezettség teljesítése körében. Emellett megfelelő garanciákkal biztosítható mind a megőrzés jogszerűsége, mind a hozzáférés célhoz kötöttsége.

A megőrzés körében törvényszerűen más típusú garanciák lehetségesek, mint a hozzáférés esetében. Az általános, minden szolgáltatóra, felhasználóra és hírközlési eszközre kiterjedő, megelőző jellegű adatmegőrzés ésszerűen nem korlátozható, hiszen itt az eszköz természetéből fakadóan ex ante helyzetben vagyunk: még nem került sor a bűncselekmény elkövetésére, vagy a hatóságoknak még nincs tudomása erről. Később, ha már egy adott cselekménnyel kapcsolatban a nemzetbiztonsági vagy bűnüldöző hatóságok beazonosítottak valamely személyt, személyeket, földrajzi helyszínt, akkor a metaadatok szolgáltató általi gyűjtésén túl más eszközök használata (így a közlések tartalmára is kiterjedő titkos információgyűjtés vagy leplezett eszközök alkalmazása) válhat indokolttá. A hatékony bűnüldözéshez fűződő igények alapján az általános adatmegőrzés nem mellőzhető, ugyanakkor a személyes adatok megfelelő védelme érdekében olyan garanciákat kell biztosítani, amely megfelelő műszaki, szervezeti intézkedések révén biztonságossá teszik az adatok tárolását, megakadályozzák az azokhoz való jogosulatlan hozzáférést, és meghatározott idő elteltével kötelezően előírják ezek törlését. A hatályos szabályozás álláspontom e garanciális rendelkezéseket tartalmazza.

Az adatmegőrzés körében előírt garanciákat kiegészítik és teljessé teszik a hozzáférés tekintetében előírt korlátozások és garanciák. A hozzáférés kérésére ex post, tehát a cselekmény elkövetését vagy gyanújának felmerülését követően, és konkrét esetben kerülhet sor. Az adatmegőrzés és az ahhoz való hozzáférés garanciái együtt biztosítják a személyes adatok megfelelő, hatékony védelmét, és együtt vizsgálandók az intézkedés szükségessége és arányossága megítélése során.

Bár az indítvány kifejezetten az adatmegőrzés előírását támadja, a megőrzött adatokhoz való hozzáférés szempontjából kifejezetten büntetőeljárás szempontból fontos felhívni a figyelmet arra, hogy a Be. 261. § (1) bekezdése értelmében a büntetőeljárás során a bíróság, az ügyészség és a nyomozó hatóság, illetve – törvényben meghatározott esetben – az előkészítő eljárást folytató szerv bármely szervtől, jogi személytől vagy jogi személyiséggel nem rendelkező szervezettől adatszolgáltatást kérhet. Az elektronikus hírközlési szolgáltatók esetében – igazodva a személyes adatok védelmének egyre szigorodó szabályaihoz – a Be. a korábbihoz képest szigorúbb szabályozást vezetett be: a 262. § (1) bekezdés c) pontja értelmében a nyomozó hatóság kizárólag a büntetőeljárást felügyelő, illetve az a fölött törvényességi felügyeletet gyakorló ügyészség engedélyével kérhet adatszolgáltatást az elektronikus hírközlési szolgáltatótól. A Be. 262. § (3) bekezdése továbbá lehetőséget ad arra, hogy késedelmet nem tűrő esetben ügyészi engedély nélkül is beszerezze a nyomozó hatóság a szükséges adatokat, azonban ebben az esetben haladéktalanul intézkedni kell az ügyészi engedély utólagos beszerzéséről. Az említett ügyészi engedély hiányában a beszerzett adat bizonyítékként az eljárásban nem használható fel, az adatot törölni kell. Ezen szabály garantálja, hogy a megfelelő engedély hiányában megszerzett, azaz illegitim forrásból származó adat akkor se kerülhessen egy eljárásban felhasználásra, ha az egyébként az alapügy felderítését szolgálná, ugyanis egy jogsértésből származó eszköz nem szolgálhat eszközüül még egy másik jogsértés feltárására sem.

3.2. Az alkotmányos büntetőjogi követelményeknek megfelelően működő büntető igazságszolgáltatás, illetve a tisztességes eljáráshoz való jog érvényesülése szempontjából is kiemelkedően fontos szempont, hogy minél kevesebb adat áll a hatóságok rendelkezésére, annál kisebb az esély, hogy érdemi döntésüket valóság-hű tényállásra alapíthatják. Mind az elkövetők, mind az áldozatok szempontjából garanciális követelmény tehát, hogy az eljáró hatóságok megállapításaikat a lehető legteljesebb mértékben felderített történeti tényállásra alapítsák. Megfelelő nyomok és bizonyítékok hiányában az állampolgárok biztonságához és a tisztességes eljáráshoz való joga is sérül: a sikertelen büntetőeljárás – amellett, hogy megghiúsítja az állam büntetőigényének érvényesítését – a sértettre, míg a mentő körülményeket megalapozó információkhoz való hozzáférés kizárása a terheltre nézve járhat hátrányos következményekkel, és ezáltal közvetve alapvető jogok, illetve alapvető jogokhoz kapcsolódó állami intézményvédelmi kötelezettségek sérelméhez vezet. A magánélethez és a személyes adatok védelméhez való jog nem értékelhető a személyek biztonságához és a tisztességes eljáráshoz való jog, továbbá a közbiztonsághoz fűződő célkitűzések rovására.

Mind a személyi biztonságához való jog, mind a tisztességes eljáráshoz való jog, mind pedig közbiztonsági cél biztosítása vonatkozásában megállapítható, hogy a metakommunikációs adatok általános megőrzési kötelezettsége előírásának nincsen hatékony alternatívája. Az elkövetővel szemben mindenképpen érvényesülnie kell az állam büntető igényének és az áldozatok szempontjából is szükséges a bűncselekményekkel megsértett egyensúly helyreállítása.

3.3. A tárgybeli ügyel kapcsolatban mindenképpen figyelembe veendő az Emberi Jogok Európai Bíróságának (a továbbiakban: EJEB) az alapvető jogokkal megegyező, az emberi jogok és alapvető szabadságok védelméről szóló, Rómában 1950. november 4-én kelt egyezmény (a továbbiakban: Egyezmény) 3. és 8. cikkében rögzített jogokkal [amelyek megegyeznek a Charta 4. cikkében (kínzás tilalma) és 7. cikkében (a magán- és a családi élet tiszteletben tartása) foglalt alapvető jogokkal] összefüggésben kialakított értelmezését tükröző esetjoga.

Az EJEB-nek ugyanis egyebek mellett az Egyezmény 3. és 8. cikkében rögzített jogokkal kapcsolatban kiterjedt a gyakorlata abban a tekintetben, hogy ezen jogok nem pusztán az államnak e jogok megsértésétől való tartózkodását követelik meg, hanem ahhoz pozitív, a jogok érvényesülését és védelmét biztosító kötelezettségek is kapcsolódnak. E körben pedig az EJEB számos ügyben állapította meg, hogy ezen kötelezettségek közé adott esetben az ezen jogokat megsértő cselekmények miatt folytatott hatékony büntetőeljárás lefolytatása is beletartozik. A bíróság különösen olyan esetekben tartotta kiemelten fontosnak e körben az eljárás hatékonyságának a vizsgálatát, ha a sérelmet szenvedett fél sérülékeny csoportba tartozó volt, így különösen ha kiskorú volt, szexuális cselekmény elszennedője vagy családon belüli erőszak áldozata¹. Ezen ügyekben az EJEB megállapította, hogy a tagállamokat az a kötelezettség terheli, hogy a gyakorlatban is működő olyan jogi szabályozást alakítsanak ki, amely a mások részéről tanúsított erőszakos magatartásokkal szemben érdemi védelmet nyújt. A különösen súlyos esetekben, mint például a gyermekek elleni szexuális erőszak, amikor a magánszféra lényegi tartalma és alapvető értékei sérülnek, a védelemnek ki kell terjednie a hatékony elrettentést megvalósító büntetőjogi szabályozásra is. Ebből kifolyólag az EJEB több ügyben is megállapította, hogy a tagállamok nem alakítottak ki hatékony büntetőjogi szabályozást vagy a konkrét esetben a lefolytatott büntetőeljárás nem volt hatékony.²

¹ Lásd például EJEB, 2012. március 20., C.A.S. AND C.S. v. Románia, ECLI:CE:ECHR:2012:0320JUD002669205; EJEB, 2009. június 6., OPUZ v. Törökország, ECLI:CE:ECHR:2009:0609JUD003340102; EJEB, 2013. november 12., SÖDERMAN v. Svédország, ECLI:CE:ECHR:2013:1112JUD000578608

² Lásd ennek összefoglalását: EJEB, 2013. november 12., SÖDERMAN v. Svédország, ECLI:CE:ECHR:2013:1112JUD000578608 78-85. §

Alláspontom szerint a fentiek alapján különösen fontos kérdést vet fel az EJEB, 2008. december 2., *K. U. kontra Finnország* ügyben hozott ítélete.

Érdeemes az ügy részleteit is kifejteni, mert így válnak igazán hangsúlyossá az abból fakadó kérdések. Eszerint Finnországban egy 12 éves kiskorú személyes adatait, elérhetőségeit és ezen keresztül a fényképét is felhasználva egy ismeretlen személy elhelyezett egy hamisított hirdetést egy párkereső honlapon, amely szerint a kiskorú azonos nemű társat keres párkapcsolati céllal. Az ezt követően indult büntetőeljárás során kiderült, hogy a finn jog alapján a szolgáltató nem volt kötelezhető arra, hogy ilyen jellegű ügyben a hirdetést feladó személy IP címét kiadja és így a kiskorúval szemben elkövetett bűncselekmény elkövetője nem volt azonosítható.

Az EJEB az ügy megítélése során eldöntendő kérdésként éppen a telekommunikációs metaadatok megőrzésével és hozzáférhetőségével kapcsolatos kérdéseket azonosította. Ennek során figyelembe vette az ezzel a kérdéssel kapcsolatban az Európa Tanács, az ENSZ és az EU keretein belül addig kialakult jogi megközelítéseket, eszközöket³ és a Helsinki Bizottság beavatkozására kifejezetten vizsgálta a kérdésnek a személyes adatok védelmével kapcsolatos jogi követelményeit, aspektusait is.⁴

Az EJEB az ügy érdemi megítélése során első körben rögzítette, hogy a sérelmes magatartást az Egyezmény 8. cikkében biztosított magán- és családi élet tiszteletben tartásához való jog szempontjából kell vizsgálni. Azt is kifejtette továbbá a bíróság, hogy ugyan az Egyezmény 8. cikke alapvetően az indokolatlan állami beavatkozástól, jogkorlátozástól való védelmet szolgálja, ugyanakkor a kérdéses jog az állam számára pozitív kötelezettségeket is eredményez, amely a magánszféra tiszteletben tartásának a polgárok egymás közötti kapcsolataiban történő biztosítását is magában foglalja. A bíróság leszögezte, hogy az e védelmet szolgáló alkalmas eszközök kiválasztásában a tagállamok széles körű mérlegelési jogkörrel bírnak, ugyanakkor a privátszféra olyan súlyos megsértése esetén, amikor a magán- és családi élet lényegi tartalma és alapvető értékei sérülnek, a tagállamoknak hatékony elrettentő eszközökkel kell rendelkezniük, mely magában foglalja a büntetőjogi eszközöket is.

Az EJEB leszögezte, hogy önmagában egy cselekmény büntetendővé nyilvánítása csak korlátozott visszatartó hatással bír, ha a jog nem biztosít eszközöket az elkövető azonosítására és ezért az nem vonható felelősségre. A bíróság azt is kimondta, hogy az Egyezmény 8. cikkében foglalt jogokhoz kapcsolódó, az államot terhelő pozitív intézkedési kötelezettség magában foglalja azt is, hogy az államok olyan szabályokat vezessenek be, amelyek hatékony bűnüldözést és vádemelést tesznek lehetővé. Az olyan esetekben pedig, amikor egy gyermek fizikai és pszichikai épsége sérül, különösen fontos a fenti követelmények teljesítése és ilyen esetekben az ezeket az értékeket sértő elkövető azonosíthatósága elengedhetetlen. A bíróság e körben számba vette a tisztességes eljárásból fakadó és a személyes adatok védelmével, bizalmasságával kapcsolatos követelményeket is, ám úgy vélte, hogy ezek nem képezhetik akadályát egy hatékony büntetőeljárásnak. A különböző alapvető jogok közötti konfliktus rendezésének és a különböző érdekek egyensúlyba hozása ugyanakkor a tagállami jogalkotó feladata. Az ítéletben mindezek alapján az EJEB megállapította, hogy Finnország megsértette a kérelmezőnek az Egyezmény 8.

³ Lásd EJEB, 2008. december 2., *K. U. kontra Finnország*, ECLI:CE:ECHR:2008:1202JUD000287202 22-32. §. Az Európai Unió jogalkotása körében kifejezetten szerepel az ítéletben 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 szóló 2006/24/EK 2006. március 15-i európai parlamenti és tanácsi irányelv.

⁴ EJEB, 2008. december 2., *K. U. kontra Finnország*, ECLI:CE:ECHR:2008:1202JUD000287202 33-34. §

cikkében meghatározott jogát azzal, hogy a finn jogi szabályozás nem tette lehetővé az elkövető azonosítását lehetővé tevő telekommunikációs adatokhoz való hozzáférést.⁵

Álláspontom szerint a fentiekben kifejtett megfontolásokat a tárgybeli ügy kapcsán sem lehet figyelmen kívül hagyni. Nyilvánvaló ugyanis, hogy ha egy országban nem érvényesül általános adatmegőrzés, akkor a fentiekhez hasonló ügyekben szinte bizonyosan nem lesz képes biztosítani, hogy az ilyen típusú vagy más súlyos bűncselekmények elkövetőit azonosítsák, az elkövetés körülményeit feltárják és felelősségre vonják. E tekintetben rá kell mutatni, hogy a fentiekhez hasonló bűncselekmények esetében szinte kizárólag múltbeli telekommunikációs adatok révén képzelhető el az elkövető azonosítása és így a hatékony büntetőeljárás lefolytatása. Feltételes vagy jövőre vonatkozó adatmegőrzés esetén mindez nem lenne lehetséges. Ebben az esetben ugyanakkor a tagállamok aligha lesznek képesek teljesíteni az EJEB által kifejtettek szerint a sértettek magán- és a családi élet tisztelgetben tartásához fűződő jogából fakadó pozitív kötelezettségeiket, amelyek közé az elkövetők azonosítása és az ehhez szükséges hatékony büntetőeljárás eszközök is beletartoznak.

3.4. Fontosnak annak hangsúlyozása, hogy a metaadatok büntetőeljárások során történő felhasználása nem pusztán elvi lehetőség és a gyakorlat során számtalan büntetőügyben jut kiemelkedő jelentőséghez. A magyar hatóságok jogalkalmazói tapasztalatai szerint az elektronikus hírközlési szolgáltatók által kezelt adatok általános megőrzési kötelezettsége és az azokhoz való hozzáférés nagymértékben biztosítja és támogatja a nyomozó hatóságok bűnmegelőzési és bűnüldözési feladatainak ellátását. Ennek megszüntetése a büntetőeljárások sikertelenségéhez, a bűncselekmények egyes elkövetési jellemzőinek azonosíthatatlanságához, az elkövetők felelősségre vonásának elmaradásához vezetne, amely az állampolgárok nyomozó szervekbe vetett bizalmának megrendülését, továbbá az állami büntetőhatalom érvényre juttatásának elmaradását okozhatja. Az általános adatmegőrzés és adathozzáférés ezért álláspontom szerint nyilvánvalóan nem szüntethető meg.

Érdemes arra is felhívni a figyelmet, hogy az igényelt, illetve szolgáltatott adatok mennyiségét gyakorlati szempontból nem a bűncselekmény súlya, hanem a bizonyítás szükségessége befolyásolja alapvetően. Egy bűncselekmény tárgyi súlya nem képezi, és nem is képezheti le egy deliktum hatásmechanizmusának teljes spektrumát. Alacsonyabb törvényi fenyegetettségű cselekménynek is lehet nagyobb társadalmi hatása, előidézhetheti a védett jogtárgy nagyobb fokú sérelmét, súlyosabban veszélyeztetheti a közrendet, mint olykor egy csupán büntetési tételkerettel ekként minősített nagyobb tárgyi súlyúnak, nem beszélve arról, hogy a tárgyi súly feltárása éppen a nyomozás ezen eszközeinek eredménye és nem ab ovo adott. Továbbá egy súlyos bűncselekményre vonatkozóan is elegendő lehet az adatok szűkebb köre, ha annak elkövetése, előkészítése rövid időre korlátozódik, de egy kisebb súlyú, ám sorozatos jelleggel elkövetett bűncselekmény is indokoltta teheti nagyobb mennyiségű adat vizsgálatát, ha a cselekmény elkövetése hosszabb időszakot ölel fel. Az egyszerű helymeghatározó adatok, melyekből pusztán az ismerhető meg, hogy az elkövető hol, mikor, kivel és mennyi ideig kommunikált, de a közlések pontos tartalma nem, a fentiek szerint bármilyen súlyú bűncselekmény esetén elengedhetetlen bizonyítási eszköz lehet és arányos eszköznek is tekinthető egy bűncselekmény felderítése, illetve bizonyítása során.

A fentiek alátámasztására a számos szóba jöhető konkrét büntetőügy közül most csak az alábbi négy konkrét ügyet vagy ügytípust kívánom kiemelni.

⁵ EJEB, 2008. december 2., K. U. kontra Finnország, ECLI:CE:ECHR:2008:1202JUD000287202 K.U. v. Finnország 43-50. §

Magyarországon az óriási felháborodást kiváltó ún. romagyilkosságok során 2008-2009-ben több elkövető kilenc helyszínen hajtott végre fegyveres támadást romák otthonai ellen. A bűncselekmény-sorozat következtében hat ember, köztük egy gyermek meghalt, öten súlyosan megsérültek. Az elkövetők összesen 78 lövést adtak le, 11 Molotov-koktélt dobtak házakra, 55 ember testi épségét veszélyeztették. A rasszista szándékkal elkövetett, összesen majdnem másfél évig folyó támadássorozat elkövetőit hosszas nyomozást követően, nem utolsósorban az elkövetések helyszínén forgalmazó telekommunikációs eszközök hívásadatainak az elemzése révén sikerült azonosítani és elfogni. Az ügyben hozott bírósági ítéleteket tanulmányozva az is látható, hogy az egyes bűncselekmények bizonyítása során a hívásforgalmazási adatok kiemelt jelentőséggel bírtak az elkövetők bűnösségének az alátámasztása során⁶. Bizonyossággal állítható, hogy az általános adatmegőrzés hiányában ezen bűncselekmény-sorozat felderítése és az elkövetők bűnösségének a bizonyítása szinte elháríthatatlan akadályokba ütközött volna. Az elkövetőket végül életfogytig tartó szabadságvesztésre ítélték.

Egy másik példaként említhető, bírósági ítélettel zárult ügy tárgya mintegy 30 rendbeli rablás bűncselekménye volt, amelyeket oly módon hajtottak végre, hogy az elkövetők meleg társkereső oldalon keresztül, telefonon léptek kapcsolatba a sértettekkel, a megismerkedés után a sértetteket lakásaikban altatószerrel elkábították és kifosztották. A három elkövető beazonosítása, más szóba jöhető személyek kizárása az elkövetői körből, valamennyi elkövetés felderítése és végül a bíróság előtti bizonyítás lehetetlen lett volna a hívásforgalmi és készülékadatok beszerzése, széles körű és módszeres elemzése nélkül. Az elkövetők számos telefont használtak és váltogatták a telefonokban a SIM-kártyákat, továbbá változatos helyszíneken és eltérő személyi összetételben követték el sorozatban a bűncselekményeket, így a SIM-kártyák, telefonkészülék-adatok és a cellainformációk rendelkezésre állása nélkül nem kerülhetett volna sor ezen kiemelkedően súlyos bűncselekmény-sorozat felgöngyölítésére és az elkövetők felelősségre vonására. Az elkövetőkkel szemben végül tizenöt, tizenöt, illetve nyolc év szabadságvesztést szabtak ki.⁷ A bírósági ítéleteket tüzetesebben tanulmányozva figyelemreméltó, hogy a megállapított tényállás a hívásforgalmi adatok részletes és egészen bonyolult elemzésén alapul.

Említést lehet tenni arról is, hogy a gyermekpornográfia miatt indult eljárásokban tipikusnak tekinthető az, hogy a rendelkezésre álló IP-cím alapján csak a szolgáltatóktól beszerzett metaadatok alapján lehetséges az elkövetők beazonosítása, illetve a későbbi bizonyítás során az elkövetés kétséget kizáró megállapítása. Az általános adatmegőrzés nélkül a hatóságok ezen elkövetői kört más módon nem lennének képesek felderíteni.

Végül meg lehet említeni az ún. darnózseli hentes ügyét is, amely ügyben – a holttest teljes eltüntetése miatt – a későbbi, közvetett bizonyítékok alapján történt elítélés minden bizonnyal lehetetlen lett volna a sértett és az elkövető telefonjainak a mozgásának a megállapítását lehetővé tevő, a szolgáltatók által megőrzött adatok nélkül.

3.5. Azt is ki kell emelni, hogy ha a tárgybeli ügyben az Alkotmánybíróság esetlegesen azt állapítaná meg, hogy az általános adatmegőrzés előírása alaptörvény-ellenes, akkor ennek elvileg beláthatatlanul széles körű következményei lehetnek büntetőügyek egész sorára. Ennek kapcsán ki kell emelni, hogy egyrészt még folyamatban lévő ügyekben is megváltoztathatja a jogi értékelést és döntően befolyásolhatja a vád megalapozottságát. Ugyanakkor már lezárt büntetőügyekre is hatással lehet, tekintettel arra, hogy a büntetőeljárás szabályozásában ismert felülvizsgálat jogintézménye éppen arra szolgál, hogy a bíróság a jogerősen már lezárt ügyek

⁶ Lásd Fővárosi Ítéltábla mint másodfokú bíróság 5.Bf.399/2014/61. számú ítélete és a Kúria mint harmadfokú bíróság Bhar.I.1320/2015/47. számú ítélete

⁷ Lásd Fővárosi Törvényszék 25.B. 539/2013/374. számú ítélete

esetében is megváltoztathassa az ügyben hozott ítéletet olyan esetekben, amikor utóbb derül fény arra, hogy például a terhelt bűnösségének a megállapítására jogsértő módon került sor.

A fentiek alapján álláspontom szerint kiemelkedő jelentőséget kell annak tulajdonítani, hogy a tárgybeli alkotmánybíróági ügyben hozott döntés eredménye messze túlmutathat a szabályozási kérdéseken és a jogalkalmazásra nézve is jelentős következményei lehetnek. Ezen hatások körülmekintő mérlegelése, a büntetőeljárásban történő bizonyíték-felhasználás, mint körülmény vizsgálata, ezért kiemelt jelentőségűnek tűnik a jelen ügyben.

3.6. Megjegyzendő, hogy a Kormány az Európai Bíróság előtt folyamatban lévő, ilyen típusú összes ügyben – számos más tagállammal együtt – konzekvensen és kimerítő részletességgel érvelt amellett, hogy a kötelező adatmegőrzés szabályozása feltétlenül szükséges az alapvető állami feladatok ellátása, illetve mások jogainak a védelme érdekében, és a digitális korban elengedhetetlen a tisztességes eljáráshoz való jog biztosításához.

4. Az Alkotmánybíróóság releváns gyakorlata

Az ügyben áttekintettem a releváns alkotmánybíróági gyakorlatot is.

„Az Alaptörvény VI. cikke különálló bekezdésben [(2) bekezdés] rendelkezik a személyes adatok védelméről. Tekintettel arra, hogy a régi Alkotmány 59. § (1) bekezdés utolsó fordulata („mindenkit megillet [...] a személyes adatok védelméhez való jog”) és az Alaptörvény VI. cikk (2) bekezdés első fordulata („Mindenkinek joga van személyes adatai védelméhez”) tartalmilag megegyezik, az Alkotmánybíróóság – az Alaptörvény értelmezési szabályainak keretei között – jelen ügyben is irányadónak tekintette a korábbi Alkotmányon alapuló határozatokban kifejtett elvi jellegű megállapításokat.

Az Alkotmánybíróóság a személyes adatok védelméhez való jogot nem hagyományos védelmi jogként értelmezte, hanem annak aktív oldalát is figyelembe véve, információs önrendelkezési jogként. A személyes adatok védelméhez való jognak eszerint az a tartalma, hogy mindenki maga rendelkezik személyes adatainak feltárásáról és felhasználásáról. **Személyes adatot felvenni és felhasználni tehát általában az érintett beleegyezésével szabad; mindenki számára követhetővé és ellenőrizhetővé kell tenni az adatfeldolgozás egész útját, vagyis mindenkinek joga van tudni, ki, hol, mikor, milyen célra használja fel az ő személyes adatát. Kivételesen törvény elrendelheti személyes adat kötelező kiszolgáltatását, és előírhatja a felhasználás módját is [15/1991. (IV. 13.) AB határozat, ABH 1991, 49, 42].**

Az Alaptörvény az egyén-közösség közötti viszonyt az egyén közösséghez kötöttsége jegyében határozta meg, anélkül azonban, hogy annak egyedi értékét érintené. Ez következik különösen az Alaptörvény O) cikkéből és II. cikkéből. Ezért az Alaptörvény értelmezése során is fenntartható a személyes adatok védelméhez való jogot információs önrendelkezési jogként értelmező korábbi alkotmánybíróági gyakorlat. **Az információs önrendelkezési jog szorosan kapcsolódik a magánszférához való joghoz és az arról való döntést foglalja magában, hogy az egyén mikor és milyen korlátok között fed fel a személyéhez köthető adatokat. Az egyénnek társadalmi lényként, szociális beágyazottsága miatt bizonyos mértékben azonban el kell tűrnie adatai kötelező kiszolgáltatását, és azok állami felhasználását. (...)**

Az Alkotmánybíróóság az információs önrendelkezési jog korlátozásának feltételeit az alapjogkorlátozás szokásosan alkalmazott tesztjéhez (szükségesség-arányosság) képest konkretizálta. **Az információs önrendelkezési jog gyakorlásának feltétele és egyben legfontosabb garanciája eszerint a célhoz kötöttség. Ez azt jelenti, hogy személyes adatot feldolgozni csak pontosan meghatározott és jogszerű célra szabad. Az adatfeldolgozásnak minden szakaszában meg kell felelnie a bejelentett és közhitelűen rögzített célnak. A célhoz kötöttségből következik, hogy a meghatározott cél nélküli, „késletre”, előre nem meghatározott jövőbeni**

felhasználásra való adatgyűjtés- és tárolás alkotmányellenes [15/1991. (IV. 13.) AB határozat, ABH 1991, 49, 42.]. Az információs önrendelkezési jogra is vonatkozik az Alaptörvény I. cikk (3) bekezdésében foglalt – a korábbi alkotmánybírósági gyakorlatban kidolgozott – általános kritérium, miszerint alapvető jognak csak más alapvető jog érvényesülése vagy valamely alkotmányos érték védelme szabhat korlátot. Az alapjogkorlátozás általános kritériumainak megjelölése tartalmazza az „elérni kívánt céllal arányosan” kitévelt, amely az adatok feldolgozása terén különösképpen kötelez a célhoz kötöttségre.” (...) A magánszféra védelméhez való jog és az információs önrendelkezési jog nem korlátlan alapjogok. A magánszférába való behatolást és a megszerzett adatok felhasználását mind bűnüldözési, mind pedig nemzetbiztonsági célok igazolhatják. Az egyén mindeközben alapjogainak csak olyan mértékű korlátozását köteles elviselni, amelynek alkotmányos törvényi alapja van.” {32/2013. (XI. 22.) AB határozat, Indokolás: [86] – [88], [90] – [91], [93]}

Összegzőképpen megállapítható, hogy az Eht. 159/A. § rendelkezései maradéktalanul megfelelnek az Alaptörvény rendelkezéseinek, mivel Magyarország biztonságának védelme érdekében, a szükséges mértékben, az elérni kívánt céllal arányos módon írnak elő adatmegőrzési kötelezettséget.