

MOHÁCSI BARBARA

Az elektronikus nyomozási eszközök alkotmányosságának kérdése Németországban

Napjainkban a bűnözés és – így szükségképpen – a bűnüldözés területén is egyre inkább terjed az internet, valamint az informatikai eszközök alkalmazása. Az elkövetők egyre nagyobb mértékben használják fel bűncselekmények elkövetéséhez a legmodernebb technikai eszközöket, és „gondosan” követik fejlődésüket. A bűnüldöző hatóságok a gyorsabb és hatékonyabb felderítés érdekében kezdték el alkalmazni a modern informatikai megoldásokat, így például a nyomozás során a telekommunikációs eszközök lehallgatását vagy az adatok biztonsági célból történő gyűjtését és készletezését.¹ Az elektronikus nyomozási intézkedések új bizonyítékgyűjtési lehetőséget teremtenek a nyomozó hatóságok számára.

Az online házkutatás

Az online házkutatás lényege, hogy az úgynevezett „trójai” szoftver² segítségével a hatóságok észrevétlenül behatolhatnak a megfigyelt személy számítógépébe, és így hozzájuthatnak az ott tárolt adatokhoz. Az online házkutatás tehát valójában az internet útján történő titkos adatszerzési tevékenység.³

A számítógépeken tárolt adatok interneten keresztüli megfigyelésének lehetőségét a 2001. szeptemberi terrorcselekmények után vezették be az Amerikai Egyesült Államokban. Az Amerikai Szövetségi Nyomozó Iroda (FBI) 2007. július 19-én alkalmazta először az online átvizsgálást egy szövetségi állami iskola felrobbantásával fenyegetődöz bűnöző személyazonosságának megállapítása érdekében. A számítógép teljes merevlemezét átvizsgáló szoftvert az interneten keresztül telepítették. A művelet befejezésével a program továbbította a hivatalnak az összes felinstallált program nevét, az internetes böngésző jellemzőit, az operációs rendszer

1 Manfred Hoffmann: Die Online-Durchsuchung – staatliches „Hacken“ oder zulässige Ermittlungsmaßnahme? Neue Zeitschrift für Strafrecht, Heft 3, 2005, S. 121.

2 A „trójai” jelző arra utal, hogy a számítógépre telepítendő szoftver más programnak álcázva jut be a célnépszerűbe.

3 Michael Sachs – Thomas Krings: Das neue „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme”. JuS, 2008, S. 481–482.

nevét, típusát, sorozatszámát, az utoljára felkeresett internetcímet és az összes IP-címet, amellyel az illető a böngészései közben kapcsolatba került. A vizsgálat sikeres volt, a hatóságok megállapították a gyanúsított kilitét, megakadályozva ezzel a további fenyegetéseket és robbantásokat.

Európában először egyes svájci kantonokban tették lehetővé (amerikai mintára) a gyanúsítottak számítógépének hatósági kémprogram útján történő átvizsgálását.

Az *Egyesült Királyságban* különösen súlyos bűncselekmények gyanúja esetén bírói engedély nélkül is lehetséges Keylogger telepítése és a számítógépek átvizsgálása.⁴

Ausztriában 2007. október 17-én határozott a Ministerrat⁵ az online kutatásnak (Online-Fahndung) nevezett új nyomozási módszer törvényi szabályozásának szükségességéről. A magánszemélyek számítógépének megfigyelésére csak a minimum tízévi szabadságvesztés büntetéssel fenyegetett bűncselekmények esetében kerülhetne sor, mégpedig kizárólag bírói határozat alapján. Az online kutatás végrehajtási szabályairól azonban a mai napig nem alkottak jogszabályt, ezért a gyakorlatban a számítógépen tárolt adatok interneten keresztül vizsgálatára a házkutatás és a telekommunikációs eszközök lehallgatására vonatkozó rendelkezéseket alkalmazzák.

Franciaországban is felvetődött az információs technikai rendszerek internet útján történő hatóság általi titkos megfigyelése. Hosszas vitákat követően 2010. szeptember 8-án fogadták el az úgynevezett „LOPPSI 2”⁶ törvénycsomagot, amelynek 23. cikke meghatározott bűncselekmények esetén lehetővé teszi a nyomozási bíró számára az online házkutatás elrendelését.

Németországban a közelmúltban politikai szinten merült fel a közbiztonság erősítése érdekében a számítógépek online átvizsgálásának lehetősége (Online-Durchsuchung). A Bundestag 2006. november 9-én hirdette meg a *Belső biztonság megerősítését szolgáló programot*.⁷ A program célja a Szövetségi Bünygyi Hivatal⁸, a rendőrség, a Szövetségi Alkotmányvédelmi Hivatal⁹ és a Szövetségi Információs Technikai Biztonsági Hivatal¹⁰ operatív nyomozási intézkedési jogkörök-

4 Computer Misuse Act 1990. Regulation of Investigatory Powers Act 2000.

5 A Ministerrat a kancellár elnökletével a kancellária hivatalában tartott kormányülés.

6 Loi d'orientation et de programmation pour la performance de la sécurité intérieure.

7 „Program zur Stärkung der Inneren Sicherheit” (PSIS).

8 A Szövetségi Bünygyi Hivatal, a Bundeskriminalamt (a továbbiakban: BKA) a belügyminisztériumon belül működő szervezet, amelyet a „Das Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und Länder in kriminalpolizeilichen Angelegenheiten” (a továbbiakban: BKA-törvény) hozott létre 1997. augusztus 1-jén.

9 Bundesamt für Verfassungsschutz.

10 Bundesamt für Sicherheit in der Informationstechnik.

kel történő felruházása volt. Ilyen tervezett intézkedés volt a BKA által véggezhető online házkutatás.¹¹

Észak-Rajna–Vesztfália tartomány alkotmánya a 2006. december 30-án hatályba lépő módosítás következtében lehetővé tette az internet információszerzés céljából történő titkos megfigyelését súlyos, egyébek között például államellenes bűncselekmények esetében.¹² Ez ellen az alkotmányi rendelkezés ellen nyújtottak be alkotmányjogi panaszt a Német Szövetségi Alkotmánybírósághoz, amely 2008. február 27-i döntésében alkotmányellenesnek minősítette és megsemmisítette az alkotmánymódosító törvény online házkutatásra vonatkozó szabályait.¹³

Készletező adattárolás

A közelmúltban került sor az Európai Unióban egy újabb, a nyomozás során is felhasználható titkos intézkedés, az úgynevezett készletező adattárolás harmonizált szabályozására. A készletező adattárolás meghatározott távközlési adatok tárolási kötelezettségét írja elő a telekommunikációs szolgáltatók számára, amely adatokhoz – a törvény által meghatározott feltételek esetén – kötelesek hozzáférést engedni a hatóságok számára.

Franciaország, Írország, Svédország és Nagy-Britannia korábban kezdeményezte a készletező adattárolásról szóló kerethatározat elfogadását¹⁴, amelyet azonban az Európai Parlament elutasított.¹⁵ A készletező adattárolás bevezetését végül a 2006/24/EK irányelv¹⁶ írta elő a tagállamok számára, amelyet – Írország és Szlovákia ellenszavazatával – az EKSZ 95. cikke¹⁷ alapján fogadtak el. Az irányelv abból a gondolatból indul ki, hogy a telekommunikációs adatok értékes eszközt jelentenek a szervezett bűnözés és a terrorizmus elleni küzdelemben. A dokumentum számol azonban azzal, hogy a tagállamokban meglévő jogi és technikai különbségek kihatnak az elektronikus telekommunikáció belső piacára, mert a telekommunikációs szolgáltatásokat kínáló különböző előírásokkal szembesülnek a mentett adatok köre és a mentés időtartama tekintetében.

11 Bertold Huber: Trojaner mit Schlapphut – Heimliche Online-Durchsuchung nach dem Nordrhein-Westfälischen Verfassungsschutzgesetz. Neue Zeitschrift für Verwaltungsrecht, Heft 8, 2007, S. 880–882.

12 § 5 Abs. 2. Nr. 11 des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen.

13 1 BvR 370, 595/07 sz. [2008. február 27.]

14 Tanácsí dokumentum 8958/04. [2004. április 28.]

15 Parlamentí dokumentum P 6 TA[2005]0348.

16 Az Európai Parlament és Tanács 2006/24/EK irányelve 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, HL L 105, 2006. április 13. 54–63. o.

17 A lisszaboni szerződés előtti számozást lásd a továbbiakban is.

Az irányelv fő célja az elektronikus hírközlés belső piacát érintő akadályok megszüntetése, a tagállamok készletező adattárolásra vonatkozó szabályainak harmonizálása. Másodsorban azonban azt a célt is szolgálja, hogy az adatok a súlyosabb bűncselekmények nyomozása és üldözése esetén rendelkezésre álljanak. Ennek érdekében az irányelv 6. cikke az adatok mentésére és tárolására nyitva álló időszakot hat hónaptól két évig terjedő időtartamban határozza meg; a 4. cikk értelmében a tagállamok kötelesek gondoskodni arról, hogy meghatározott esetekben a nemzeti joggal egyetértésben az adatokat az illetékes nemzeti (bűnüldöző) hatóságoknak továbbítani lehessen. A 7. cikk pedig az adatbiztonság minimális követelményeinek megtartását rögzíti.

Az irányelv érvényességét és az uniós alapjogoknak való megfelelését sokan kétségbe vonták.¹⁸ 2009. február 10-én az Európai Bíróság visszautasította Írország keresetét, amely semmisségi eljárás keretében kérte az irányelv megsemmisítését arra hivatkozva, hogy azt nem megfelelő jogalapon fogadták el. Az írek véleménye szerint ugyanis nem az EKSZ 95. cikke, hanem az EUSZ rendőrségi és igazságügyi együttműködésre vonatkozó 30. és 31. cikke alapján kellett volna megalkotni a szabályozást, amely azonban egyhangú döntéshozatali követelt volna meg.¹⁹

Az irányelvet átültető nemzeti jogszabályok alkotmányosságával kapcsolatban több tagállamban kezdeményezték a nemzeti alkotmánybíróságok eljárását. A készletező adattárolásról szóló irányelv átültetését megalvalósító nemzeti jogszabály megsemmisítését először a román alkotmánybíróság mondta ki 1258. számú határozatában 2009. október 8-án.

Németországban egy törvénymódosítás 2007. december 21-től újraszabályozta a telekommunikációs eszközök megfigyelését, rendelkezett a 2006/24/EK irányelv alapján bevezetett készletező adattárolás részletes szabályairól és azok büntetőeljárásbeli felhasználhatóságáról.²⁰ Az új törvényi szabályokkal ellentétben több alkotmányjogi panaszt is benyújtottak a telekommunikációs titokhoz fűződő jog és az információs önrendelkezéshez való jog sérelmére hivatkozással. A Szövetségi Alkotmánybíróság 2010. március 2-i döntésében megsemmisítette a telekommunikációs törvény készletező adattárolásra vonatkozó szabályait.²¹

18 Valószínűleg ezt jelzi, hogy a 2006/24/EK. irányelvet a mai napig nem ültette át több állam, például Görögország, Ausztria és Svédország, holott az átültetésre nyitva álló határidő 2007. szeptember 15-én lejárt.
19 Az Európai Bíróság C-301/06. sz. Írország kontra Parlament és Tanács-ügyben 2009. február 10-én hozott ítélete.

20 A telekommunikációról szóló törvény. Telekommunikationsgesetz vom 22. 06. 2004 (a továbbiakban: TKG) 113a § és 113b §; valamint a büntetőeljárásról szóló törvény, Strafprozessordnung vom 12. 09. 1950 (a továbbiakban: StPO) 100g §. Vö.: Hans Kudlich: Die Zulässigkeit strafprozessualer Online-Durchsuchungen. Humboldt Forum Recht, 2007, Beitrag 19, S. 1–12.

21 1 BvR 356/08, 1 BvR 263/08, 1 BvR 586/08 sz. (2010. március 2.)

A magyar Alkotmánybíróság előtt is megtámadták az irányelvet átültető elektronikus hírközlésről szóló 2003. évi C. törvény vonatkozó rendelkezéseit, az Alkotmánybíróság eljárása azonban még folyamatban van.

További érdekesség, hogy 2010. május 5-én az ír legfelsőbb bíróság előzetes döntéshozatali kérelemmel fordult az Európai Unió Bíróságához a készletező adat-tárolásról szóló irányelv uniós alapjogoknak való megfelelése kérdésében.

Az új elektronikus nyomozási eszközök célja és technikai megvalósítása

Az online házkutatás

Az online házkutatás tulajdonképpen titkos, a kommunikációs hálózaton keresztül történő állami beavatkozást jelent más információs technikai rendszerbe.²² Magában foglalja az egyszeri és a hosszabb ideig tartó folyamatos megfigyelő tevékenységet is. Általános célja a biztonság növelése a terrorizmussal szemben, konkrét célja a terhelt aktivitására utaló jelek vagy bizonyítékok feltárása. A szabályozással a tagállamok azt kívánják elérni, hogy a nyomozó hatóságok előnybe kerüljenek, vagy legalább lépést tartsanak az elkövetőkkel.

Az online házkutatás technikai megvalósítása egymásra épülő, többszintű informatikai lépések alkalmazásával történhet. Elsőként a hatóságok a számítógépre juttatják a hatósági kémiszoftvert, majd az installálás után történik az adatnyerés és a kommunikáció, az adatátvitellel pedig befejeződik az intézkedés. A szoftvert két módon lehet a számítógépre telepíteni: a terhelt lakásában közvetlenül a nyomozó hatóság tagja által, illetve közvetett módon az interneten keresztül. Az internet lényegében az adatok továbbításához szükséges.²³ A szoftver számítógépes rendszerbe juttatásának tipikus módja, amikor a felhasználónak ajánlatokat tartalmazó e-maileket küldenek, amelyeket meg kell nyitni a kémiszoftver aktiválásához.²⁴ Ez persze előzetes tájékozódást igényel a megfigyelt személyről, mert ha érdektelen az ajánlatok iránt, akkor nem fogja megnyitni az e-maileket, és a program nem aktiválódik.

A sikeres feltelepítés után kerül sor a tulajdonképpeni online házkutatásra. Az interneten keresztül a kémiszoftver segítségével a nyomozók hozzáférhetnek a szá-

22 Tido Park: Handbuch Durchsuchung und Beschlagnahme. 2. Aufl, H. Beck Verlag, München, 2009, S. 765.

23 Gerrit Hornung: Ermächtigungsgrundlage für die Online-Durchsuchung? Datenschutz und Datensicherheit, 8/2007, S. 575–576.

24 Ulf Buermeyer: Die Online-Durchsuchung. Die technische Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme. Online Zeitschrift für Höchstrichterliche Rechtsprechung im Strafrecht, 4/2007, S. 156.

mítógépen lévő adatokhoz. Az adatok lementése akkor is lehetséges, ha az internetes kapcsolat időközben megszakad, mert a kémiszoftver az internetes kapcsolat befejezésekor megszakítja az adatátvitelt, a számítógép újracsatlakoztatása esetén pedig ugyanott folytatja tovább, ahol félbeszakadt a mentési folyamat. A mai hordozható számítógépek többségében már van beépített kamera és mikrofon. Technikailag könnyen kivitelezhető akár a beépített, akár a csatlakoztatott kamera és mikrofon aktiválása, illetve a felvett audio- és videoadatokhoz való hozzáférés, amely tulajdonképpen a magánlakás megfigyelését, lehallgatását teszi lehetővé az internet segítségével. Az online házkutatás befejeztével a kémiszoftvert el kell távolítani a célszemély számítógépéről.²⁵

Mivel a kémiszoftver gyakorlatilag vírus módjára viselkedik, ezért veszélyt jelenthetnek rá a vírusirtó programok és az illetéktelen behatolás ellen védő tűzfal. A szakemberek szerint technikailag nem oldható meg teljes biztonsággal, hogy a hatósági kémiszoftverben ne tegyenek kárt a vírusirtó programok. Következésképpen érdemes lenne az államoknak valamilyen együttműködést kialakítaniuk az antivírus-programok előállítóival olyan megoldások kidolgozása érdekében, amelyek beiktatása révén a vírusirtók nem lennének veszélyesek a hatósági megfigyelőprogramra. Ez azonban egyelőre nem tűnik reális elképzelésnek, mivel a szoftvergyártók olyan programokat terveznek, amelyeket világszerte alkalmaznak, és nem érdekük az egyedi kérések figyelembevétele.²⁶

További probléma, hogy a szakemberek szerint a rendszer nem igazolja a kapott adatok valódiságát; nem garantált, hogy a folyamat a nyomozók vagy a használók által teljesen ellenőrzött legyen. Minthogy maga az állami kémiszoftver is képes az adatok megváltoztatására, a megfigyelési határozattal való visszaélés lehetősége sem zárható ki.²⁷ A manipulálás előfordulhat abban az esetben is, ha a megfigyelt terhelt felfedezi a kémiszoftvert. Ez oda vezethet, hogy a gyanúsított eltávolítja a szoftvert, idő előtt megszakítva ezzel az online házkutatást, vagy felhasználja a saját céljaira. A hatóságok nem képesek észlelni ugyanis, ha a gyanúsított manipulálja a kémiszoftver által továbbított adatokat. Ez annál inkább veszélyes, mert az adatok megváltoztatásával a terhelt akár harmadik személyre is terelheti a gyanút, vagy más módon teljesen félrevezetheti a nyomozó hatóságokat. Még az is előfordulhat, hogy a felhasználó és a nyomozók mellett harmadik

25 Markus Hansen – Andreas Pfiztmann – Alexander Roßnagel: Die Online-Durchsuchung. Deutsche Richterzeitung, Heft 08/2007, S. 227–228.

26 Ulf Buermeyer: i. m. 159. o.

27 Már ismert olyan eset, amikor egy állami tisztviselő a hivatali technikai apparátust magáncélokra használta. Berliner Zeitung, 5. 9. 2007.

személy részleges ellenőrzést gyakorol a rendszer felett, például közös felhasználók vagy rendszergazdák által vezérelt több elemből álló egységek esetén.

Súlyos jogi problémát okozhat, ha a kémszoftver az ügyben nem érintett, harmadik személyeket is megfigyel (ami technikailag könnyen kivitelezhető). Ha a szoftvert e-mailen keresztül juttatták el a gyanúsított számítógépére, annak továbbküldésével további számítógépekre installálódhat a program, s ugyanezzel járhat, ha a gyanúsított a saját számítógépéről küld át fájlokat a harmadik személynek.²⁸

Az online házkutatás természetéből következik, hogy a végrehajtás csak addig lehetséges, amíg a terhelt csatlakozik az internethez. Ez már önmagában jelentős korlátja a hatékonyságnak. Az adatok átmásolásának időtartama az adatátviteli sebességtől függ, amely összefügg az internetkapcsolat minőségével. Lassabb, modem-es internet esetén előfordulhat, hogy a merevlemez teljes átmásolása ötven napig is eltarthat. Ezért a szoftver először a mentett adatok listáját továbbítja a nyomozó hatóságoknak, ebből a hatóságok a rendelkezésükre álló információk alapján kiválaszthatják a relevánsnak ígérkező adatállományokat.

Megkérdőjelezheti az online házkutatás sikerességét, ha a gyanúsított lementi az adatokat adathordozóra, és törli őket a számítógépről. A törölt adat azonban nem feltétlenül semmisül meg, mert technikailag lehetséges az adatok teljes vagy részleges helyreállítása. A törölt adatok felhasználhatóságnak jogi megengedése azonban több okból is megkérdőjelezhető. Az egyik, jelenleg megoldatlan, gyakorlati probléma, hogy rendszerint a törölt adatok azok, amelyek különösen jelentőssek a nyomozás szempontjából.

A készletező adattárolás célja és végrehajtása

A készletező adattárolás lényege, hogy a telekommunikációs szolgáltatóknak legalább hat hónapig tárolniuk és az állami feladatok ellátása érdekében rendelkezésre kell bocsátaniuk azokat az adatokat, amelyek információkat tartalmaznak a telekommunikációs kapcsolatban részt vevő személyekről, a kommunikációs folyamat idejéről és helyéről. Az adattárolási kötelezettség vonatkozik a vezetékes telefonra, mobiltelefonra, internetre, sms, mms és más jellegű üzenetekre, e-mail kapcsolatokra. A határidő lejártával az adatokat egy hónapon belül törölni kell. A kommunikáció tartalmát és a lehívott internet oldalon lévő adatokat nem lehet tárolni.²⁹

Az adatok felhasználására és más hatóságokhoz történő továbbítására csak meghatározott célból kerülhet sor. Ilyen célok a bűnüldözés, a közbiztonságot, vagy a szövetségi és tartományi alkotmányos szervek, szövetségi hírszerző szolgál-

28 Markus Hansen – Andreas Pfiztmann – Alexander Roßnagel: i. m. 225–228. o.
29 TKG 113a §, 113b §.

latok, katonai hírszerzés feladatait fenyegető jelentős veszély elhárítása. Bármely bűncselekmény esetén van azonban lehetőség arra, hogy bírói engedély alapján a bűnüldöző hatóságok, amennyiben ismerik az IP-címet, információt kapjanak az IP-címhez tartozó konkrét személyről.

A német büntetőeljárás törvény rendelkezik a tárolt adatok büntetőeljárásban történő közvetlen felhasználásáról, amennyiben az a tényállás felderítése vagy a terhelt tartózkodási helyének meghatározása érdekében szükséges.³⁰ További feltétel, hogy az információ megszerzése más módon kilátástalan lenne, vagy aránytalan nehézségekkel járna. A szabály előírja az érintettek utólagos értesítési kötelezettségét is. A készletező adattárolás gyakorlati megvalósításának részletes feltételeit (például az adatok tárolásának vagy továbbításának végrehajtását) szövetségi és tartományi szabályokban kell rögzíteni, erre azonban eddig nem került sor.

Az online házkutatás és a készletező adattárolás célja alapvetően megegyezik más nyomozási eszközök célkitűzéseivel, a különbséget a titkos jelleg adja, illetve az, hogy olyan információk megszerzése is lehetővé válik, amelyekre a hagyományos nyomozási eszközökkel nem lenne lehetőség.³¹ Összességében megállapítható azonban, hogy az online nyomozási eszközök alapvetően nem új intézkedések, hanem a meglévő nyomozási intézkedések „modernizált” változatai, amelyek igazodnak a modern technika legújabb fejlődési folyamataihoz.

Az online házkutatással és a készletező adattárolással kapcsolatban felmerülő alkotmányjogi problémák a Német Szövetségi Alkotmánybíróság határozatainak tükrében

A Szövetségi Alkotmánybíróság 1 BvR 370, 595/07 számú, 2008. február 27-i döntése az online házkutatásról

Az online házkutatás több alkotmányos alapjogot is érint, egyebek között az általános személyiségi jogot, az információs önrendelkezéshez való jogot, a privát szférához és a magánlakás sérthetetlenségéhez fűződő jogot.

A német alkotmánybíróság álláspontja szerint az online házkutatás alkotmányossági vizsgálatával kapcsolatban a kiindulópontot az általános személyiségi jogként meghatározható, a személyiség szabad kibontakoztatásához fűződő jog

30 StPO 100g §.

31 Kai Cornelius: Besonderheiten des Strafrechts und Strafprozessrechts. In: Andreas Leupold – Silke Glossner (Hrsg.): Münchener Anwalts Handbuch. C. H. Beck Verlag, München, 2008, Teil 8., Rn. 180.

jelenti az emberi méltósághoz való joggal összefüggésben.³² Az általános személyiségi jog a személyiség azon elemeit védi, amelyek nem tárgyai a német alkotmány más alapjogainak, de jelentősek a személyiség védelme szempontjából. Ez a „hézagpótló”, kiegészítő védelem különösen akkor válik szükségessé, ha újfajta veszélyek alakulnak ki, például a tudományos-technikai fejlődés vagy új életviszonyok következtében.³³

Az online házkutatás által érintett alkotmányos alapjogok

A német alkotmány 10. cikkében foglalt telekommunikációs titokhoz fűződő jog alapvetően a két ember közötti kommunikációs folyamatot védi, azaz az információk telekommunikáció által történő továbbítását a címzetthez.³⁴ Abban az esetben nyújt védelmet, ha a telekommunikációs eszköz megfigyelése kizárólag a lefolytatott vagy a folyamatban lévő kommunikációs folyamatra irányul. Nem terjed ki azonban a védelem arra a bizalmi viszonyra, amely az internetes kommunikáció során fennáll, továbbá arra az esetre sem, ha a számítógép merevlemezét internet segítségével átvizsgálják. A 10. cikk alapvetően a kommunikációs folyamatban közvetített adatokat védi, de nem jelent megfelelő garanciát az olyan speciális veszélyekkel szemben, amelyek az információs technikai rendszer használatából következhetnek.³⁵

A német alkotmánybíróság értelmezése szerint az alkotmány 13. cikke garantálja az egyének számára azt az élethez szükséges, alapvető privát területet, amelyen belül az érintett személy nyugalma csak kivételesen háborítható. A magánlakás védelme nemcsak a közhatalom fizikai behatolása ellen nyújt védelmet, hanem a lakáson kívülről történő technikai eszköz segítségével végbemenő beavatkozásra is vonatkozik.³⁶

Egyértelmű, hogy a lakáson kívül található számítógép megfigyelése nem tartozik a 13. cikk alá. Felvetődik azonban a kérdés, hogy az alkotmánybírósági döntés során az online házkutatást miért nem a „házi joggal” vetették össze abban az esetben, amikor a számítógép a lakásban helyezkedik el. Az alkotmánybíróság

32 Peter Schade: Grundgesetz mit Kommentierung, 7. Auflage, Berlin, 2006, S. 24.

33 1 BvR 1531/96 vom 10. 11. 1998, BVerfGE 99, 185 (193); 1 BvR 185/77 vom 03. 06. 1980, BVerfGE 54, 148 (153); 1 BvR 209/83 vom 15. 12. 1983, BVerfGE 65, 1 (41); 1 BvR 1550/03 vom Juni 2007, Neue Juristische Wochenschrift, 2007, 2464.

34 1 BvR 1494/78 vom 20. 06. 1984, BVerfGE 67, 157 (172); 1 BvR 1611/95, 1 BvR 805/98 vom 09. 10. 2002, BVerfGE 106, 28 (35).

35 1 BvR 370, 595/07 vom 27. Februar 2008, 189–190. V6.; Michael Sachs – Thomas Krings: i. m. 483. o.

36 1 BvR 253/56 vom 16. 01. 1957 BVerfGE 6, 32 (41); 1 BvL 19/63 vom 16. 07. 1969 BVerfGE 27, 1 (6); 2 BvR 454/71 vom 31. 01. 1973 BVerfGE 34, 238 (245); 2 BvR 1062/87 vom 14. 09. 1989 BVerfGE 80, 367 (373); 1 BvR 1084/99 vom 03. 03. 2004 BVerfGE 109, 279 (309–313).

csak azokat az eseteket ismerte el a 13. cikk alá tartozónak, amikor a rendszerhez csatlakoztatott más eszközök (mikrofon, kamera) segítségével a lakás megfigyelése is megvalósulhatott. A mai modern számítógépek szinte mindegyikében van beépített kamera és mikrofon, ezért a 13. cikk alkalmazása gyakorlatilag majdnem minden esetben fennállhat.

Az alkotmánybíróság álláspontja szerint a 13. cikk összességében nem jelent általános, a beavatkozás módjától független védelmet az információs technikai rendszerbe történő beavatkozással szemben; és a lakásban található információs technikai rendszerbe történő beavatkozással szemben sem garantál általános védelmet.³⁷

A magánszféra védelme lehetővé teszi az egyénnek, hogy mentesüljön a nemkívánatos megfigyelésektől.³⁸ *Az alkotmánybíróság kifejtette, hogy a magánszférához fűződő jog kapcsán nincs helye az egyéni érdekek és a köz érdekében történő bűnüldözés közötti mérlegelésnek, mert a privát sféra korlátozása az emberi méltósághoz való jog sérelmét jelentené, amely korlátozhatatlan, abszolút jog.³⁹ Az online házkutatás tehát nem korlátozhatja a privát sférához fűződő jogot. Mérlegelésre csupán annyiban kerülhet sor, hogy az online megfigyelés tárgyul szolgáló érinti-e az egyén magánszféráját.*

Az információs önrendelkezéshez való jog túlmutat a magánszféra védelmén. Az egyéneknek alapvetően joguk van maguknak meghatározni személyes adataik kiszolgáltatását és felhasználását. Az információs önrendelkezéshez való jog védelme nemcsak a szenzitív adatokra terjed ki, hanem azokra az információkra is, amelyek informatív értéke önmagában csekély, de más adatokkal összekapcsolva hatással lehet az érintett személyiségének fejlődésére és cselekvési szabadságára.⁴⁰

Az alkotmánybíróság álláspontja szerint az információs önrendelkezéshez való jog nem számol teljes körűen a személyiség veszélyeztetettségével, amely abból adódik, hogy az egyén személyisége kibontakoztatása során egyre jobban rá van utalva az információs technikai rendszer használatára, és ennek során kényszerűen adatokat szolgáltat. Az a harmadik személy, aki beavatkozik a rendszerbe, potenciálisan nagy adatállományhoz juthat hozzá anélkül, hogy adatszerzési vagy adatfeldolgozási tevékenységet kellene végeznie. Az alkotmánybíróság álláspontja sze-

37 1 BvR 370, 595/07 vom 27. Februar 2008, 193–195.

38 1 BvR 13/68 vom 15. 01. 1970, BVerfGE 27, 344 [350]; 2 BvR 988/75 vom 24. 05. 1977, BVerfGE 44, 353 [372]; 1 BvR 1689/88 vom 26. 04. 1994, BVerfGE 90, 255 [260]; 1 BvR 653/96 vom 15. 12. 1999, BVerfGE 101, 361 [382].

39 1 BvR 2378/98 vom 3. 3. 2004 BVerfGE.

40 1 BvR 209/83 vom 15. 12. 1983, BVerfGE 65, 1 [43]; 1 BvR 239/90 vom 11. 06. 1991, BVerfGE 84, 192 [194]; 1 BvR 1550/03 vom 13. Juni 2007. Neue Juristische Wochenschrift, 2007, 2464, 2466.

rint az adatállomány nagy kiterjedésére és ebből következően a személyiségi jogba történő beavatkozás különös súlyára tekintettel az információs önrendelkezéshez való jog nem nyújt elegendő védelmet az információs technikai rendszerekbe történő beavatkozásokkal szemben.⁴¹

Egy modernizált „klasszikus” alapjog, az információs technikai rendszer bizalmasságának és integritásának védelme

Az alkotmánybíróági eljárás során felvetődött az a kérdés, hogy szükség van-e új, önálló alapjogra, amely általános védelmet nyújt az információs technikai rendszer használatával összefüggésben. Új alapjog kialakítása ritkán fordult elő a Német Szövetségi Alkotmánybíróság gyakorlatában, de nem példa nélküli. Az alkotmánybíróóság határozataiban alakította ki ugyanis az általános személyiségi jog speciális értelmezéseit; egyebek között az általános személyiségi jogból vezették le az információs önrendelkezéshez és a magánszféra védelméhez való jogot.

Az információs önrendelkezéshez való jog olyan adatvédelmi alapjog, amelyet kifejezetten nem jelenik meg a német alkotmány rendelkezéseiben, amelyet az alkotmánybíróóság az úgynevezett „népszámlálási döntésében” ismert el alapjogként.⁴² A magánszféra védelme az általános személyiségi jog egyik alcsoportja, tartalmaz más alapjogok, a magánlakás sérthetlensége, a levél-, postai és távközlési titok védelme konkretizálják.

Az új alapjog kialakítását az a társadalmi jelenség indokolta, hogy az információs technika személyiségre és a személyiség kibontakoztatására gyakorolt hatását tekintve korábban előre nem látott jelentőségre tett szert.⁴³ A számítógépek hálózatos összekapcsolódásának lehetősége kiterjesztette az információs technika alkalmazásának határait, ami új veszélyeket jelent a személyiségre nézve. Az internet lehetőséget teremt harmadik személyeknek a technikai beavatkozásra, adatok kifürkészésére és manipulálására; ez új dimenzióba helyezte az adat és információ vonatkozású alapjogvédelmet.⁴⁴ Alapjogvédelmi igény keletkezett az információs technikai rendszer bizalmasságának és integritásának védelmére.

A Szövetségi Alkotmánybíróság álláspontja szerint más alkotmányos alapjogok, illetve az általános személyiségi jog eddig kialakult értelmezései nem garan-

41 1 BvR 370, 595/07 vom 27. Februar 2008, 200. Vö.: Michael Sachs – Thomas Krings: i. m. 483–484. o.

42 1 BvR 209, 269, 362, 420, 440, 484/83 vom 15. Dezember 1983.

43 Burkhard Hirsch: Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme – Zugleich Anmerkung zu BverfG: Neue Juristische Wochenschrift, 2008, S. 822; Neuen Juristischen Online-Zeitschrift, 2008, S. 1907–1909.

44 Gabriele Britz: Vertraulichkeit und Integrität informationstechnischer Systeme. Die Öffentliche Verwaltung, 2008, S. 411.

tájják teljes körűen az adatjogi és az információs önrendelkezéshez való speciális védelmet. Egyes vélemények szerint azonban az úgynevezett „IT-alapjog” valójában nem új alapjog, hanem a személyiség szabad kibontakoztatásához fűződő jognak a modern adatfeldolgozásra és a kommunikációs technikára adaptált változata, amely az alkotmánybíróság eddigi töretlen gyakorlatára épül.⁴⁵

A személyiséget érintő jogsértésekkel szembeni alapjogi védelem nem új gondolat, az információs technikai rendszerek kapcsán felvetődő normatív tartalom azonban újdonság. Az egyének személyiségük kibontakoztatása során egyre inkább rá vannak utalva az információs technikai rendszerre, hiszen az egyre jobban jelen van az állampolgárok mindennapi életében, a magán- és az üzleti szférában. Az alapjogi védelem olyan rendszerekre vonatkozik, amelyek önmagukban vagy technikai hálózatokkal az érintettek személyes adatait tartalmazhatják, és az ebbe történő beavatkozással képet lehet alkotni egy adott személyiségről vagy annak jelentős részéről. A számítógép mellett az alkotmánybíróság példalázó jelleggel említi a mobiltelefont vagy az elektronikus határidőnaplót.⁴⁶

A felhasználóknak érdekük, hogy adataik bizalmasak maradjanak, emellett megjelenik egy általános elvárás a bizalom és az integritás garanciája iránt. A két érdek nem azonos, és nem feltétlenül esik egybe. A Német Szövetségi Alkotmánybíróság döntésének újdonsága tulajdonképpen a „bizalmasság” jogosultságként történő elismerésében rejlik. A lakással összefüggő bizalmassági követelmény a 13. cikk, a kommunikáció meghatározott formáival szembeni bizalmassági követelmény a 10. cikk hatálya alá esik. Az alkotmánybíróság ezzel a döntésével gyakorlatilag kiterjesztette a bizalmassági követelmények körét. Egy olyan rendszert, amely nagy mennyiségű és sokféle személyes adatot tartalmaz vagy tartalmazhat, megillet az alapjogvédelem még akkor is, ha a rendszer az említett adatmennyiséget nem tartalmazza. Az új alapjog tulajdonképpen az érintett személy személyiségének kifürkészése ellen nyújtana védelmet.⁴⁷

Az általános személyiségi jognak ezért garantálnia kell az információs technikai rendszer integritásának és bizalmasságának védelmét. Ez a jog az információs önrendelkezéshez való jogon alapszik, védi az alapjog jogosultjának személyes és magánéleti viszonyait az információs technika révén történő állami beavatkozásoktól. Fontos kiemelni az „állami” jelzőt, ugyanis a magánszemélyek beavatkozásától az információs önrendelkezéshez való jog véd.

45 Burkhard Hirsch: i. m. 1910. o.

46 1 BvR 370, 595/07 vom 27. Februar 2008, 203. A mobiltelefonokkal kapcsolatban azonban meg kell jegyezni, hogy az újabb modellek már „kis” számítógépnek felelnek meg, mert alkalmasak internetezésre, kép- és hangfelvétel rögzítésére, illetve GPS-adatok tárolására.

47 Gabriele Britz: i. m. 411. o.

Az „IT-alapjog” feladata tulajdonképpen a magánszféra olyan részének védelme, amelynek alapjogvédelmi igénye jobban garantált az új alapjog által, mint az információs önrendelkezéshez való jog segítségével. Az új alapjog akkor jöhet számításba, ha a másik három alapjog – az információs önrendelkezéshez való jog, a magánlakás sérthetlensége, a privátszféra védelme – egyike sem nyújt megfelelő védelmet. A védelem az információs technikai rendszer egészébe történő beavatkozásra is kiterjed, nemcsak az egyes kommunikációs folyamatok vagy a mentett adatok lehetnek a védelem tárgyai.

Az információs technikai rendszer bizalmosságának és integritásának védelméhez való jog korlátozhatósága

Az információs rendszer bizalmosságának és integritásának védelme nem korlátozhatatlan.⁴⁸ A beavatkozás preventív és bűnüldözési céllal is történhet. A korlátozásoknak azonban meg kell felelniük az alkotmányos követelményeknek, így különösen a normavilágosság és az arányosság elvének. A normavilágosság a jogállamiság elvéből vezethető le. A normavilágosság elve értelmében az alapjogkorlátozásról szóló lényegi döntések körét és azok hatályát a demokratikusan legitímált törvényhozónak kell meghatároznia, s erre alapozva rendelhet el a kormány és a közigazgatás törvény által irányított és behatárolt intézkedéseket. A jogi kontrollt a bíróság gyakorolja. A tágabb értelemben vett normavilágosság elvébe beletartozik, hogy az érintett személy tisztában van a jogi helyzetével, ezáltal fel tud készülni a lehetséges korlátozó, terhelő intézkedésekkel kapcsolatos védekezésre.⁴⁹

Az arányosság elve értelmében az alapjogi beavatkozásnak 1. legitím célt kell szolgálnia; 2. a cél elérésére alkalmasnak; valamint 3. ahhoz szükségesnek; és 4. arányosnak kell lennie.⁵⁰ A törvényhozó feladata az alapjogkorlátozás érdekeinek és a korlátozás súlyának megfelelő szintű egymás mellé rendelése. Előfordulhat, hogy egy intézkedést nem lehet az általános érdekek védelmében alkalmazni, mert az abból következő alapjogi korlátozások súlyosabbnak tekintendők, mint az érvényesítendő érdekek védelme.

1. Az online házkutatás *legitim cél*, a szabad, demokratikus társadalmi rend, a szövetségi rendszer és a tartományok fennállásának, Németország érdekeinek védelmében⁵¹ történhet, hogyha közvetlenül fenyegető, konkrét veszélyhelyzet áll

48 1 BvR 370, 595/07 vom 27. Februar 2008, 201, 207.

49 1 BvF 3/92 vom 03. 03. 2004, BVerfGE 110, 33 [52].

50 1 BvR 1084/99 vom 03. 03. 2004, BVerfGE 109, 279 [335].

51 Az állam biztonsága, a béke, a rend, a népesség biztonsága, az emberi test és élet a legmagasabban védett érdekek közé tartoznak. BVerfGE 49, 24 [56]; BVerfGE 115, 320 [346].

fenn. A „konkrét veszélyhelyzet” azt jelenti, hogy nagy valószínűséggel megállapítható, állami beavatkozás nélkül belátható időn belül kár következne be a felsorolt védett jogtárgyakkal kapcsolatban. A veszély bekövetkezésének időbeli közelsége nem feltétel.⁵²

2. Az *alkalmasság* feltétele akkor teljesül, ha az adott intézkedés alkalmas a megfogalmazott cél elérésére. Az *alkalmasság* nem követeli meg, hogy az intézkedések mindig vagy többnyire sikeresek legyenek, elegendő az a törvényhozói prognózis, hogy egyedi esetekben a beavatkozás sikerrel járhat.⁵³ Az online házkutatás alkalmas a felsorolt védett jogtárgyakkal kapcsolatos veszélyhelyzet megelőzésére, *alkalmasságát* nem érinti az a tény, hogy az érintett személyeknek lehetőségük van az információs technikai eszközökbe történő beavatkozással szembeni védekezésre, adott esetben a szoftverrel történő beavatkozás megakadályozására.
3. Az intézkedés *szükségessége* azt jelenti, hogy az a lehető legkisebb korlátozást valósítja meg a cél elérése érdekében, azaz nincs olyan megoldás, amely a cél elérésére alkalmas és az érintettek jogait kevésbé korlátozná. A német alkotmánybíróság álláspontja szerint az online házkutatás szükséges, megfelelő intézkedésnek tekinthető, mert nem ismert olyan megoldás, amely a cél elérésére ugyanilyen hatékony lenne, de az érintettre nézve kisebb jogkorlátozással járna.
4. A szűkebb értelemben vett *arányosság elve* megköveteli, hogy az intézkedés által okozott alapjogi korlátozások arányban álljanak az elrendelés indokaival.⁵⁴ A szövetségi alkotmánybíróság álláspontja szerint azonban az online házkutatás jelenlegi szabályozása nem felel meg a szűkebb értelemben vett arányosság elvének, mert az olyan intenzív alapjogi korlátozásokkal jár együtt, amelyek nem állnak arányban az elrendelés indokál szolgáló általános nyomozási érdekekkel; különös tekintettel az intézkedés időtartamára, az adatanyag terjedelmére, a titkosságra, valamint a független kontroll, azaz az intézkedés bírói engedélyhez kötöttsége hiányára.⁵⁵ Az általános társadalmi érdekek nem igazolják az abszolút védelem alatt álló, a személyiség szabad kibontakoztatásához fűződő jog korlátozását. A határozat összességében megállapította, hogy az online házkutatás németországi szabályozása nem tartalmaz megfelelő garanciákat az online házkutatás elrendelésének tényleges okaira, a jogvédelemre, valamint a magánélethez való jog védelmére vonatkozóan.

52 1 BvR 370, 595/07 vom 27. Februar 2008, 251. Vö.: Gabriele Britz: i. m. 414. o.

53 1 BvR 370, 595/07 vom 27. Februar 2008, 222.

54 2 BvL 43/92 vom 09. 03. 1994, BVerfGE 90, 145 [173]; 1 BvR 1084/99 vom 03. 03. 2004, BVerfGE 109, 279 [349].

55 1 BvR 370, 595/07 vom 27. Februar 2008, 228.

Az online házkutatás által megvalósított állami adatszerzés jelentős potenciált teremt az érintett személyiségének kifürkészésére. Az információs technikai rendszer komplex felhasználási lehetőségei következtében a célrendszer adatállománya az érintettre vonatkozó személyes adatokat, naplószerű feljegyzéseket, képeket, hangfelvételeket tartalmazhat. Az adatok önmagukban vagy összességükben utalhatnak az érintett személy személyiségére, személyes életviszonyaira vagy életmódjára. A beavatkozás intenzitását befolyásolja a megfigyelés időtartama és titkossága. Szakértők szerint az intézkedés olyan károkozással is együtt járhat, amely nem áll összefüggésben a nyomozással. Akár az eljáró hatóságok, akár harmadik személy visszaélhet a hozzáférést lehetővé tevő programmal, manipulálhatja, törölheti, megváltoztathatja az adatokat vagy újakat hozhat létre.⁵⁶

Összességében az online házkutatás bevezetésének szükségessége erősen vitatott, mert nagyon erős az alapjogokba történő beavatkozás, és az intézkedés alkalmazása kapcsán olyan visszaélésekre van lehetőség, amely harmadik személyeket is érinthet. Alkotmányjogi szempontból azonban nem jelenthető ki teljes bizonyossággal, hogy az online házkutatás mint nyomozási eszköz általában véve alkotmányellenes lenne. Az új „IT-alapjog” viszont nagyon körültekintő szabályozást igényel a törvényalkotó részéről. Az online házkutatás kizárólag különösen fontos jogi érdek közvetlen fenyegetettsége esetén bírói engedéllyel alkalmazható, ha a szabályozás átlátható, egyértelmű, és megfelel a normavilágosság követelményének.⁵⁷

A német alkotmánybíróság készletező adattárolással kapcsolatos
1 BvR 356/08, 1 BvR 263/08, 1 BvR 586/08 számú, 2010. március 2-i döntése

Az alkotmánybíróság határozatának bevezetőjében kifejtette, hogy nem a szóban forgó 2006/24/EK irányelv, hanem az irányelvet átültető nemzeti jogszabály alkotmányosságát vizsgálja. Megállapította, hogy az irányelvben foglalt célkitűzéseket és szabályokat összeegyeztethetőnek tartja az alkotmánnyal, ezért nem fordult az Európai Unió Bíróságához előzetes döntéshozatali kérelemmel.

A telekommunikációs titokhoz fűződő jog érintettsége

A német alkotmány 10. cikke az információs önrendelkezéshez való joghoz képest speciális, ezért a készletező adattárolással összefüggésben az alkotmánybíróság a telekommunikációs titokhoz fűződő jog érintettségét vizsgálta. Formális szempont-

⁵⁶ 1 BvR 370, 595/07 vom 27. Februar 2008, 231–232, 240.

⁵⁷ 1 BvR 370, 595/07 vom 27. Februar 2008, 207, 247, 257.

ból a támadott rendelkezések nem alkotmányellenesek, mert a korlátozó szabályokat megfelelő jogforrási szinten, törvényben fogadta el a jogalkotó, emellett az adott terület szabályozása szövetségi hatáskörbe tartozik.⁵⁸

A 10. cikk által biztosított védelem nemcsak a kommunikáció tartalmára terjed ki, hanem a kommunikációs folyamat körülményeinek bizalmasságára, különösen arra, hogy mely személyek mikor és milyen gyakran vesznek részt telekommunikációs folyamatokban. A telekommunikációs jog törvény által korlátozható. Alapjogkorlátozást jelent a közhatalom által történő minden ismeretszerzés, feljegyzés, adatkezelés, illetve az adatok vagy a tartalom értékelése. A 10. cikk nem tilt meg minden mentésre vagy adatkezelésre irányuló tevékenységet, hanem a cél nélküli, aránytalan adatgyűjtéstől véd. Szigorúan tiltott ennek megfelelően a személyiséghez kapcsolódó adatok határozatlan és nem meghatározható célból történő gyűjtése és tárolása.

A kifogásolt rendelkezések szerinti készletező adattárolás, az adatok mentése beavatkozás a telekommunikációs titokhoz fűződő jogba, mert az állam kötelezővé teszi a szolgáltatók számára az adatok mentését. Az alapjogsértés nemcsak a mentéssel, hanem az adatok továbbításával kapcsolatban is fennáll. A döntés értelmében tehát a kifogásolt szabályok sértik az alkotmány 10. cikkében foglalt telekommunikációs titokhoz fűződő jogot.

A jogkorlátozás arányosságának kérdése

1. Az alkotmánybíróság ezen a ponton megállapította, hogy a hat hónapig tartó, privát szolgáltatók által történő készletező adattárolás önmagában nem összeegyeztethetetlen a német alkotmány 10. cikkével. A bűnüldözés hatékonyságának növelése, a veszély elhárítása és a titkosszolgálatok feladatainak teljesítése olyan legitim célok, amelyek érdekében a telekommunikációs titokhoz való jog alapvetően korlátozható.⁵⁹
2. Az alkotmánybíróság véleménye szerint a készletező adattárolás alkalmas a bűnüldözési és veszélyelhárítási célok elérésére. Az alkalmasság kritériumával kapcsolatban ismételtelen kiemelték annak fontosságát, hogy az intézkedésnek nem kell minden esetben sikeresnek lennie. Ha az potenciálisan alkalmas a cél elérésére, akkor teljesül az alkalmasság kritériuma.
3. A testület álláspontja szerint a szükségességi feltétel is teljesül, mert jelenleg nem ismert más olyan eszköz, amely kisebb jogkorlátozással ugyanazon eredmény eléréséhez vezetne, mint a készletező adattárolás.

⁵⁸ 1 BvR 356/08, 1 BvR 263/08, 1 BvR 586/08 vom 2. März 2010, 93–96, 181–183, 197.

⁵⁹ 1 BvR 356/08, 1 BvR 263/08, 1 BvR 586/08 vom 2. März 2010, 204–206.

4. Mindazonáltal látni kell, hogy a készletező adattárolás nagyon erőteljes alapjogi beavatkozás. Az adatgyűjtéssel szorosan összefügg a visszaélések lehetősége, amely fokozottan fennáll abban az esetben, ha az adatgyűjtést magán- és nem állami szolgáltatók végzik. A Szövetségi Alkotmánybíróság megállapította, hogy a készletező adattárolás ezért csak abban az esetben felel meg a szűkebb értelemben vett arányosság elvének, ha megfelelő szabályozást tartalmaz a) az adatbiztonságra; b) az adatok felhasználásának terjedelmére; c) az átláthatóságra és a jogvédelemre.
- a) Az adatbiztonságra vonatkozó szabályok megalkotásánál figyelembe kell venni a technika jelenlegi állását. A jogalkotó szabadon alakíthatja ki az adatbiztonságra vonatkozó technikai szabályokat, azonban fontos, hogy azokat átláthatóvá és egyértelművé tegye a szolgáltatók számára, valamint biztosítsa a megfelelő ellenőrzést és a hatékony szankcionálást a szabályok be nem tartása esetére. A kifogásolt szabályok nem teremtenek kiegyenlített szankciórendszer, mert az adatbiztonságra vonatkozó szabályok megsértésének szankciói enyhébb súlyúak a tárolásra vonatkozó kötelezettség megszegésének szankcióinál.
- b) Az adatok felhasználását a legszűkebb területre kell korlátozni, emellett terület-specifikus, precíz és egyértelmű szabályokat kell kialakítani. Az alkotmánybíróság véleménye szerint a büntetőeljárás normák akkor lesznek összeegyeztethetők az alkotmánnyal, ha nemcsak utalásszerűen, hanem taxatív meghatározzák azoknak a különös jelentőségű bűncselekményeknek a körét, amelyek esetén az így szerzett adatok felhasználhatók a büntetőeljárásban. Az adatok felhasználása abban az esetben lesz alkotmányos, ha kiemelkedően fontos jogi érdekek konkrét veszélyeztetése esetén a veszély elhárítása céljából történik. Ilyen kiemelkedő fontos jogi érdekek a személyek testi épsége, élete vagy szabadsága, valamint Németország vagy valamely tartomány biztonsága. A veszéllyel kapcsolatban az alkotmánybíróság az online házkutatásra vonatkozó döntésében foglaltakat tekinti irányadónak. Kiegészítette azonban a követelményrendszerrel azzal, hogy az adatokat a továbbítás után haladéktalanul értékelni, és amint a felhasználás célja megszűnt, azonnal törölni kell. Garanciális követelmény, hogy az adatok továbbításáról és felhasználásáról jegyzőkönyvet kell készíteni.⁶⁰
- c) Fő szabályként az adatokat lehetőleg nyíltan, az érintett tudtával kell kezelni, ám ha ez nem lehetséges, akkor az érintettet legalább utólag értesíteni kell az intézkedés végrehajtásáról. Azokról a kivételes esetekről, ha az érintett nem ér-

tesíthető, bírónak kell döntenie. A bírói mérlegeléshez kijelölt orientációs pont, hogy az értesítés akkor mellőzhető, ha a közlés valaki életének, testi épségének veszélyeztetésével járna.

A jogsértések esetére előírt szankciókról bírósági határozatban kell rendelkezni, mert a bíró függetlensége és törvényhez kötöttsége garantálja az érintett jogainak tiszteletben tartását. További garanciális rendelkezés a bírósági határozatok részletes indokolása. Törekedni kell arra, hogy a törvény valamennyi jogsértést szankcionáljon, a törvény be nem tartása, vagy jogosulatlan személyek adatszerzése ne maradjon jogkövetkezmények nélkül.⁶¹

Az állampolgár számára előzetes és folyamatos védelmet jelent tehát az engedélyezés feltételeinek törvényi szintű, az előbbi követelményeket kielégítő szabályozása, a bírói beavatkozás és ellenőrzés, utólagos védelmet pedig a jogsértések kellő súlyú szankcionálása.

Az alkotmánybíróság álláspontja szerint a telekommunikációról szóló törvény jelenlegi szabályozásából hiányzik a különösen magas biztonsági feltételek és a megfelelő adatbiztonsági előírások szavatolása. Nem biztosítja a szabályozás a kiegyenlítő szankciórendszert sem, mert az adatbiztonság megsértését sokkal kevésbé szankcionálják, mint a mentési kötelezettség elmulasztását.⁶²

Az adatok továbbítására vonatkozó szabályok sem felelnek meg az alkotmányossági követelményeknek. Az adatok továbbítása alapvetően bűnüldözési céllal történhet, azonban hiányzik az alapul szolgáló bűncselekmények taxatív felsorolása. A törvény csak azt tartalmazza, hogy a súlyosabb bűncselekmények és a telekommunikációs rendszerekkel összefüggő bűncselekmények esetén kerülhet sor az adatok továbbítására. Ez a megfogalmazás praktikusán valamennyi bűncselekmény esetén lehetővé teszi az adatok továbbítását és felhasználását. Az értesítési kötelezettség sem tekinthető alkotmányosnak, mert a német büntetőeljárás törvényi szabályai szerint az érintett utólagos értesítése mérlegelésen alapul.

A határozathoz fűzött különvélemények

A döntéshez két alkotmánybíró különvéleményt fűzött.⁶³ Álláspontjuk szerint a készletező adattárolás eleget tesz az arányosság követelményének, különös tekintettel arra, hogy a telekommunikációs titok védelme alapvetően az állami ismeretszerzés

61 1 BvR 356/08, 1 BvR 263/08, 1 BvR 586/08 vom 2. März 2010, 239, 247–248.

62 1 BvR 356/08, 1 BvR 263/08, 1 BvR 586/08 vom 2. März 2010, 269.

63 Schluckebier és Eichberger alkotmánybírák. 1 BvR 356/08, 1 BvR 263/08, 1 BvR 586/08 vom 2. März 2010, 310–345.

ellen nyújt védelmet, az adattárolási kötelezettséget pedig magánszolgáltatók számára írták elő. Mindezek alapján – véleményük szerint – a készletező adattárolás nem valósít meg különösen erőteljes alapjog-korlátozást. Az állampolgárok jogainak védelme, illetve az állam bűnüldözési kötelezettsége közötti összhang és egyensúly ugyanis az intézkedés által garantált; az elérni kívánt cél tekintetében pedig arányosnak tekinthető az egyén alkotmányos alapjogainak korlátozása. Hangsúlyozták: fontos, hogy megfelelő kereteket teremtsenek az érintett személyek jogvédelmének, de a bűnüldözés számára is gondoskodni kell azokról a hatékony eszközökről, amelyek a technikai fejlődés miatt állandóan változnak.

A különvélemények nem tartják alkotmányosan aggályosnak, ha bizonyos alapjog-korlátozó intézkedésre nem taxatívén felsorolt bűncselekmények esetén kerülhet sor, hanem a jogalkotó csak a veszélyeztetett érdekekkel írja körül a bűncselekményi kört. Álláspontjuk szerint indokolt a telekommunikációval összefüggő bűncselekmények felderítésére a telekommunikációs eszközök igénybevételeének lehetősége, amelyek hiánya nagyban megnehezítené vagy esetleg ellehetetlenítené az ilyen jellegű bűncselekmények felderítését.⁶⁴

Hangsúlyozzák emellett, hogy az StPO további feltételként rögzíti: csak abban az esetben kerülhet sor az intézkedésre, ha az információk más módon nem deríthetők ki, vagy felderítésük aránytalan nehézségekkel járna, illetve kilitáztatlan lenne. Véleményük szerint ez a szubszidiárius feltétel szavatolja az intézkedés alkalmazásának arányosságát. Az értesítési kötelezettséggel kapcsolatban kiemelik, hogy az utólagos értesítési kötelezettség, illetve az értesítési kötelezettség korlátozása a titkos nyomozási eszközöknél alapvetően jellemző, és maga az alkotmánybíró is több döntésében elismerte, hogy a nyomozás során bizonyos esetekben indokolt a titkosság és a titkos eszközök alkalmazása.⁶⁵

Az online házkutatás új szabályozása Németországban

2008. november 27-én az Európai Unió Tanácsa elfogadta az internetes bűnözés elleni küzdelemről szóló stratégiát.⁶⁶ A tervek szerint a következő öt évben olyan operatív intézkedéseket hajtanának végre, mint az internetes folyamatok megfigyelése, elektronikus házkutatás lefolytatása, illetve közös nyomozó csoportok együttműködése. Konkrét intézkedésként irányozták elő a kölcsönös együttműködés és

64 1 BvR 356/08, 1 BvR 263/08, 1 BvR 586/08 vom 2. März 2010, 313, 317–325.

65 1 BvR 356/08, 1 BvR 263/08, 1 BvR 586/08 vom 2. März 2010, 331–335.

66 Sajóközlemény: „Kampf gegen die Internet-Kriminalität: Cyber-Patrouillen und Internet-Untersuchungen unterstützen die EU-Strategie. Brüssel, 27. November 2008 IP/08/1827.

az információcserre továbbfejlesztését. A stratégia lehetséges eszközként említi a határon átnyúló online kutatásokat, amennyiben az adott tagállam jogi szabályozása azt lehetővé teszi.

Németországban a belügyminiszter és az igazságügy-miniszter hosszas vitája után 2008. szeptember 15-én terjesztették a Bundestag elé a nemzetközi terrorizmus elleni védekezésről szóló törvény tervezetét.⁶⁷ A javaslatot kisebb változtatásokkal a Bundestag 2008. november 12-én jóváhagyta, november 28-án azonban a Bundesrat elutasította.⁶⁸ Kompromisszumos megoldásként fogadták el 2008. december 17-én a BKA-törvény újabb módosítását, amely 2009. január 1-jén lépett hatályba.⁶⁹

A módosítás egyebek között kivételesen, bírói engedéllyel lehetővé tette a Szövetségi Bünyügyi Hivatal számára az online házkutatás lefolytatását.⁷⁰ A törvény először teremtette meg a preventív rendőrségi intézkedések lefolytatásának jogalapját. Ez azt jelenti, hogy a nyomozó hatóság nem közvetlenül a meghatározott, releváns veszélyekre reagál, hanem a konkrét veszély vagy bűncselekmény gyanúját megelőzően információszerezés céljából tevékenykedik, azaz úgynevezett proaktív nyomozást folytat.⁷¹

A BKA a nemzetközi szervezett bűncselekmények⁷² absztrakt veszélye esetén illetékes bűnüldöző hatóság. Ha konkrétan felmerül ilyen jellegű bűncselekmény elkövetésének gyanúja, a szövetségi főügyészség jár el.⁷³ A nemzetközi szervezett bűnözés már a bűncselekmények tervezési fázisában is rendkívüli veszélyekkel járhat, ezért tűnik indokoltnak az ilyen absztrakt veszélyekkel szemben a megelőző intézkedések foganatosítása. Az ügyészség hatáskörének „elvonása” és „áttétele” egy szövetségi szintű nyomozó hatósághoz csak különösen indokolt esetben történhet, ezért is hangsúlyozza a törvény az online házkutatás kivételes jellegét.

A BKA az érintett tudta nélkül megfigyelheti az adott személy által használt információs technikai rendszert, onnan adatokat szerezhet meg, ha az emberi élet vagy szabadság elleni bűncselekmény elkövetésének veszélye áll fenn, illetve olyan általános közjavak „konkrét” veszélyeztetése merül fel, amelyek érinthetik az

67 „Entwurf eines Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt” [BT-Drs 16/9588].

68 Németországban az alkotmány határozza meg, hogy melyek azok a törvényhozási tárgykörök, amelyben a Bundestag és a Bundesrat együttes hozzájárulására van szükség. Ilyen úgynevezett hozzájárulási eljárás [Zustimmungsverfahren] keretében tárgyalták az új terrorizmusellenes törvény tervezetét [GG 77. cikk].

69 Neuregelung des BKA-Gesetzes in Kraft getreten. Neue Juristische Wochenschrift-Spezial, 2009, S. 58.

70 A BKA-törvény 20k §-a szabályozza az információstechnikai rendszerbe történő tiltkos beavatkozás lehetőségét.

71 Frederik Roggan: Das neue BKA-Gesetz – Zur weiteren Zentralisierung der deutschen Sicherheitsarchitektur. Neue Juristische Wochenschrift, 2009, S. 257.

72 Német büntető törvénykönyv. Strafgesetzbuch vom 13. 11. 1998 (StGB) 129a §, 129b §.

73 Frederik Roggan: i. m. 258. o.

állam és az emberi lét alapjait. További feltétel, hogy az intézkedés által bekövetkező jövőbeni károkozás valószínűsége csekély, valamint az említett közvetlen veszély elhárításához a cselekmény feltétlenül szükséges, más módon az elhárítás nem lehetséges, vagy aránytalan nehézségekbe ütközne.⁷⁴

Az online házkutatás technikai végrehajtásának részletszabályait a törvény nem tartalmazza, azonban – az alkotmánybíróság online házkutatásról szóló határozatában foglaltaknak megfelelően – a lakásba vagy helyiségbe történő fizikai behatolás tiltott. Az interneten keresztüli beavatkozás előnye abban rejlik, hogy minimálisan csökken annak a veszélye, hogy a megfigyelt személy felfedezi a szoftvert. Továbbra is probléma lehet azonban, hogy (technikailag) nem zárható ki annak lehetősége, hogy harmadik, az eljárásban nem érintett személyeket is megfigyeljenek.

Az online házkutatás elrendelése írásban történik, és maximum három hónapra szólhat. Hogyha az elrendelés feltételei továbbra is fennállnak, az engedély még egy, maximum három hónapos időtartamra meghosszabbítható. Ellenkező esetben az intézkedés végrehajtását haladéktalanul meg kell szüntetni.

A törvény leszögezi, hogy a tárolt adatokat nem lehet módosítani, törölni vagy továbbítani. Ennek garantálására valamennyi, a technika jelen állása szerinti megoldást alkalmazni kell. Jegyzőkönyvben kell rögzíteni a beavatkozás kezdő időpontját és időtartamát, az információs technikai rendszer azonosításához szükséges adatokat, valamint azt a szervezetet, amely az intézkedést végrehajtotta. A jegyzőkönyvet csak akkor lehet felhasználni, ha az adott eljárásban az intézkedéssel szerzett adatok bizonyítási eszközként szerepelnek, egyébként a jegyzőkönyvet az adott naptári évet követő egy évig kell megőrizni, és utána automatikusan törölni kell, kivéve ha az intézkedés elrendelésének és fenntartásának céljai továbbra is fennállnak.⁷⁵ Az online házkutatás azonban ebben az esetben is csak a törvény által előírt három, illetve hat hónapig tarthat.

Az információs technikai rendszerbe történő titkos beavatkozás csak bírói engedéllyel végezhető. Az intézkedést a BKA vezetője vagy annak képviselője indítványozhatja az illetékes bíróságnál. A Német Szövetségi Alkotmánybíróság 2008. februári döntésében a bírói engedélynek tulajdonította a legnagyobb jelentőséget az online házkutatás alkotmányossági vizsgálata során, mert a titkos nyomozási intézkedések olyan erős alapjogi korlátozásokkal járnak, amely szükségessé teszi egy független fórum kontrollját.

A BKA-törvény 20k §-a tartalmazza a magánszféra védelmére vonatkozó garanciális rendelkezéseket is, és a Német Szövetségi Alkotmánybíróság által kidolgozott

⁷⁴ BKA-törvény 20k § (1) bekezdés.

⁷⁵ BKA-törvény 20k § (3) bekezdés.

ügynevezett „kétfélcpsős védelmi koncepciót”⁷⁶. Az első lépcső az adatok felhasználásának tilalma, amennyiben a személyiség szabad kibontakoztatásához fűződő jog területére tartozó adatok érintettsége merül fel. Ha megalapozottan feltehető, hogy az intézkedéssel szerzett adatok a személyiség szabad kibontakoztatásához való jog területéhez tartoznak, akkor az intézkedést nem lehet elrendelni.

A második lépcső a mentett adatok átvizsgálását és a magánszféra területére tartozó adatok védelmét szolgálja. Amennyire lehetséges, technikailag biztosítani kell, hogy ilyen jellegű személyes adatok rögzítésére ne kerüljön sor. Ennek megfelelően a mentett és tárolt adatokat a BKA adatvédelmi felelőse és további két BKA-tisztviselő átvizsgálja az illetékes bíróság felügyelete mellett. A szabályozás azonban nem rendelkezik arról, hogyan kapcsolódik be az illetékes bíróság az ellenőrzési folyamatba. A személyes adatokat az eljárás során nem használhatják fel, és haladéktalanul rendelkezni kell a törlésükről, ami dokumentálandó. Ez a dokumentáció kizárólag adatvédelmi ellenőrzés céljára szolgálhat. Az adatokat legkésőbb a dokumentációt követő év végéig törölni kell, ha azok megőrzése az adott adatvédelmi cél eléréséhez már nem szükséges.⁷⁷

A BKA 2009. októberi közleménye szerint addig egyetlen esetben sem indítványozták online házkutatás lefolytatását a bíróságoknál. A BKA az online házkutatást elengedhetetlenül szükséges nyomozási eszköznek tartja a terrorizmus ellen folytatott küzdelemben, de az intézkedés csak speciális esetben alkalmazható, ezért eddig nem került rá sor. A kritikusok szerint azonban azért nem alkalmazták, mert a szükséges technikai háttér még nem áll rendelkezésre.

Bajorországban a BKA-törvény módosításával még 2008-ban megalkották az online házkutatás végrehajtásával kapcsolatos tartományi szintű szabályokat. A bűnüldözési célú online házkutatás végrehajtásáról szóló külön törvényt 2008. július 4-én nem szavazta meg a tartományi parlament, így a meglévő törvény módosításával kellett a megfelelő szabályozást kialakítani.⁷⁸ Rajna-Pfalz a második tartomány, ahol az online házkutatás lehetővé válhat. Az erről szóló törvényjavaslat végleges szövegét 2010. augusztus 18-án fogadták el, a tartományi parlament decemberben fog róla szavazni.⁷⁹ Az online házkutatásról szóló szabályok a tervek szerint 2011. január 1-jén léphetnek hatályba.

⁷⁶ Frederik Roggan: i. m. 259–261. o.; Vö.: 1 BvR 370, 595/07 vom 27. Februar 2008, 207.

⁷⁷ BKA-törvény 20k § [7] bekezdés.

⁷⁸ Lásd Gesetz über die Aufgaben und Befugnisse der Bayerischen Staatlichen Polizei – Polizeiaufgabengesetz (PAG) vom 17. September 1990, Art. 34d: „Verdeckter Zugriff auf informationstechnischer Systeme”. Vö.: Robert Käß: Die Befugnis zum verdeckten Zugriff auf informationstechnische Systeme im bayerischen Polizeiaufgabengesetz., BayVBl 2010, 1; BeckOK StPO § 100a I. 111c.

⁷⁹ Gesetzentwurf der Landesregierung zur Änderung des Polizei- und Ordnungsbehörden-gesetzes Drucksache 15/4879.

A BKA-törvény módosításával szemben még 2009 áprilisában újabb két alkotmányjogi panaszt nyújtottak be arra hivatkozva, hogy az még mindig nem tesz eleget maradéktalanul a Német Szövetségi Alkotmánybíróság 2008. februári döntésében foglaltaknak. Az alkotmánybíróság eljárása még folyamatban van.

Zárszó

„Egy állami intézkedés alapvetően nem felel meg az arányosság elvének, ha annak az érintett személyiségének teljes kifürkészése az ára.”⁸⁰ Ez a gondolat a Német Szövetségi Alkotmánybíróság online házkutatással és készletező adattárolással kapcsolatos határozatában is jelen van. Az online házkutatás nem azonos a telekommunikációs adatok készletezési és tárolási kötelezettségével, de mindkét intézkedés veszélyeztetheti az információs technikai rendszer integritásához fűződő bizalmat. Az alkotmánybíróság önmagában sem az online házkutatást, sem a készletező adattárolást nem tekinti alkotmányellenesnek, a megfelelő garanciákkal az intézkedések összeegyeztethetők lehetnek a német alaptörvénnyel.

A technika és technológia fejlődése szükségessé teszi az eddigi jogi megoldások felülvizsgálatát, az új jelenségekhez való alkalmazkodást. Egy ilyen fejlődési irány mutatkozik meg a Német Szövetségi Alkotmánybíróság gyakorlatában az új IT-alapjog kialakításával és az elektronikus alapú nyomozási intézkedések létjogosultságának elismerésével kapcsolatban. A bűnözés új formáinak kialakulása magával hozza az új nyomozási intézkedések szükségességét. Az újfajta bűnözés új veszélyt jelent az egyének és a társadalom számára, ami megalapozhatja az egyéni alkotmányos jogok korlátozásának szükségességét.

Az alkotmányos jogok korlátozásakor azonban meg kell felelni az alkotmány, illetve az alkotmánybíróság által megfogalmazott alkotmányos követelményeknek. Az állam feladata az új bűnözéssel kapcsolatos közösségi bűnüldözési érdek és az egyéni jogok védelme közötti konfliktus feloldása. Fontos azonban megjegyezni, hogy mindkét alkotmánybírósági döntés előrevetíti a szabályozó és gondoskodó állam, valamint az „orwelli” felügyelő állam közötti határvonal elmosódásának lehetőségét⁸¹, amely gondolat felveti azt a kérdést, hogy meddig terjedhet az állam „totális” ellenőrzése a társadalom védelme érdekében.

80 1 BvR 370, 595/07 vom 27. Februar 2008, 248.

81 Dirk Uwer: George Orwells „1984” – Antiutopie und Totalitarismuswarnung zwischen 1949 und 2009. Neue Juristische Wochenschrift, 2009, S. 723.