A Német Szövetségi Köztársaság Alkotmánybíróságának
2008. február 27-én kelt ítélete

Az Első Szenátus 2008. február 27-én kelt ítéletének alapelvei

1. Az általános személyiségi jog (Alaptörvény[1] 2. cikk (1) bekezdés az 1. cikk (1) bekezdésével összefüggésben) felöleli az információtechnikai rendszerek bizalmas volta és sérthetetlensége biztosításának alapjogát.

2. Egy információtechnikai rendszerbe való titkos betelepülés, melynek révén a rendszer használata megfigyelhető és adathordozói kiolvashatók, alkotmányjogilag csak akkor megengedhető, ha tényleges támpontok merülnek fel egy túlnyomóan jelentős jogtárgy konkrét veszélyeztetésére vonatkozóan. Túlnyomóan jelentős a személy testi épsége, élete és szabadsága vagy olyan közösségi javak, melyek fenyegetése az állam alapjait vagy fennállását, vagy az ember egzisztenciájának alapjait érintik. Az intézkedés jogilag már akkor is igazolható, ha megfelelő valószínűséggel még nem állapítható meg, hogy a veszély a közeli jövőben fellép, amennyiben bizonyos tények egy túlnyomóan jelentős jogtárgyat az adott esetben bizonyos személyek által fenyegető veszélyre engednek következtetni.

3. Egy információtechnikai rendszerbe való titkos betelepülés végrehajtásához elvileg bírósági rendelkezés szükséges. Az ilyen beavatkozásra felhatalmazást adó törvénynek a magánéletvitel belső magját védő intézkedéseket kell tartalmaznia.

4. Amennyiben egy felhatalmazás olyan állami intézkedésre korlátozódik, melynek során a számítógép-hálózaton folyó távközlés tartalmát és körülményeit rögzítik vagy az arra vonatkozó adatokat kiértékelik, a beavatkozást az Alaptörvény 10. cikk (1) bekezdésében foglaltakhoz kell mérni.

5. Ha az állam az arra technikailag alkalmas eszközön folyó Internet-kommunikáció tartalmáról szerez tudomást, egy beavatkozás csak akkor sérti az Alaptörvény 10. cikk 1. bekezdését, ha az állami szervet e tudomásszerzésre a kommunikációban résztvevő nem hatalmazza fel. Ha az állam az Interneten a nyilvánosság számára hozzáférhető kommunikációs tartalmakról szerez tudomást, az alapjogokba elvileg nem avatkozik bele.

[1] Grundgesetz (tkp. Alkotmány)

A nép nevében

Az alkotmányjogi panaszokkal kapcsolatos eljárásban,
melyek benyújtói
1. a) W…. úrnő,
b) B…. úr
meghatalmazottja:
Dr. …. ügyvéd

az ÉWA[2] 5. § 2. bekezdés 1. pontja ellen a 7. § (1) bekezdésével, 5. § (3) bekezdésével, 5a § (1) bekezdésével és 13. §-ával összefüggésben, ahogyan ezt az Északrajna-Westfália alkotmányvédelmi törvényének módosításáról szóló, 2006. december 20-án kihirdetett törvény[3] tartalmazza,

továbbá
2. a) B…. úr
b) Dr. R…. úr
c) S…. úr
meghatalmazottai:
1. ügyvédek ….
2. ügyvéd ……

az ÉWA 5. § (2) bekezdés 11. pontja, 5. § (3) bekezdése, 8. § (4) bekezdés 2. mondata ellen a 10. §, 11§ és 17. § (1) bekezdésével összefüggésben, ahogyan ezt az Északrajna-Westfália alkotmányvédelmi törvényének módosításáról szóló, 2006. december 20-án kihirdetett törvény tartalmazza,

a Szövetségi Alkotmánybíróság Első Szenátusa
Papier elnök, Hohmann-Dennhardt, Hoffmann-Riem, Bryde, Gaier, Eichberger, Schluckebier, Kirchhof, bírónők és bírók szóban lefolytatott tárgyalása alapján, 2007. október 10-én az alábbi

ÍTÉLET

szerint jognak nyilvánította:
Északrajna-Westfália alkotmányvédelmi törvénye[4] 5. § (2) bekezdése 11. pontja a 2008. december 20-ai törvény [5] megfogalmazásában összeegyeztethetetlen az Alaptörvény 2. § (1) bekezdésével összefüggésben az Alaptörvény 1. § (1) bekezdésével, 10. § (1) bekezdésével és 19. § (1) bekezdés 2. mondatával és semmis.
2. Ezzel elintézést nyert a panaszosoknak az Északrajna-Westfália alkotmányvédelmi törvénye 5. § (3) bekezdése és 17. § ellen benyújtott kifogása.
3. Az 1b-ben megnevezett panaszosok alkotmányjogi panaszát az Alkotmánybíróság elutasítja, amennyiben az az Északrajna-Westfália alkotmányvédelmi törvénye 5a § (1) bekezdése ellen irányul.
4. Az alkotmányjogi panaszokat egyebekben az Alkotmánybíróság elutasítja.
5. Északrajna-Westfália tartomány a panaszosok indokolt költségeinek háromnegyed részét tartozik megtéríteni.

[2] Északrajna-Westfália alkotmányvédelmi törvénye
[3] GVBl NW 2006, S. 620
[4] Gesetz über den Verfassungsschutz in Nordrhein-Westfalen
[5] Gesetz- und Verordnungsblatt für das Land Nordrhein-Westfalen, Seite 620

Indokolás

A.

1

Az alkotmányjogi panaszok tárgyát Északrajna-Westfália alkotmányvédelmi törvényének (a továbbiakban: ÉWA) azok az előírásai képezik, amelyek egyrészt az Alkotmányvédelmi Hatóság különféle, különösen információtechnikai (a továbbiakban: IT) rendszerekből való adatgyűjtésre vonatkozó jogosultságokat, másrészt a gyűjtött adatok kezelését szabályozzák.

I.

2

A támadott rendelkezéseket túlnyomóan az Északrajna-Westfália alkotmányvédelmi törvényének módosításáról szóló, 2006. december 20-án kihirdetett törvény[6] iktatta be vagy módosította.

3

1. Mindkét alkotmányjogi panasz kifogásolja az ÉWA 5. § (2) bek. 11. pontjának alkotmányosságát. Ez az előírás a nyomozás két fajtájára hatalmazza fel az Alkotmányvédelmi Hatóságot: egyrészt az Internet titkos megfigyelésére és egyéb felderítésére (1. fordulat), másrészt IT- rendszerekhez való titkos hozzáférésre (2. fordulat).

4

a) Az Internet számítógép-hálózatok elektronikus összessége. Következésképpen IT-rendszerekből áll és ezen felül maga is IT-rendszernek tekinthető. AZ ÉWA 5. § (2) bek. 11. pontjában szabályozott intézkedéstípus a technikai hozzáférés külső megjelenését tekintve az IT-rendszerre irányul. Az Internet titkos felderítésén olyan intézkedést kell érteni, melynek révén az Alkotmányvédelmi Hatóság az Internet-kommunikáció tartalmáról az arra technikailag alkalmas módon tudomást szerez. Északrajna-Westfália tartományi kormánya ilyen intézkedésekről mint szerverorientált Internet-felderítésről beszél.

5

Egy IT-rendszerhez való titkos hozzáférésen ezzel szemben technikai betelepülést kell érteni, amely mintegy kihasználja a célrendszer biztonsági hézagait vagy kémprogramok betelepítésével jár. A célrendszerbe való betelepülés teszi lehetővé használata megfigyelését, sőt még a célrendszer távoli vezérlését is. Északrajna-Westfália tartományi kormánya ilyen intézkedésekről mint az Internet kliensorientált felderítéséről beszél. A támadott előírás egyébként nem utal arra, hogy azok kizárólag egy szerver-kliens-modellre orientált hálózati struktúra keretében alkalmazható intézkedések lehetnek.

6

b) Minthogy az ÉWA 5. § (2) bek. 11. pont 1. mondat 1. fordulata az Internet titkos felderítésére ad felhatalmazást, a norma mindenek előtt azt szabályozza, hogyan jutnak a nyilvánosság számára hozzáférhető kommunikációs tartalmak az Alkotmányvédelmi Hatóság tudomására. Erre példa: hozzáférés ellen nem biztosított weboldalak felkeresése a világhálón web-böngésző segítségével. A törvény indokolása szerint az Alkotmányvédelmi Hatóságot továbbá képessé kell tenni arra, hogy álcázva csevegésekben, árveréseken vagy csereakciókban vegyen részt vagy rejtett weboldalakat felkutasson[7]. Ezen túlmenően az is elképzelhető, hogy az Alkotmányvédelmi Hatóság egyéb úton – például informátortól vagy az un. billentyűzés-naplózás[8] segítségével – megszerzett jelszót használ, hogy egy e-mail postafiókhoz vagy egy hozzáférés-védett weboldalhoz hozzáférjen. Az Alkotmányvédelmi Hatóság ilyen esetekben is az erre szolgáló úton kívül ismeri meg az Internet-kommunikáció tartalmát.

7

---

[6] GVBl NW 2006, S. 620

[7] V. ö. LTDrucks 14/2211, S 17. (a Tartományi Gyűlés dokumentuma, tkp. tartományi közlöny)

[8] Keylogging vagy keystrokelogging

c) AZ ÉWA 5. § (2) bek. 11. pont 1. mondat 2. fordulatában szabályozott, az IT-rendszerekhez való, technikai betelepüléssel végrehajtott hozzáférést a legutóbbi időben a politika és a jogtudomány „online-átkutatás/online-megfigyelés“ címszó alatt behatóan tárgyalja. Egy-egy ilyen intézkedést szövetségi hatóságok már minden különös törvényes felhatalmazás nélkül is végrehajtottak. Az eddigi „online-átkutatások“-ról és eredményeikről keveset tudunk. A szóbeli tárgyaláson a Szenátus meghallgatta a Szövetségi Bűnügyi Hivatal és a Szövetségi Alkotmányvédelmi Hivatal elnökeit, ám ők, minthogy a nyilatkozattételre megfelelő engedélyt nem kaptak, nem adhattak erre vonatkozó tájékoztatást. Ilyen intézkedések végrehajtását egyébként időközben megszüntették, mert a Szövetségi Legfelsőbb Bíróság úgy határozott, hogy ilyen intézkedéseknek a büntetőeljárási rendben nincs jogalapja.

8
aa) A vizsgálat tárgyát képező tartományi norma az első és mindeddig az egyetlen, amely egy német hatóságnak „online-átkutatás“-ra kifejezett felhatalmazás ad. Szövetségi szinten egyelőre vitatott, mely hatóságok és milyen feltételek mellett kaphatnak felhatalmazást „online-átkutatás“-ra. Jelenleg mindenekelőtt azt vizsgálják, kapjon-e ilyen felhatalmazást a Szövetségi Bűnügyi Hivatal a nemzetközi terrorizmus veszélyeinek elhárításával kapcsolatos – az un. föderalizmus reformja keretében az Alaptörvénybe iktatott – feladatai végrehajtásához.

9
bb) Az „online-átkutatás“-nak számolnia kell a nyomozás nehézségeivel, amikor is a – különösen szélsőséges és terrorista körökhöz tartózó – bűnelkövetők bűncselekmények előkészítésével és végrehajtásával kapcsolatos kommunikációhoz IT-eszközöket, különösen az Internetet veszik igénybe. A Szövetségi Bűnügyi Hivatal és a Szövetségi Alkotmányvédelmi Hivatal elnökei szóbeli meghallgatásuk alkalmával elmondták, hogy IT-rendszereket használnak erőszakos terrorista cselekmények előkészítéséhez szükséges, az egész világot átfogó kapcsolatok kiépítésére és fenntartására. A hagyományos módszerekkel végzett nyomozás, pl. IT-rendszerek és tároló eszközök lefoglalása vagy a távközlés egy hálózatra alapozott megfigyelése, különösen ha a szélsőséges vagy terrorista körökhöz tartozó személyek tárolt adataikat és kommunikációs tartalmaikat titkosítják vagy elrejtik, felettébb nehézzé vagy teljességgel lehetetlenné válik.

10
Egy IT-rendszerhez való hozzáférés meglehetős nehézségekkel járhat, különösen ha a célrendszer használója biztonságtechnikai intézkedéseket tett és operációs rendszerét rendszeresen frissíti. A szóban meghallgatott szakértők szerint az érintett a hozzáférést a szóba jöhető betelepülési módok némelyike esetében eredményesen megakadályozhatja. Egy ilyen betelepülés – az adott eset jellemzőitől függően – legalábbis tekintélyes időt vehet igénybe.

11
A sikeres betelepülés a szokásos nyomozási módszerekhez képest számos előnnyel jár. Minthogy a hozzáférés titkos, az érintett – eltérően a nyíltan végrehajtott házkutatástól – azt nem úgy fogja fel, mint figyelmeztetést a jövőre vonatkozóan. Ha adatait egy számítógép használója mindig titkosított formában tárolja, úgy ezekhez az adatokhoz az „online átkutatás“ keretében adott esetben a hatóság dekódolva juthat hozzá, mert a számítógépbe való betelepülés révén az adatokhoz úgy férhet hozzá, ahogyan azokat a használó a kérdéses időpontban kezeli. A titkosítási technika megkerülésének előnyei a folyó Internet-kommunikáció megfigyelésekor is megmutatkoznak. Ha ugyanis titkosítják, mint különösen gyakran a beszédtelefon esetében, azt csak a végfelhasználó készülékén lehet eredményesen megfigyelni. A számítógép használatának tartós megfigyelése révén a titkosítási technológiák és egyéb biztonsági intézkedések hatékonyan megkerülhetők. Mindezen túl mód nyílik olyan illékony adatok megszerzésére is, mint pl. jelszavak és további, az érintett használati szokásaira vonatkozó információk. Ilyesmikhez a klasszikus nyomozási módszerekkel aligha juthatunk.

12
d) Az ÉWA 5. § (2) bek. 11. pontja az Alkotmányvédelmi Hatóságot a szabályozott intézkedésre a hírszerző-szolgálati adatgyűjtésre vonatkozó általános feltételek között hatalmazza fel, melyeket az 5.

§ (2) bek. a 7. § (1) és a 3. § (1) bekezdéssel összefüggésben rögzít. Eszerint alapvető követelmény, hogy ilyen módon alkotmányvédelmi szempontból releváns törekvésre vagy cselekményre, vagy ilyen információszerzéshez szükséges forrásokra vonatkozó információt lehessen szerezni. Ha a támadott norma szerinti intézkedés levél-, posta- vagy távközlési titkot sért vagy jellegét és súlyát tekintve azzal egyenértékű, az csak levél-, posta- vagy távközlési titok korlátozásáról szóló törvény[9] (a továbbiakban: titoktörvény) előírásai betartásával megengedett.

13
e) Csak a 2-ben megnevezett panaszosok kifogásolják az ÉWA 17. §-át az ÉWA 5. § (2) bek. 11. pontjával összefüggésben, amely a személyes vonatkozású adatoknak az Alkotmányvédelmi Hatóság által való továbbítását szabályozza.

14
2. Mindkét alkotmányjogi panasz az ÉWA 5. § (3) bekezdését is támadja. Ennek a rendelkezésnek a tárgya az érintett értesítése arról, hogy alkalmazzák az ÉWA 5. § (2) bekezdésében szabályozott hírszerző-szolgálati eszközöket. E bekezdés 1. mondata az értesítést elvileg kötelezővé teszi, melyek alól a 2. mondat több kivételt tartalmaz.

15
3. Csak az 1-ben megnevezett panaszosok támadják az ÉWA 5a § (1) bekezdését. Ez a rendelkezés felhatalmazza az Alkotmányvédelmi Hatóságot, hogy hitelintézetektől a fizetési forgalomban résztvevőkről és pénzmozgásokról, pénzbeli befektetésekről felvilágosítást szerezzen. Ennek előfeltétele, hogy tényleges támpontok merüljenek fel az alkotmányosan védett jogtárgyak súlyos veszélyeztetésére vonatkozóan.

16
Felhatalmazást számlatartalmak gyűjtésére az alkotmányvédelmi törvény már a 2006. december 20-ai módosítást megelőzően is tartalmazott. A rendelkezés támadott szövegezésében újdonság, hogy számlatartalmak akkor is gyűjthetők, ha tudomást kell szerezni az ÉWA 3. § (1) bek. 1. pontja szerinti törekvésekről, olyanokról ugyanis, amelyek általában a szabad demokratikus alaprend, a szövetség vagy egy tartomány fennállását vagy biztonságát veszélyezteti. A törvény indokolása szerint ez lehetővé teszi, hogy belföldi terrorisztikus hálózatok un. „home-grown-networks“ pézügyi folyamatait felderítsék[10].

17
4. Ugyancsak csupán az 1-ben megjelölt panaszosok támadják az ÉWA 13. § alkotmányellenességét. Ez a norma felhatalmazza az Alkotmányvédelmi Hatóságot, hogy információit más biztonsági hatóságokkal közös adatállományokban feldolgozza. Az adatállományok kezelésének indoka, terjedelme és további követelményei tekintetében a norma egyéb szövetségi és tartományi jogszabályokra utal. E jogszabályokat az 1-ben megnevezett panaszosok egyébként nem tették alkotmányjogi panaszuk tárgyává.

18
5. Csak a 2-ben megnevezett panaszosok támadják az ÉWA 7. § (2) bekezdését. Ez a rendelkezés lakások akusztikai és optikai megfigyelésére hatalmazza fel az Alkotmányvédelmi Hatóságot. A rendelkezés 1994-ben lépett hatályba és az alkotmányvédelmi törvény módosítása is érintetlenül hagyta, s ámbár átdolgozása vagy törlése megfontolás tárgyát képezte, végül is változatlan maradt[11].

19
6. Végül ismét csupán a 2-ben megnevezett panaszosok támadják az ÉWA 10. és 11. §-ban rögzített, az un. elektronikus esetiratok vezetésére vonatkozó szabályozást. Ezek a rendelkezések

[9] Artikel 10-Gesetz - G 10; Gesetz zu Art. 10 Grundgesetz
[10] V. ö. LTDrucks 14/2211, S. 19
[11] V. ö. LTDrucks 14/2211, S. 16

összességükben előírják, hogy azok a személyes vonatkozású adatok, amelyeket ilyen esetiratok tartalmaznak, csak akkor tárolhatók, ha az érintett személyhez magához az Alkotmányvédelmi Hatóságnak nyomozati érdeke már nem fűződik. Így biztosítható, hogy az elektronikusan vezetett esetiratok megfelelnek az elektronikus dokumentumkezelés teljességével szemben támasztott követelménynek. Az adatvédelmi követelmények azáltal teljesülnek, hogy az érintett személyes vonatkozású adatok többé már nem felkutathatók és korlátozás nélküli felhasználásukra sem kerülhet sor.

20
7. Az alkotmányvédelmi törvény [12] a tárgybeli eljárással összefüggésben kivonatosan az alábbi rendelkezéseket tartalmazza:

21
3. §
Feladatok

22
(1) Az Alkotmányvédelmi Hatóság feladata információk gyűjtése és kiértékelése, különös tekintettel olyan tényleges és személyes vonatkozású tartalmakra, hírekre és dokumentumokra, amelyek

23
1. a szabad demokratikus alaprend, a Szövetség vagy egy tartomány fennállása ellen irányuló törekvésekről árulkodnak vagy céljuk a Szövetség vagy egy tartomány vagy tagjaik alkotmányos szervei hivatalos hatáskörei törvényellenes korlátozása,

24
2. idegen hatalom számára végzett, biztonságot veszélyeztető vagy titkosszolgálati tevékenységre engednek következtetni,

25
3. olyan törekvésekre mutatnak, amelyek erőszak alkalmazásával vagy arra irányuló előkészítő tevékenységekkel a Német Szövetségi Köztársaság külügyi érdekeit veszélyeztetik,

26
4. olyan törekvésekre és tevékenységekre utalnak, amelyek a népek közötti megértés eszméje [Alaptörvény 9. § (2) bek.] vagy a népek békés együttélése (Alaptörvény 9. §) ellen irányulnak,

27
az Alaptörvény alkalmazási területén belül, amennyiben ilyen törekvésekre vagy tevékenységekre mutató tényleges támpontok merülnek fel.

28
….

29
5. § Jogosultságok

30
(1) ….

31
(2) Az Alkotmányvédelmi Hatóság a 7. § szerint információszerzésre mint hírszerző-szolgálati módszerre az alábbi intézkedéseket foganatosíthatja:

[12] ÉWA

32
….

33
11. az Internet titkos megfigyelése vagy egyéb felderítése, mint különösen az álcázott részvétel kommunikációs berendezéseiben vagy azok felkutatása, valamint a titkos hozzáférés információtechnikai rendszerekhez, ideértve technikai eszközök alkalmazását is. Ha ilyen intézkedések a levél-, posta- és távközlési titokba való beavatkozásnak minősülnek, vagy annak módját és súlyát tekintve azzal egyenértékűek, azok csak az Alaptörvény 10. §-áról szóló törvény előfeltételei mellett megengedhetők.

34….

35
(3) Hírszerző-szolgálati eszközökkel nyert személyes vonatkozású adatokat meg kell jelölni és az intézkedés végrehajtását követően közölni kell azzal a személlyel, akiről ezeket az információkat gyűjtötték. E közlésre nincs szükség, ha

36
1. a feladat ellátását a közlés veszélyeztetheti,

37
2. a közlés teljesítése veszélyeztetheti a forrásokat vagy az Alkotmányvédelmi Hatóság informáltságának vagy munkamódszerének feltárása aggályosnak mutatkozik,

38
3. az értesítés veszélyezteti a közbiztonságot vagy egyébként a Szövetség vagy egy tartomány érdekeire nézve hátrányokkal járhat, vagy

39
4. az adatokat vagy a feldolgozás eredményeit jogszabályi előírásnak megfelelően vagy harmadik személy túlnyomóan jogos érdekeire való tekintettel titokban kell tartani,

40
5. az 1-4-ben rögzített előfeltételek az intézkedést követő öt év elteltével is fennállnak és a bizonyossággal határos valószínűséggel a jövőben is fenn fognak állni.

41….

42
5a §
Különös jogosultságok

43
(1) Az Alkotmányvédelmi hatóság bizonyos esetben hitelintézetektől, pénzügyi vállalkozásoktól is költségmentesen szerezhet be információt a fizetési forgalomban résztvevőkről és pénzmozgásokról és pénzbefektetésekről, ha ez a 3. § (1) bekezdésben rögzített feladataik ellátásához szükséges és tényleges támpontok merülnek fel a 3. § (1)-ben rögzített védett érdekek súlyos veszélyeztetésére vonatkozóan.

44 (2) …

45
(3) Az (1) és (2) bekezdésekben meghatározott felvilágosítás csak kérelemre adható. A kérelmet az alkotmányvédelmi részleg vezetője vagy helyettese írásba foglalja és megindokolja. A kérelemről a

belügyminiszter határoz. A G 10-bizottságot [az Alaptörvény 10. §-áról szóló törvény végrehajtásáról rendelkező törvény 3. § (1) bek.] a határozat tárgyát képező kérelemről annak végrehajtását megelőzően haladéktalanul tájékoztatni kell. Ha a késlekedés veszéllyel jár, a belügyminiszter a határozat végrehajtását már a Bizottság tájékoztatását megelőzően is elrendelheti. A G 10-bizottság hivatalból vagy panaszok alapján ellenőrzi a felvilágosítások beszerzésének szabályszerűségét és szükségességét. Északrajna-Westfália tartománynak az Alaptörvény 10. §-áról szóló törvény végrehajtásáról rendelkező törvénye 3. § (1) bekezdését annak az intézkedésnek megfelelően kell alkalmazni, amely szerint a Bizottság ellenőrzési jogosultsága az (1) és (2) bekezdések szerint megszerzett személyes vonatkozású adatok feldolgozására és felhasználására terjed ki. Azokat a felvilágosításra vonatkozó határozatokat, amelyeket a G 10-bizottság nem szabályszerűnek vagy nem szükségszerűnek nyilvánít, a belügyminiszternek haladéktalanul vissza kell vonnia. Az (1) és (2) bekezdések szerint megszerzett adatok feldolgozására Északrajna-Westfáliának az Alaptörvény 10. §-áról szóló törvény végrehajtásáról rendelkező törvénye 4. §-át kell megfelelően alkalmazni. A felvilágosításra irányuló kérelemről és a továbbított adatokról az érintettnek vagy harmadik személyeknek felvilágosítást nyújtó tájékoztatást nem adható. Az Alaptörvény 10. §-áról szóló törvény végrehajtásáról rendelkező törvény 5. §-át megfelelően alkalmazni kell.

46…

47
7. §
Az adatgyűjtés különös formái

48
(1) Az Alkotmányvédelmi Hatóság feladatai ellátásához nem közjogi szervezetek megkérdezésével, az 5. § (2) bekezdésében meghatározott eszközökkel információkat, különösen személyes vonatkozású adatokat gyűjthet, ha tények alapján feltételezhető, hogy

49
1. így tudomás szerezhető a 3. § (1) bekezdése szerinti törekvésekről vagy tevékenységekről, vagy az ilyen tudomásszerzéshez szükséges forrásokról, vagy

50
2. erre az Alkotmányvédelmi Hatóságnak szüksége van munkatársai, eszközei és forrásai védelmére biztonságot veszélyeztető vagy titkosszolgálati tevékenységekkel szemben.

51
(1) A közbiztonságot fenyegető veszély, különösen általános veszély vagy életveszély [Alaptörvény 13. § (4) bek.] esetében magánlakásban elhangzó, nem a nyilvánossághoz szóló beszéd technikai eszközökkel titkosan lehallgatható vagy feljegyezhető. Az 1. mondat megfelelően alkalmazható kép- és videofelvételekre is. Az 1. és 2. mondat szerinti intézkedéseket az alkotmányvédelmi részleg vezetője vagy helyettese rendeli el, ha bírósági határozatot kellő időben megszerezni nem lehet. A bírósági határozatot utólag haladéktalanul meg kell szerezni. Erre az Alkotmányvédelmi hatóság székhelye szerinti járásbíróság illetékes[13]. Az eljárásra az önkéntes igazságszolgáltatási ügyekről szóló törvény [14] előírásait kell megfelelően alkalmazni. A gyűjtött információkat csak Északrajna-Westfáliának az Alaptörvény 10. §-áról szóló törvény végrehajtásáról rendelkező törvénye 4. § (4) bekezdése szerinti intézkedésekre használhatók fel. Az 1. és 2. mondat szerinti technikai eszközök ezen felül a lakásokban tartózkodó személyek védelmére is bevehetők, ha ez életüket, egészségüket vagy szabadságukat fenyegető veszély elhárításához elengedhetetlen [Alaptörvény 13. § (5) bek.]. A 8. mondat szerinti intézkedéseket az alkotmányvédelmi részleg vezetője vagy helyettese rendeli el. A 8. mondatban rögzített célon kívül az Alkotmányvédelmi Hatóság az így gyűjtött adatokat csak veszélye elhárítására használhatja fel a 3. § (1) bek. 2-4. pontjában meghatározott feladatai keretében, továbbá

[13] Amtsgericht. Lásd: Gesetz über die Angelegenheiten der freiwilligen Gerichtsbarkeit
[14] Gesetz über die Angelegenheiten der freiwilligen Gerichtsbarkeit

Északrajna-Westfáliának az Alaptörvény 10. §-áról szóló törvény végrehajtásáról rendelkező törvény 4. § (4) bek. 1. és 2. pontja szerinti továbbításra. A felhasználás csak akkor megengedhető, ha az intézkedés jogszerűségét a bíróság megállapította; ha a késlekedés veszéllyel jár a bírósági döntést utólag haladéktalanul meg kell szerezni. Északrajna-Westfáliának az Alaptörvény 10. §-áról szóló törvény végrehajtásáról rendelkező törvénye 4. § (6) bekezdését megfelelően alkalmazni kell. A lakás sérthetetlenségének alapjoga (Alaptörvény 13. §) ennyiben korlátozódik.

52….

53
8. §
Személyes vonatkozású adatok feldolgozása

54
(1) Az Alkotmányvédelmi Hatóság feladatai ellátásához az írott vagy elektronikus iratokban rögzített személyes vonatkozású adatokat és személyről vezetett adatállományokat feldolgozhatja, ha

55
tényleges támpontok alapján felmerül a 3. § (1) bekezdésben meghatározott törekvések és tevékenységek gyanúja,

56
ez a 3. § (1) bekezdésben meghatározott törekvések vagy tevékenységek felkutatásához és kiértékeléshez szükséges, vagy

57
ez a 3. § (2) bekezdésében rögzített feladatai ellátásához szükséges.

58….

59
(4) Az elektronikus esetiratokban rögzített személyes vonatkozású adatokhoz való hozzáférést jegyzőkönyvezni kell. Az elektronikus esetiratokban tárolt személyes vonatkozású adatok a személyről vezetett adatállományok törlését követően a 3. § (2) bekezdése szerinti feladatok ellátásához nem használhatók fel és más hatóságokhoz nem továbbíthatók. Ilyen adatok elektronikusan nem kutathatók.

60….

61
10. §
Személyről vezetett adatállományok helyesbítése, törlése és zárolása

62
(1) Az Alkotmányvédelmi Hatóság az adatállományokban tárolt személyes adatokat, ha tévesek, helyesbíti.

63
(2) Az Alkotmányvédelmi Hatóság az adatállományokban tárolt személyes adatokat törloi, ha tárolása nem volt megengedett vagy ismeretükre a feladatai ellátásához már nincs szükség.

64….

65
11. §

Írásbeli vagy elektronikus iratokban tárolt személyes vonatkozású adatok helyesbítése és törlése, iratmegsemmisítés

66
(1) Ha az Alkotmányvédelmi Hatóság megállapítja, hogy írásbeli vagy elektronikus iratokban tárolt személyes vonatkozású adatok tévesek, azokat helyesbítenie kell.

67
(2) Az Alkotmányvédelmi Hatóságnak írásbeli vagy elektronikus iratokban tárolt személyes vonatkozású adatokat zárolnia kell, ha az adott esetben megállapítja, hogy zárolásuk hiányában az érintett személy védelemre méltó érdekei csorbulnának és az adatokra feladatai ellátásához a jövőben már nincs szükség.

68
(3) Az Alkotmányvédelmi Hatóságnak a személyről vezetett adatállományokat meg kell semmisítenie, ha azok feladatai ellátásához már nem szükségesek és a megsemmisítés az érintett személy védelemre méltó érdekével nem ellentétes.

69….

70
13. §
Közös adatállományok

71
Az Alkotmányvédelmi Hatóság jogosult közös adatállományokban rögzített személyes vonatkozású adatokat a Szövetség és a tartományok Alkotmányvédelmi Hatóságaival és más biztonsági hatóságokkal feldolgozni, ha különös szövetségi jogi vagy tartományi jogi előírások ennek lehetőségét, terjedelmét és egyéb adatvédelmi követelményeit szabályozzák.

72
14. §
Tájékoztatás

73
(1) Az Alkotmányvédelmi Hatóság a kérelmező személy írásbeli kérelemére költségmentesen tájékoztatás ad a személyére vonatkozó tárolt adatokról, a tárolás céljáról és jogalapjáról. Iratbetekintésre nincs lehetőség.

74….

75
17. §
Személyes vonatkozású adatok továbbítása

76
(1) Az Alkotmányvédelmi Hatóság személyes vonatkozású adatokat bíróságoknak és belföldi hatóságoknak továbbíthat, ha ez feladataik ellátásához szükséges vagy az adatokra a továbbítás címzettjének feladatai ellátásához a szabad demokratikus alaprend védelme vagy a közbiztonság egyéb céljára van szükségük.

77
(2) Az Alkotmányvédelmi Hatóság személyes vonatkozású adatokat továbbíthat a belföldön állomásozó haderők szolgálati szerveinek, ha a Német Szövetségi Köztársaságot erre kötelezi az Észak-atlanti Szerződés Felei között fennálló Szerződéshez csatolt, 1959. augusztus 3-án kelt, a Felek

csapatai jogállásáról szóló Kiegészítő Szerződés[15] 3. §-a, amely e jogállást a Német Szövetségi Köztársaságban állomásozó külföldi csapatok tekintetében szabályozza.

78
(3) Az Alkotmányvédelmi Hatóság személyes vonatkozású adatokat külföldi közjogi szervnek, valamint nemzetek feletti és nemzetközi szervezeteknek, ha a továbbítást feladataik ellátása vagy a címzettet fenyegető jelentős veszély elhárítása szükségessé teszi.

79….

80
AZ ÉWA 5. § (2) bek. 11. pont 2. mondatában hivatkozott, az Alaptörvény 10. §-áról szóló törvény a távközlésnek az Alkotmányvédelmi Hatóság által folytatott megfigyeléséről többek között az alábbi rendelkezéseket tartalmazza:

81
1. §
A törvény tárgya

82 (1)

83
1. A Szövetség és a tartományok Alkotmányvédelmi Hatóságai … a szabad demokratikus alaprend, a Szövetség vagy egy tartomány fennállását, továbbá az Északatlanti Szerződés Feleinek a Német Szövetségi Köztársaságban állomásozó csapatai biztonságát fenyegető veszélyek elhárítása céljából,

84
2. …

85
a távközlést megfigyelhetik és feljegyezhetik. …

86
…

87
3. §
Előfeltételek

88
(1) Az 1 § (1) bek. 1. pontban rögzített korlátozások az ott megjelölt előfeltételek esetében rendelhetők el, ha tényleges támpontok alapján felmerül a gyanú, hogy valaki olyan bűncselekményt tervez, elkövet vagy elkövetett, amely

89
1. a béke ellen irányul vagy hazaárulás (Büntető Törvénykönyv[16] 80-83. §)

90
2. veszélyezteti a demokratikus jogállamiságot [Büntető Törvénykönyv 84-86. §, 87-89. §, az Egyesületi Törvény[17] 20. § (1) bek. 1-4. pont],

---

[15] Zusatzabkommen zu dem Abkommen zwischen den Parteien des Nordatlantikvertrages über die Rechtsstellung ihrer Truppen (BGBl. II 1961 S. 1183, 1218)
[16] *Strafgesetzbuch – StGB*
[17] Vereinsgesetz

91
3. árulás és a külsőbiztonság veszélyeztetése (Büntető Törvénykönyv 94-96. §, 97-100a §),

92
4. a honvédelem ellen irányul (Büntető Törvénykönyv 109e-109g §),

93
5. az Északatlanti Szerződés nem német Feleinek a Német Szövetségi Köztársaságban állomásozó csapatai biztonsága ellen irányul (Büntető Törvénykönyv 87., 89., 94-96., 98-100., 109e-109g §) az 1957. június 11-ei, a büntetőjog módosításáról szóló törvény[18] 7. §-ával összefüggésben a törvény 1968. június 25-én kelt szövege[19] szerint,

94
6. bűncselekmény

95
a) a Büntető Törvénykönyv 129a-130. §, valamint

96
b) a Büntető Törvénykönyv 211. §, 212. §, 239a §, 239b §, 306-306c §, 308. § (1)-(3) bek., 315. § (3). bek., 316b § (3) és 316c § (1) és (3) bek. szerint, amennyiben ezek a szabad demokratikus alaprend, a Szövetség vagy egy tartomány fennállása vagy biztonsága ellen irányulnak,
vagy

97
7. bűncselekmény a tartózkodásról szóló törvény[20] szerint.

98
Ugyanez érvényes, ha tényleges támpontok alapján felmerül a gyanú, hogy valaki egy olyan egyesület tagja, amelynek célja vagy tevékenysége a szabad demokratikus alaprend, a Szövetség vagy egy tartomány fennállása vagy biztonsága ellen irányuló bűncselekmény elkövetése.

99
(2) A rendelkezés csak akkor megengedhető, ha a tényállás felkutatása más módon kilátástalan vagy jelentősen nehezebb lenne. Az csupán a gyanúsítottak vagy olyan személyek ellen irányulhat, akikről bizonyos tények alapján feltételezhető, hogy a gyanúsítottaknak szánt vagy tőlük származó közléseket fogadnak vagy továbbadnak, vagy ismeretségüket a gyanúsított kihasználja. Küldeményekre vonatkozó intézkedések csak olyan küldemények tekintetében megengedhetők, melyekkel kapcsolatban igazolható az a feltevés, hogy azoktól származik vagy azok a címzettjei, akik ellen a rendelkezés irányul. A Német Bundestag vagy a tartományok parlamentjei képviselőinek a postaküldeményeit egy olyan intézkedés nem érintheti, amely harmadik személy ellen irányul.

100
4. §
A felülvizsgálat, a megjelölés és a törlés kötelezettsége, továbbítás, célhoz kötöttség

101
(1) Az információt gyűjtő szerv haladéktalanul és ezt követően legalább hat hónaponként felülvizsgálja, szüksége van-e a gyűjtött, személyes vonatkozású adatokra önmagukban vagy a már rendelkezésre álló adatokkal együtt feladatai ellátásához az 1. § (1) bek. 1. pontjában rögzített célra.

[18] Viertes Strafrechtsänderungsgesetz (BGBl. I S. 597)
[19] BGBl. I S. 741
[20] Aufenthaltsgesetz

Ha az adatokra e célból nincs szükség és azokat más szerveknek nem kell továbbítani, az adatokat bírósági hivatali minősítéssel rendelkező tisztviselő felügyelete mellett haladéktalanul törölni kell.

102….

103
9. §
Kérelem

104
(1) E törvény szerinti korlátozó intézkedések csak kérelemre rendelhetők el.

105….

106
10. §
Elrendelés

107
(1) Korlátozó intézkedések elrendelésére a tartományok Alkotmányvédelmi Hatóságai kérelme esetében az illetékes legfelsőbb tartományi hatóság, egyébként a szövetségi kancellár által megbízott szövetségi minisztérium illetékes.

108….

109
AZ ÉWA 5a § (3) bekezdésében hivatkozott, Északrajna-Westfáliának az Alaptörvény 10. §-áról szóló törvény végrehajtásáról rendelkező törvénye 4. és 5. §-a kivonatosan az alábbi rendelkezéseket tartalmazza:

110
4. §
A felülvizsgálat, a megjelölés és a törlés kötelezettsége, továbbítás, célhoz kötöttség

111
(1) Az információt gyűjtő szerv haladéktalanul és ezt követően legalább hat hónaponként felülvizsgálja, szüksége van-e a gyűjtött, személyes vonatkozású adatokra önmagukban vagy a már rendelkezésre álló adatokkal együtt feladatai ellátásához az Alaptörvény 10. §-áról szóló törvény 1. § (1) bek. 1. pontjában rögzített célra. Ha az adatokra e célból nincs szükség és azokat más szerveknek nem kell továbbítani, az adatokat bírósági hivatali minősítéssel rendelkező tisztviselő felügyelete mellett haladéktalanul törölni kell.

112….

113
5. §
Az érintett tájékoztatásának ellenőrzése a G 10-bizottság által

114
(1) A korlátozó intézkedésekről megszüntetésüket követően az érintettet a belügyminisztérium tájékoztatja, ha kizárható, hogy a korlátozás célját az nem veszélyezteti.

115….

II.

116
1. Az 1a-ban megnevezett panaszos újságíró és mindenekelőtt egy online-publikáció számára ír. Foglalkozása keretében olyan Internet-oldalakat is felkeres, amelyeket alkotmányellenes személyek és szervezetek működtetnek. Ezen felül foglalkozik az adatvédelem jogi kérdéseivel és másokkal együtt működteti a www.stop1984.com honlapot. E honlappal összefüggésben lehetőség nyílik un. csevegésekben részt venni. Ezzel a lehetőséggel szélsőséges jobboldaliak is élnek. E személyekkel kapcsolatos információkat az 1a-ban megnevezett panaszos magánéletben és foglalkozása során használt számítógépei merevlemezein tárolja.

117
Az 1b-ben megnevezett panaszos aktív tagja a DIE LINKE párt Északrajna-Westfália tartományi szövetségének, melyet Északrajna-Westfália Alkotmányvédelmi Hatósága megfigyel. Politikai tevékenységéhez az Internethez csatolt számítógépét is használja. Emellett, az 1a-ban megnevezett panaszoshoz hasonlóan, az Internetet használja magánjellegű kommunikációra és folyószámlájáról teljesített fizetései lebonyolítására is.

118
A 2a-ban és a 2b-ben megnevezett panaszosok egy ügyvédi iroda partnerei. A 2a-ban megnevezett panaszos mint ügyvéd egyebek mellett menekültek ügyeivel is foglalkozik. Ezek egyike a PKK, a kurd Munkáspárt tagja, aki az Északrajna-Westfália Alkotmányvédelmi Hatósága megfigyelése alatt áll. Lakásában és az iroda helységeiben ő is számítógép-hálózatokat használ, melyek az Internethez kapcsolódnak. Az irodai hálózatot használja mind a 2b-ben, mind pedig a 2c-ben megnevezett panaszos, akit az iroda mint szabadfoglalkozásút foglalkoztat.

119
2. Amennyiben az alkotmányjogi panaszok az ÉWA 5. § (2) bek. 11. pontjára irányulnak, a panaszosok az Alaptörvény 2. § (1) bekezdésének sérelmét kifogásolják az Alaptörvény 1. § (1), 10. § (1) és 13. § (1) bekezdéseivel összefüggésben.

120
Amennyiben a norma az Internet kommunikációs berendezéseiben való részvételről rendelkezik, a távközlési jogba való beavatkozást szabályozna. A normában továbbá szabályozott titkos hozzáférés IT rendszerekhez az Alaptörvény 13. §-át akkor sérti, ha a hozzáférésre használt számítógép egy lakásban van. E tekintetben az a mérvadó, hogy személyes viselkedési módok, különösen ha egy térben elhatárolt lakásban valósulnak meg, különös védelmet élveznek. Ilyen intézkedések ezen felül az általános személyiségi jogba és a távközlési titokba is beavatkoznak.

121
Amennyiben az ÉWA 5. § (2) bek. 11. pontja szerinti intézkedéseket az Alaptörvény 13. § szerinti beavatkozásnak tekintjük, a rendelkezés már csak azért is alkotmányellenes, mert nem felel meg az Alaptörvény 13. § (2)-(7) bekezdéseiben rögzített különös korlátozó kikötéseknek. Nem teljesül továbbá az Alaptörvény 19. § (1) bek. 2. mondatában rögzített hivatkozási követelmény sem.

122
AZ ÉWA 5. § (2) bek. 11. pontja ezen túlmenően nem felel meg a normavilágosság követelményének. A norma 2. mondatának utalása a titoktörvényre sem előfeltételeiben, sem kiterjedésében nincs megfelelően meghatározva. Hiányoznak továbbá a magánéletvitel belső magjában folyó egyéni kibontakozást védő megfelelő normatív előfeltételek is. Ilyen előfeltételekre szükség van, mert a magánhasználatban lévő számítógépek manapság különösen arra szolgálnak, hogy felettébb személyes tartalmú adatok dolgozzanak fel. Végül nem érvényesül az arányosság elve. A törvényes beavatkozási küszöb túl alacsony. Ezen felül hiányzanak az érintett védelmét szolgáló eljárási óvintézkedések, mint például a bíróság kikötése. Mi több, a gyűjtött adatokat széleskörűen, céltól idegen módon vagy más hatóságokhoz továbbíthatják.

123
3. A panaszosok kifogásolják továbbá, hogy az ÉWA 5. § (3) bekezdése sérti az Alaptörvény 19. § (4) bekezdését, valamint azokat az anyagi alapjogokat, amelyekbe az ÉWA 5. § (2) bekezdése szerinti intézkedések beavatkoznak. A rendelkezés 2. mondata az alapjogilag elrendelt értesítési kötelezettségre vonatkozó messzemenő kivételeket írja elő, amelyek ezt messzemenően kiüresítik.

124
4. Az 1-ben megnevezett panaszosok felfogása szerint az ÉWA 5a § (1) bek. sérti az információs önrendelkezési jogot. A rendelkezés számlatartalmak gyűjtését teszi lehetővé túlságosan tág előfeltételek mellett, melyek azért aránytalanok.

125
AZ ÉWA 13. § nem felel meg a titkosszolgálatok és a rendőre szervek elkülönítésére vonatkozó követelménynek, melyet az információs önrendelkezési joggal összefüggésben a jogállamiság követelménye megjelenési formájának kell tekinteni.

126
5. A 2-ben megnevezett panaszosok előadják, hogy az ÉWA 7. § (2) sérti az Alaptörvény 13. § (1) bekezdését. A rendelkezés nem felel meg annak az előírásnak, amelyet a Szövetségi Alkotmánybíróság a lakótér büntetőeljárásban alkalmazott akusztikai megfigyelésére vonatkozó határozatában rögzített.

127
AZ ÉWA 8. § (4) bek. 2. mondata sérti az információs önrendelkezési jogot, mert a személyes jellegű adatok törlésére vonatkozó szabályozás hiányzik. A norma ezzel lehetővé teszi az adatok készletre való megengedhetetlen tárolását.

128
Végül amennyiben olyan adatokról van szó, melyekhez az ÉWA 5. § (2) bek. 11. pontja szerinti intézkedésekkel jutottak, továbbításuknak az ÉWA 17 § (1) bekezdésében rögzített szabályozása alkotmányellenes, és ellentétes a célhoz kötöttség, a normavilágosság és az arányosság követelményével.

III.

129
Az alkotmányjogi panaszhoz írásbeli állásfoglalást nyújtott be: a Szövetségi Kormány, Északrajna-Westfália Tartomány Kormánya és Tartományi Gyűlése, a Szövetségi Közigazgatási Bíróság, az adatvédelem és információszabadság szövetségi biztosa és adatvédelem és információszabadság északrajna-westfáliai biztosa. Északrajna-Westfália Tartományi Gyűlése SPD és BÜNDNIS 90/DIE GRÜNEN frakciói egy részükre készített jogi szakvéleményt nyújtottak be. Ezen felül a Szenátus írásbeli szakértői állásfoglalásokat szerzett be Andreas Bogk, Dirk Fox, Prof. Dr. Felix Freiling, Prof. Dr. Andreas Pfitzmann és Prof. Dr. Ulrich Sieber uraktól.

130
1. A Szövetségi Kormány a támadott normára közvetlenül nem hivatkozva általában tárgyalja az IT rendszerekhez való, technikai eszközökkel végrehajtott titkos hozzáférés alkotmányjogi kérdéseit.

131
Ezeket az intézkedéseket meg kell különböztetni a távközlésnek az Alaptörvény 10. §-a alá tartozó megfigyelésétől. A Szövetségi Alkotmányvédelmi Hivatal által a múltban egy-egy esetben végrehajtott „online-átkutatás“ esetében abból indultak ki, hogy ennek alapjogi szabálya egyedül az Alaptörvény 2. § (1) bekezdése az 1. § (1) bekezdésével összefüggésben. Mindazonáltal fokozottan előtérbe kerül az Alaptörvény 13. § (1) bekezdése mint az „online-átkutatás“ esetleg megfelelő szabálya. Az „online-átkutatás“-t az ismételt behatolás technikai lehetőségei vagy egy számítógépben

egy hosszabb időn át tartó benntartózkodás minősítik inkább megfigyelésnek. Legfeljebb az érintett személy érzi úgy, hogy a számítógépben koncentrálódhat magánszférájának felettébb jelentős része, melyet korábban egy lakás terében szórt szét.

132
A hozzáférés mint az alkotmányvédelem minősített módja sajátos alkotmányjogi biztosítékokat követel. A magánéletvitel belső magjának védelméről gondolkodni kell akkor is, ha az a szoftver által alkalmasnak tartott kereső-paraméterek alapján relevánsnak ítélt információk másolása vagy átjátszása során még nem, hanem csak az adatállományoknak a hatóság számítógépén való utólagos átnézése során biztosítható. Tekintettel a lakás átkutatására és a lakás megfigyelésére irányuló intézkedések hasonlóságára, mérlegelni kell, nem szükséges-e a hozzáférés bírósági jóváhagyása. Elvileg az értesítési kötelezettséggel is számolni kell. Az „online-átkutatás"-nak ezen felül fokozott arányossági követelményeknek kell megfelelnie. Az Alkotmányvédelmi Hatóság ilyen intézkedése beavatkozásának intenzitására való tekintettel csak ultima ratio lehet.

133
2. Északrajna-Westfália Tartományi Kormánya az alkotmányjogi panaszt nem befogadhatónak, de legalábbis megalapozatlannak tartja.

134
AZ ÉWA 5. § (2) bek. 11. pontjában rögzített intézkedések nem sértik az Alaptörvény 13. §-át. Ez az alapjog csak akkor sérülne, ha egy állami intézkedés egy konkrét térre irányulna, vagyis ha térbeli elhatárolásokon túlnyúlna. Itt nincs erről szó. Az Internet felderítését célzó olyan intézkedéseket, mint az e-mail forgalom vagy az Internet-telefon megfigyelése, egyébként az Alaptörvény 10. §-a szerint kell megítélni. Egyebekben az információs önrendelkezési jog a mérvadó.

135
AZ ÉWA 5. § (2) bek. 11. pontja megfelel a normavilágosság követelményének. A normát úgy fogalmazták meg, hogy a technika fejlődésével megjelenő újdonságok alkalmazását is lehetővé tegye. A norma továbbá figyelembe veszi a magánéletvitel belső magját. A belső mag megkövetelt védelmét a hivatkozott titoktörvény, annak is a 4. § (1) bekezdése biztosítja. Az Alkotmányvédelmi Hatóság cselekvésterének azzal is számolnia kell, hogy éppen az alkotmányellenes törekvésekkel kapcsolatos kommunikáció súlypontja helyeződik át az Internetre. A hozzáférés egyes számítógépekhez elengedhetetlen, mert kommunikációs tartalmakat technikailag lehetséges úgy továbbítani, hogy a hozzáférés a továbbítás során lehetetlen. Ennyiben az ÉWA 7. § (1) bekezdése megfelelő beavatkozási küszöböt állapít meg. További anyagi kritériumok és eljárásjogi óvintézkedések adódnak különösen a titoktörvény 3. §-ából. Becslés szerint az IT-rendszerekhez való hozzáférések száma az évi tízet nem fogja meghaladni.

136
AZ ÉWA 5. § (3) bekezdése, amely a megjelölésre és a tájékoztatási kötelezettségre vonatkozó szabályozást tartalmazza, alkotmányjogilag ugyancsak nem kifogásolható. Az Internet felderítését célzó, az ÉWA 5. § (2) bek. 11. pontja szerinti intézkedésekre mellesleg nem az ÉWA 5. § (3) bekezdése, hanem a titoktörvény 12. §-a vonatkozik.

137
AZ ÉWA 5a § (1) bekezdésében rögzített, a számlatartalmak lehívására vonatkozó jogosultság ugyancsak megfelel az alkotmányos követelményeknek. Az un. home-grown-networks jelensége, amely belföldi támadások célpontjait követi, újfajta és fokozott veszélyre utaló helyzetről tanúskodik. A jogosultság személyes összefonódások és – például fegyver vásárlással és militáns csoportok finanszírozásával kapcsolatos – pénzmozgások felderítéséhez járulhat hozzá.

138
3. Az alkotmányjogi panaszokat Északrajna-Westfália Tartományi Gyűlése ugyancsak megalapozatlannak tartja.

139
A nemzetközi terrorizmus terjedése újfajta veszélyhelyzetet teremt, amely az államot a terrorizmus elleni hatékony védelem érdekében az alapjogok korlátozására kényszeríti. A jogállam – hogy az új kihívásokkal szembenézzen – kénytelen a rendelkezésére álló jogi eszköztárat gondosan továbbfejleszteni. Különösen a biztonsági hatóságok információtechnikai cselekvőképességét kell az aktuális keretfeltételekhez igazítani. Korszerű kommunikációs technikákat vetnek be a legkülönfélébb bűntettek elkövetésére és előkészítésére, melyek a bűncselekmények hatékonyságát fokozzák.

140
Jóllehet a klasszikus rendőri jog az intenzív alapjogi beavatkozást csak a gyanú erőssége, illetőleg a veszély meghatározott foka esetében engedi meg, ez azonban egy olyan hatósági feladatkörön nyugszik, amely az Alkotmányvédelmi Hatóságoktól alapvetően különbözik. Főszabályként terrorisztikus cselekmények felderítését célzó strukturális előzetes információk megszerzése nem vezethet az érintettre nézve közvetlen szankciókhoz és következményekhez.

141
Az Alaptörvény 13. §-át az ÉWA 5. § (2) bek. 11. pontja nem érinti. A tárolt adatokhoz való hozzáférésnek nem célja egy lakás térbeli határainak átlépése. A lakásban folyó eseményeket sem figyelik meg. Ezzel szemben adott esetben az Alaptörvény 10. §-ába való beavatkozás valósulhat meg. A norma azonban megfelel a beavatkozás jogosultságával szemben támasztott alkotmányjogi követelményeknek.

142
AZ ÉWA 5. § 3. bek. 2. mondatában szabályozott, az értesítési kötelezettségre vonatkozó kivételek is összeegyeztetőek az Alaptörvénnyel.

143
4. Szász Állam Kormánya kifejti, hogy iszlám és iszlám terrorisztikus csoportosulásokon belül a kommunikáció leginkább az Interneten folyik. Az autonomisták is Internetet és mobiltelefont használnak lehetőleg védett kommunikációra. Minthogy a megfigyelt személyek többnyire IT-rendszereket használnak, a hozzáférés a klasszikus titkosszolgálati módszerekkel részben lehetetlenné vált.

144
AZ ÉWA 5. § (2) bek. 11. pontja nem ad felhatalmazást az Alaptörvény 10. § (1) bekezdésébe vagy 13. § (1) bekezdésébe való beavatkozásra. A rendelkezés egyébként elegendően meghatározott és arányos. A magánéletvitel belső magját nem érinti, mivel a polgár nem kényszerül egy személyi számítógép használatára, ha fokozottan személyes kommunikációt akar folytatni. AZ ÉWA 5. § (1) bek., 5a § (1) bek. és 13. § az Alaptörvénnyel összhangban vannak.

145
5. A Szövetségi Közigazgatási Bíróságnak az IT-rendszerekhez való titkos hozzáférésre felhatalmazást adó ÉWA 5. § (2) bek. 11. pontjával szemben alkotmányjogi kételyeinek ad hangot. Nyomós érvek szólnak az Alaptörvény 13. §-ának alkalmazása mellett és ellen egyaránt. A szabályozott hozzáférés minden esetre beavatkozás az információs önrendelkezési jogba. Kétségesnek látszik e beavatkozás arányos volta. Kézenfekvő, hogy – tekintettel az alapjogi beavatkozás súlyára – az „online-átkutatás“-t meghatározott jogtárgyakat fenyegető tényleges veszély fennállásától tegyék függővé. A törvény nem tartalmaz a magánéletvitel belső magját védő intézkedést.

146
6. Az adatvédelem és információszabadság szövetségi biztosa és az adatvédelem és információszabadság északrajna-westfáliai biztosa a támadott normákat alkotmányellenesnek tartják. Ezzel kapcsolatos állításaik mind érvelésük módját, mind következtetéseiket tekintve a panaszosok előterjesztésével messzemenően összecseng.

147
7. Északrajna-Westfália Tartományi Gyűlése SPD és BÜNDNIS 90/DIE GRÜNEN frakciói egy részükre készített jogi szakvéleményt nyújtottak be. E szakvélemény szerint a támadott normák sem az Alaptörvénnyel, sem az északrajna-westfáliai Tartományi Alkotmánnyal nem összeegyeztethetők.

148
8. A szakértők, Andreas Bogk, Dirk Fox, Prof. Dr. Felix Freiling és Prof. Dr. Andreas Pfitzmann urak mindenekelőtt az IT-rendszerekhez való titkos hozzáféréssel, Prof. Dr. Ulrich Sieber úr pedig összehasonlító jogi kérdésekkel és a szóban forgó intézkedések jogszerűségére vonatkozó követelményekkel kapcsolatban nyilatkoztak.

IV.
149
A szóbeli tárgyaláson a következők nyilatkoztak: a panaszosok, a Szövetségi Kormány, A Szövetségi Bűnügyi Hivatal, a Szövetségi Alkotmányvédelmi Hivatal, az Információtechnikai Biztonsági Hivatal, Északrajna-Westfália Tartományi Kormánya és Tartományi Gyűlése, Északrajna-Westfália Tartományi Alkotmányvédelmi Hivatala, az adatvédelem és információszabadság szövetségi biztosa, az adatvédelem és információszabadság északrajna-westfáliai biztosa, valamint Andreas Bogk, Dirk Fox, Prof. Dr. Felix Freiling, Prof. Dr. Andreas Pfitzmann és Prof. Dr. Ulrich Sieber urak mint szakértők.

B.
150
Az alkotmányjogi panaszok csak részben befogadhatóak.

I.
151
Amennyiben az alkotmányjogi panaszok az ÉWA 5. § (2) bek. 11. pontja ellen irányulnak, befogadhatóságuk nem vitatható.

II.
152
A minden panaszos által támasztott kifogás az ÉWA 5. § (3) bekezdése alkotmányellensége tekintetében az alkotmányjogi panaszok csak annyiban befogadhatók, amennyiben azok egy, az ÉWA 5. § (2) bek. 11. pontja szerint foganatosított intézkedésre vonatkozó értesítéssel kapcsolatosak. Egyebekben az alkotmányjogi panaszok megalapozottsága nem felel meg a Szövetségi Alkotmánybíróságról szóló törvény[21] 23. § (1) bek. 2. mondatának és 92. §-ának. Ezek szerint az alkotmányjogi panaszt megfelelő érvekkel kell megalapozni. A panaszosnak be kell mutatnia, hogy a támadott intézkedés mely alkotmányjogi követelményekkel ellentétes. Ezen felül ki kell fejtenie, hogy azok mennyiben sértik a megjelölt alapjogokat.

153
Ez itt annyiban hiányzik, amennyiben a panaszosok általában kifogásolják, hogy az ÉWA 5. § (2) bekezdés értelmében vett hírszerző-szolgálati intézkedésekkel kapcsolatos értesítés szabályozása nem felel meg az alkotmányjogi követelményeknek. Ha az Alaptörvény az állam titkos információs intézkedésével érintett személy értesítését írja elő, ez egyebek mellett döntően attól függ, hogy ez az intézkedés beavatkozik-e az érintett alapjogaiba, s ha igen, milyen intenzitással. AZ ÉWA 5. § (2) bekezdése több különböző intézkedést irányoz elő, amelyek a beavatkozás minőségére és a beavatkozás intenzitására nézve egymástól jelentősen eltérnek. E tekintetben a panaszosok bemutathatták volna és be is kellett volna mutatniuk, hogy ezek közül az intézkedések közül melyek azok, amelyek esetében véleményük szerint az értesítés kötelező, továbbá hogy az értesítési kötelezettségre vonatkozó, az ÉWA 5. § (3) bekezdése 2. mondatában szabályozott kivételek

[21] Bundesverfassungsgerichtsgesetz – BVerfGG

mennyiben nem mérhetők a mindenkori alapjogi beavatkozás súlyához. Efféle, megfelelően kifejtett érvelések azonban csupán az ÉWA 5. § (2) bek. 11. pontjában rögzített intézkedésekre vonatkozóan találhatók.

III.

154

A 2-ben megnevezett panaszosok alkotmányjogi panasza is befogadható, amennyiben az ÉWA 17. §-a ellen irányul. Ennyiben a Szövetségi Alkotmánybíróságról szóló törvény 93. § (3) bekezdésében rögzített, a panasz benyújtására nyitva álló határidő teljesül. AZ ÉWA 5. § (2) bek. 11. pontjának hatályba lépésével az ÉWA 17. § szerinti általános továbbítási szabályozás alkalmazási területe kiterjed az újonnan szabályozott intézkedésekre és így részben kibővül. Ezáltal a panasznak egy új, alapjogi oka áll fenn, amely a panasz benyújtására nyitva álló határidő számítását újraindítja. A 2-ben megnevezett panaszosok kifogása a panasznak erre az új okára korlátozódik.

IV.

155

Az 1b-ben megnevezett panaszosok alkotmányjogi panasza annyiban is befogadható, amennyiben az ÉWA 5a § (1) bekezdése ellen irányulnak. Az 1b-ben megnevezett panaszosok kifogása a norma alkalmazási területének az alkotmányvédelmi törvény módosításával megvalósuló kiterjesztésére korlátozódik.

156

Az 1a-ban megnevezett panaszos az ÉWA 5a § (1) bekezdésére vonatkozó alkotmányjogi panasza ellenben nem befogadható, mert nem mutatta be, hogy a támadott norma érinti-e őt magát, s az érintettsége jelenleg is fennáll-e. Ehhez ki kellett volna fejtenie, hogy a támadott jogi normákon nyugvó intézkedések néni valószínűséggel az ő alapjogait is érintik. Ez itt nem látható. Az 1a-ban megnevezett panaszos semmiféle olyan állítást nem fogalmazott meg, amelyből akár csekély valószínűséggel is kitűnne, hogy számlatartalmának adatai iránt az Alkotmányvédelmi Hatóság érdeklődést mutatna. AZ ÉWA 5a § (1) bekezdésének a tényállásra vonatkozó előfeltételeire és a szabályozott intézkedések jellemzőire való tekintettel nem lehet gyakorlatilag bárkinek a lehetséges érintettségére következtetni.

V.

157

Amennyiben a 2-ben megjelölt panaszosok alkotmányjogi panasza az ÉWA 7. § (2) bekezdése ellen irányul, a Szövetségi Alkotmánybíróságról szóló törvény 93. § (2) bekezdésében rögzített, a panasz benyújtására nyitva álló határidő nem teljesül. Ez a rendelkezés már 1994-ben hatályba lépett. Itt nincs jelentősége annak, hogy a törvényhozó az alkotmányvédelmi törvény módosítása alkalmával azt az ÉWA 7. § (2) bekezdésébe akaratával megegyezően ismét felvette, mivel ezáltal a panasz benyújtására nyitva álló határidő számítása nem indul újra.

158

A 2-ben megnevezett panaszosoknak amiatt, hogy az ezzel a ponttal kapcsolatos alkotmányjogi panasz nem befogadható, megmarad a lehetőségük a támadott norma alkotmányellenessége kifogásolására. Ha a 2-ben megnevezett panaszosok tartanak attól, hogy az ÉWA 7. § (2) bekezdésében rögzített intézkedések érintettjei lesznek, azzal szemben a Közigazgatási Bíróságoktól nyerhetnek védelmet. Ennek során elvileg mind ideiglenes, mind megelőző jogvédelemben részesülhetnek. Az a körülmény, hogy ehhez elegendő jogvédelmi érdeket és egy terhelő intézkedés alkalmazásának elegendő valószínűségét kell igazolni, a szakági bíróság által biztosított jogvédelem alapvető lehetőségét nem zárja ki. A szakági bíróság eljárása során a jogvédelmi érdekre vonatkozó követelmények a hatékony alapjogi védelmet nem múlhatják felül.

VI.

159

A 2-ben megnevezett panaszosok alkotmányjogi panasza annyiban sem befogadható, amennyiben az ÉWA 10. és 11. §-ával összefüggésben az ÉWA 8. § (4) bek. 2. mondata ellen irányulnak, amely az elektronikus esetiratokban rögzített személyes vonatkozású adatok kezelésére vonatkozik. E szabályozás tekintetében az alkotmányjogi panasz nem felel meg a szubszidiaritás elvének.

160
A szubszidiaritás elve szerint a támadott jogi normával érintett alapjogi alany alkotmányjogi panasza akkor nem befogadható, ha a bírósághoz fordulva elvárható módon jogvédelemben nem részesülhet. Ezzel elkerülhető, hogy a Szövetségi Alkotmánybíróság bizonytalan tényeken és jogokon alapuló, messze ható határozatokat hozzon.

161
Eszerint a 2-ben megnevezett panaszosok a személyes vonatkozású, elektronikus esetiratokban rögzített adatok kezeléséről rendelkező szabályozással szemben jogvédelemért mindenekelőtt a szakági bírósághoz fordulhatnak.

162
A 2-ben megnevezett panaszosok ugyancsak kifogásolják az alkotmányvédelmi törvénynek a szerintük már nem szükséges személyes vonatkozású adatok tárolására vonatkozó szabályozását. Azt, hogy a törvény ilyen adatok törlését kizárja, mindenekelőtt az alkotmányjogon kívüli hatóságoknak és más szakági bíróságoknak kell tisztáznia. AZ ÉWA 10. §-ának szövegezése azt semmi esetre sem zárja ki, hogy az e rendelkezés értelmében vett törlési szabályokat azokra az adatokra is alkalmazzák, amelyeket az elektronikus esetiratok rögzítenek. A törvény egyébként nem tartalmaz kifejezett szabályozást a már nem szükséges elektronikus esetiratok kezelésére vonatkozóan, úgyhogy a jogi helyzet ennyiben sem egyértelmű.

163
A 2-ben megnevezett panaszosok számára észszerű, hogy az alkotmányjogon kívüli helyzetet az illetékes szakági bíróságok tisztázzák. A panaszosokat egyébként éppen ezért ténylegesen semmi sem gátolja, hogy a bírósághoz forduljanak, mert az őket érintő adattárolásról tudomást nem szerezhetnek. A 2-ben megnevezett panaszosok véleményével ellentétben az ÉWA 14. § (1) bekezdésének szövegéből nem adódik az a kényszer, hogy az elektronikus esetiratok személyes vonatkozású, az ebben a normában szabályozott értesítési kötelezettséggel kapcsolatos adatait eleve felvegyék, úgyhogy nincs kizárva, hogy ennyiben az értesítést meg kell adni. Ezen felül a 2-ben megnevezett panaszosoknak az ÉWA 8. § (4) bek. 2. mondata ellen irányuló kifogása nem egy olyan, célzott alapjogi beavatkozás kiküszöbölésére irányul, amelyet egy utólagos jogvédelem csak korlátozottan képes orvosolni. Inkább anyagi jogi törlési igényeket kívánnak érvényesíteni, amelyek a szakági bírósági eljárásban is biztosíthatók.

164
Amennyiben az 1-ben megnevezett panaszosok az ÉWA 13. § alkotmányellenességét kifogásolják, alkotmányjogi panaszuk a követlen érintettség hiánya miatt nem befogadható. AZ ÉWA 13. § az Alkotmányvédelmi Hatóságnak lehetőséget ad arra, hogy adatokat közös adatállományokba vonjon össze, amelyeket szövetségi vagy tartományi rendelkezéseknek megfelelően kezelnek. Csupán ezeknek az egyéb rendelkezéseknek az alapján lehet olyan intézkedéseket tenni, amelyek alapjogi beavatkozásnak lehetne tekinteni. AZ ÉWA 13. § nyitott normája, amely az adatállomány-kezelésre vonatkozó releváns szabályozás nélkül kiüresedik, magában véve irreleváns. A tekintetbe vett normákat azonban, mint amilyenek például a 2006. december 22-én hatályba lépett antiterrorista adatállományokról szóló törvény rendelkezései, az 1-ben megnevezett panaszosok alkotmányjogi panasza nem támadja.

C.
165
Az alkotmányjogi panaszok, amennyiben befogadhatók, messzemenően megalapozottak. Az ÉWA 5. § (2) bekezdés 11. pontja második, ott rögzített fordulatát tekintve alkotmányellenes és semmis (I).

Ugyanez érvényes e norma 2. fordulatára (II). A semmisség következtében elintézést nyernek az ÉWA 5. § (3) és 17. § ellen irányuló kifogások (III). AZ ÉWA 5a § (1) bekezdésével szemben viszont alkotmányjogi aggályok nem merülnek fel (IV).

I.

166

Az ÉWA 5.§ (2) bekezdés 11. pont 1. mondat 2. fordulata, amely az IT-rendszerekhez való titkos hozzáférést szabályozza, sérti az általános személyiségi jognak az IT-rendszerek bizalmas volta és sérthetetlensége biztosítására vonatkozó alapvető jogként való különös megjelenési formáját.

167

Az általános személyiségi jog e megjelenési formája az IT-rendszerekbe való beavatkozás ellen véd, ha ilyen védelmet más alapjogok, mint különösen az Alaptörvény 10. cikke vagy 13. cikke, továbbá az információs önrendelkezési jog nem nyújtanak (1). A beavatkozás alkotmányjogilag nem igazolható: az ÉWA 5.§ (2) bekezdés 11. pont 1. mondat 2. fordulata nem felel meg a normavilágosság követelményének (2a), nem érvényesíti az arányosság elvét (2b), s a norma továbbá nem tartalmaz elegendő intézkedést a magánéletvitel belső magjának védelmére (2c). A támadott norma semmis (2d). Egyéb alapjogok további vizsgálatára nincs szükség.

168

1. Az ÉWA 5.§ (2) bekezdés 11. pont 1. mondat 2. fordulata felhatalmazást ad az általános személyiségi jogba, annak az IT-rendszerek bizalmas volta és sérthetetlensége biztosítására vonatkozó alapvető jogként való különös megjelenési formájába való beavatkozásra; ez összefüggésben áll ennek az alapjognak egyéb megjelenési formáival, mint például az információs önrendelkezési joggal, továbbá az Alaptörvény 10. és 13. cikkében rögzített szabadságok biztosításával.

169

a) Az általános személyiségi jog a személyiségnek azokat az elemeit védi, amelyek nem képezik tárgyát az Alaptörvény különös szabadságainak, konstitutív jelentőségük azonban azokéval összemérhető. Egy ilyen hézagpótló védelem különösen az újszerű veszélyekkel szemben szükséges, melyekkel a tudományos-technikai fejlődés és a megváltozott életviszonyok következtében találkozunk. Egy konkrét jogvédelmi intézkedés hozzárendelésének a személyiségi jog különféle aspektusaihoz mindenek előtt a személyiség fenyegetettsége módjához kell igazodnia.

170

b) Az IT használata az egyén személyiségét és kibontakozását tekintve korábban be nem látható jelentőségre tett szert. A modern információtechnika új lehetőségeket kínál az egyénnek, ugyanakkor újfajta veszélyeket is jelent a személyiségnek.

171

aa) Az IT fejlődésének újabb eredményei oda vezettek, hogy az IT-rendszerek mindenütt jelen vannak és használatuk sok polgár életvitelében központi jelentőségűvé vált.

172

Ez mindenekelőtt a személyi számítógépekre jellemző, amelyeket az ország háztartásainak többségében használnak. Az efféle számítógépek teljesítménye, operatív tárának és egyéb, hozzá kapcsolt tároló eszközeinek kapacitása egyaránt megnőtt. A személyi számítógépeket manapság számos különféle célra használhatjuk, saját személyes vagy üzleti ügyeink átfogó intézésére és archiválására éppen úgy, mint digitális könyvtárként vagy számos lehetséges szórakozási forma eszközeként. Mindennek megfelelően a személyi számítógép jelentősége a személyiség kibontakoztatására nézve felettébb megnőtt.

173

Az IT-nek az egyéni életvitellel való összefüggése nem merül ki a személyi számítógépek növekvő elterjedésében és teljesítményében. Számos egyéb, a lakosság nagy része által naponta használt eszköz

létezik, amely IT-elemeket tartalmaz. Ilyenek például azok a távközlési és elektronikus készülékek, amelyek sok-sok lakásban vagy gépjárműben fellelhetők.

174
bb) Az IT-rendszerek teljesítménye és a személyiség kibontakozásában betöltött jelentősége tovább növekszik, ha e rendszereket egymással összekapcsoljuk, mint ahogyan az mind jobban megszokottá vált a lakosság széles köreiben az Internet növekvő használata által.

175
Az IT-rendszerek hálózatba kapcsolása általában lehetővé teszi feladatok e rendszerek közti szétosztását és a számítási összteljesítmény növelését. Így például a hálózatba kapcsolt egyedi rendszerekből származó adatok kiértékelhetők és a rendszerek meghatározott reakciókra késztethetők. Ily módon az egyes rendszerek funkcióképessége is kibővíthető.

176
Különösen az Internet mint számítógép-hálózatok komplex összessége nyújt egy rákapcsolódó számítógép használójának hozzáférést az információ egy gyakorlatilag beláthatatlan halmazához, amelyet más, a hálózatra kapcsolt számítógépek kínálnak. Mindemellett számos egyéb, újszerű kommunikációs szolgáltatás áll rendelkezésünkre, melyek igénybe vételével aktív társadalmi kapcsolatokat létesíthetünk és ápolhatunk. Mindezen felül a technikai konvergencia oda vezet, hogy a távközlés hagyományos formái is mind nagyobb terjedelemben megjelennek az Interneten is (pl. a beszédtelefon).

177
cc) A hálózatba kapcsolt IT-rendszerek növekvő elterjedése azonban az egyén számára nem csak a személyiség kibontakoztatását segítő lehetőségeket kínál, hanem újabb, a személyiséget fenyegető veszélyekkel is jár.

178
(1) Ezek a veszélyek már abból is adódnak, hogy a komplex IT-rendszerek, köztük személyi számítógépek a használat lehetőségeinek széles spektrumát nyitják meg, mely lehetőségek mindegyike adatok előállításával, feldolgozásával és tárolásával jár. Hangsúlyozni kell, hogy nem csak olyan adatokról van szó, melyeket a számítógép felhasználója tudatosan megad vagy tárol. Az adatfeldolgozási folyamat során az IT-rendszerek maguk is sok egyéb adatot állítanak elő, amelyeket éppen úgy, mint a felhasználó által tárolt adatokat, viselkedése és tulajdonságai értékelésére használhatnak fel, aminek következtében az ilyen rendszerek operatív tárában és tároló eszközein számos, a használó személyes körülményeire, társadalmi kapcsolataira és tevékenységére vonatkozó adatok találhatók. Ha ezeket az adatokat harmadik személy megszerzi és kiértékeli, messzemenő következtetéseket vonhat le a használó személyiségére nézve, sőt azokból személyiségi profilját is elkészítheti.

179
(2) Egy hálózatra, különösen egy Internetre kapcsolódó rendszer esetében e veszélyek különféle vonatkozásokban fokozódnak. A felhasználási lehetőségeknek a hálózatba kapcsolásból adódó bővülése például azzal jár, hogy még több és még többféle adat keletkezik és képezi további feldolgozás vagy tárolás tárgyát, mint egyedi rendszerek esetében. Ezek az adatok mind a kommunikációs tartalmak, mind a hálózati kommunikációval összefüggő adatok lehetnek. A használó viselkedésére vonatkozó adatok tárolása és kiértékelése a személyiségére vonatkozó mély információkhoz vezethet.

180
A rendszer hálózatba kapcsolása azonban mindenek előtt technikai hozzáférési lehetőséget nyújt, mely arra is felhasználható, hogy a rendszerben fellelhető adatokat kikémleljék vagy manipulálják. Az egyén ilyen hozzáférésekről az esetek többségében tudomást sem szerezhet, s még kevésbé tudja azokat elhárítani. Az IT-rendszerek időközben olyan bonyolulttá váltak, hogy a társadalmi vagy

technikai önvédelem nagy nehézségekkel jár és az átlagos felhasználó lehetőségeit mindenképpen meghaladja. A technikai önvédelem ráadásul magas költséggel vagy a védett rendszer funkcióiba való beavatkozással járhat. Az önvédelem számos lehetősége – mint pl. az érzékeny adatok kódolása vagy elleplezése – egyébiránt meglehetősen hatástalan, ha harmadik személynek az adatokat tartalmazó rendszerbe egyszer már sikerült betelepülni. Végül az információtechnológia fejlődésére vonatkozó prognózisok nem adnak megbízható információt arra vonatkozóan, milyen technikai önvédelmi lehetőségei lesznek a felhasználónak a jövőben.

181
c) Az a jelentős szerep, melyet az IT-rendszerek használata a személyiség kibontakoztatásában játszik, továbbá azok a veszélyek, melyek e használat során a személyiséget fenyegetik, alapjogilag fokozott védelmi szintet igényelnek. Az egyén arra számít, hogy e rendszerek integritásával szemben táplált jogos elvárásait, tekintettel a személyiség korlátozástól mentes kibontakoztatására, az állam tiszteletben tartja. Sem az Alaptörvény 10. és 13. cikke alapjogi garanciái, sem az általános személyiségi jognak az Alkotmánybíróság korábbi ítéleteiben kialakított megjelenési formái nem veszik kellő súllyal figyelembe az információtechnológia fejlődéséből fakadó védelmi igényt.

182
aa) Az Alaptörvény 10. cikk (1) bekezdésben rögzített távközlési titok garantálása a távközlésforgalmi eszközök segítségével védi az információnak a címzett egyénhez való immateriális átvitelét, az IT-rendszerek bizalmas voltát és integritását azonban nem.

183
(1) Az Alaptörvény 10. cikk (1) bek. a távközlést mint olyat védi, tekintet nélkül az átvitel módjára (kábel vagy rádióhullám, analóg vagy digitális továbbítás) és az átvitt információ megjelenési formájára (beszéd, kép, hang, jel vagy egyéb adatok). A távközlési titok védelme ezért felöleli az Internet kommunikációs szolgáltatásait is. Hangsúlyozni kell, hogy a védelem nem csupán a távközlési eszközön továbbított tartalomra vonatkozik, hanem a távközlés körülményeire is. Ide tartoznak különösen a következő adatok: mikor, milyen gyakran és mely személyek vagy távközlési berendezések között zajlott távközlési forgalom vagy került kezdeményezésre. E keretek között a távközlési titoknak szembe kell néznie a személyiséget fenyegető régi és új veszélyekkel, amelyek az információtechnikának az egyén kibontakozásában játszott növekvő jelentőségéből adódnak.

184
Ha a felhatalmazás olyan állami intézkedésre korlátozódik, melynek révén a számítógép-hálózaton folyamatban lévő távközlés tartalma és körülményeinek adatai megszerezhetők vagy az ezekre vonatkozó adatok kiértékelhetők, a beavatkozást egyedül az Alaptörvény 10. cikk (1) bekezdéséhez kell mérni. Az alapjog védelmi területe független attól, hogy az intézkedés technikailag az átviteli hálózaton vagy a hálózati végberendezésben valósul meg. Ez elvileg akkor is érvényes, ha a végberendezés egy hálózatba kapcsolt komplex IT-rendszer, melynek távközlési eszközként való használata több használati lehetőségének csupán az egyike.

185
(2) Az AT 10. cikk (1) bekezdésében rögzített alapjogi védelem egyébként nem terjed ki a távközlés tartalmának és körülményeinek a kommunikáció résztvevője magánterületén, a kommunikációs folyamat befejezését követően tárolt adatokra, ha az adatok titkos hozzáférésével szemben maga is óvintézkedéseket tehet. Ez esetben ugyanis már nem állnak fenn a térben elkülönült kommunikációt fenyegető sajátos veszélyek, amelyek ellen a távközlési titoknak kell védelmet nyújtania.

186
(3) A távközlési titok védelme akkor sem áll fenn, ha egy állami szerv az IT-rendszer mint olyan használatát megfigyeli vagy a rendszer tároló eszközeit átkutatja. A folyamatban lévő távközlésen kívül eső tartalom vagy körülmények adatainak megszerzése az Alaptörvény 10. cikk (1) bek. szerint akkor sem áll fenn, ha a megszerzett adatoknak a kiértékelésüket végző hatósághoz való továbbítására olyan távközlési kapcsolatot használnak, mint amilyen pl. az online-hozzáférés tárolt adatokhoz.

187
(4) Ha az IT-rendszerhez való titkos hozzáférés olyan adatokra irányul, amelyeket az AT 10. cikk (1) bek. hozzáféréssel szemben nem véd, védelmi hézag áll fenn, amelyet az általános személyiségi jognak kell zárnia, mely itt az IT-rendszerek bizalmas volta és sérthetetlensége védelme formájában jelenik meg.

188
Ha egy komplex IT-rendszerbe a távközlés megfigyelése céljából a betelepülést végrehajtották („a távközlés forrásának megfigyelése“), elhárult az akadálya annak, hogy a rendszert a maga teljességében kikémleljék. Ez a veszély messze túlmutat azon, amely a folyamatban lévő távközlés puszta megfigyelésével kapcsolatos. Íly módon olyan, a személyi számítógépben tárolt adatokhoz is hozzá lehet férni, amelyeknek a rendszer távközlési használatához semmi közük sincsen. Ilyenek például: a személyi számítógép magáncélú használatának jellemzői, egyes szolgáltatások igénybevételének gyakorisága, különös tekintettel a módosított adatállományok tartalmára vagy – ha a rendszer háztartási készülékeket vezérel – a lakáson belüli viselkedési szokások.

189
A meghallgatott szakértők szerint egyébként az is megtörténhet, hogy a betelepülés révén olyan adatokhoz is jutnak, jóllehet szándékuk ilyenre nem irányul, amelyeknek a folyamatban lévő távközléshez semmi közük sincsen. Következésképpen – eltérően a hagyományos távközlési hálózaton folyó kommunikáció megfigyelésétől – fennáll annak a kockázata, hogy a távközlés tartalmán és körülményein kívül további személyes vonatkozású információkhoz is jutnak. A személyiséget ezáltal érő sajátos veszélyekkel szemben az Alaptörvény 10. § (1) bek. nem nyújt védelmet vagy nem elegendő védelmet nyújt.

190
Az Alaptörvény 10. cikk (1) bek. ezzel szemben az egyetlen alapjogi mértéke „a távközlés forrásának megfigyelésére“ vonatkozó felhatalmazás megítélésének, ha a megfigyelés kizárólag az aktív távközlési folyamatból származó adatokra korlátozódik, amit technikai intézkedésekkel és jogi előírásokkal kell biztosítani.

191
bb) Az Alaptörvény 13. cikk (1) bek. garantálja ugyan a magánlakás, s ezáltal – tekintettel emberi méltóságára és személyisége kibontakozásának érdekében – az egyén alapvető élettere sérthetetlenségét, melybe csak az Alaptörvény 13. cikk (2) – (7) bekezdésében rögzített feltételek mellett lehet beavatkozni, meghagyja azonban az IT-rendszerekhez való hozzáféréssel szemben jelentkező védelmi hézagot.

192
Az alapjogi védelem tárgya itt az a térbeli szféra, melyben a magánélet kibontakozik. Az Alaptörvény 13. cikk védelme a magánlakások mellett az üzemi és üzleti helyiségekre is kiterjed. Az alapjogi védelem mindazonáltal nem csak a lakásba való fizikai behatolás elhárítását öleli fel. Az Alaptörvény 13. cikkében rögzített beavatkozásnak kell tekinteni azokat az intézkedéseket, amelyekkel az állami szervek sajátos eszközök segítségével – a védett téren kívülről – bepillantást nyernek a lakáson belül zajló folyamatokba, például a lakótér akusztikus vagy optikai megfigyelésével, vagy éppenséggel annak az elektromágneses sugárzásnak a mérésével, amellyel egy IT-rendszer használata megfigyelhető. Ez arra a rendszerre is vonatkozik, amely off-line működik.

193
Egy IT-rendszerhez való titkos technikai hozzáféréssel kapcsolatos állami intézkedést ezen túlmenően az Alaptörvény 13. cikk (1) bek. szerint kell megítélni, például ha és amikor a nyomozó hatóság munkatársai egy lakásként védett helyiségbe behatolnak, hogy egy ott található IT-rendszert fizikailag manipuláljanak. Az Alaptörvény e rendelkezése alkalmazásának további esete a betelepülés a lakásban található IT-rendszerbe, hogy annak segítségével bizonyos, a lakáson belül zajló folyamatokat

megfigyeljenek, melyhez például a rendszerhez kapcsolt perifériás eszközt, mikrofont, kamerát stb. használnak.

194
Az Alaptörvény 13. cikk (1) bek. egyébként nem nyújt általános, a hozzáférés módjától független védelmet az IT-rendszerbe való titkos betelepülés ellen, még akkor sem, ha a rendszer egy lakásban található. Minthogy a behatolás a helyszíntől függetlenül hajtható végre, a térbeli védelem az IT-rendszerek sajátos veszélyeztetését nem háríthatja el. Ha a behatolás az érintett számítógépnek egy számítógép-hálózatra való kapcsolódását kihasználja, a lakás térbeli határaival biztosított magánszféra érintetlen marad. A rendszer fizikai elhelyezkedésének a nyomozási intézkedések szempontjából sok esetben nincs jelentősége, sőt a hatóságok számára – különösen mobil IT-rendszerek, hordozható személyi számítógépek, PDA-ak, mobil telefonok stb. – esetében egyenesen felismerhetetlen.

195
Az Alaptörvény 13. cikk (1) bek. nem véd továbbá azoknak az adatoknak a megszerzésétől sem, amelyek – mint az IT-rendszer operatív tárában vagy egyéb tároló eszközein rögzített adatok – a lakásban található rendszerbe való betelepüléssel váltak hozzáférhetővé.

196
cc) Az általános személyiségi jogoknak a Szövetségi Alkotmánybíróság korábbi ítéleteiben elismert megjelenési formái, különösen a magánszféra és az információs önrendelkezési jog védelmének garantálása sem nyújtanak kellő mértékű védelmet az IT-rendszer használóját fenyegető különös veszélyekkel szemben.

197
(1) Az általános személyiségi jog különös, a magánszféra védelmeként megjelenő formája az egyénnek egy térben és tematikailag meghatározott területet biztosít, amelynek alapjogilag a nem kívánt megfigyeléstől mentesnek kell maradnia. Egy IT-rendszer használójának védelmi igénye azonban nem csupán azokra az adatokra korlátozódik, amelyek a privátszférájával vannak összefüggésben. Egy ilyen összefüggés gyakran attól a kontextustól függ, melyben az adatok keletkeznek és melyben vagy melyekben egyéb adatokhoz kapcsolódnak. Az adaton magán sokszor nem látszik, mi a jelentősége az érintett számára és milyen jelentőségre tehet szert más adatokkal összefüggésben. Ennek az a következménye, hogy a rendszerbe való betelepülés révén nem csupán elkerülhetetlenül személyes adatok szerezhetők meg, hanem minden adat hozzáférhetővé válik, melyekből a rendszer használójáról részletes kép alkotható.

198
(2) Az információs önrendelkezési jog túlnyúlik a magánszféra védelmén, s elvileg az egyént jogosítja fel arra, hogy személyes adatai megadásáról és felhasználásáról határozzon. Ez a jog a magatartás szabadsága és a magánszféra alapjogi védelmével határos, azt kibővíti azáltal, hogy azt már a személyiség veszélyeztetése kezdetének tekinti. A veszélyeztetettségnek ilyen helyzete állhat elő megnevezhető jogok konkrét fenyegetettsége előterében, különösen ha személyes információkat oly módon használnak és kapcsolnak össze, melyet az érintett sem átlátni, sem megakadályozni nem tud. Az információs önrendelkezési jog védelme mindazonáltal nem csak azokra az információkra terjed ki, melyek jellegüknél fogva érzékenyek és már ezért alapjogi védelemben részesülnek. Azoknak az adatoknak a kezelése is – a hozzáférés céljától, továbbá a rendelkezésre álló feldolgozási és összekapcsolási lehetőségektől függően – alapjogi jelentőségű kihatásai lehetnek az érintett magánszférájára és magatartása szabadságára, amelyeknek önmagukban kevés az információtartalmuk.

199
A személyiséget fenyegető veszélyek, melyekkel szemben az információs önrendelkezési jognak védelmet kell nyújtania, abból a sokféle lehetőségből adódik, amely az államnak és adott esetben magánszemélyeknek a személyes adatok megszerzésére, feldolgozására és felhasználására rendelkezésre állnak. Ezekből az adatokból, főleg elektronikus adatfeldolgozás segítségével, további

információk állíthatók elő és olyan következtetések vonhatók le, amelyek veszélyeztethetik az érintett alapjogilag védett titoktartási érdekeit, és beavatkozást jelenthetnek magatartási szabadságába is.

200
Az információs önrendelkezési jog azonban nem nyújt teljes körű védelmet a személyiséget fenyegető veszélyekkel, különösen azokkal szemben, amelyek abból adódnak, hogy személyisége kibontakoztatásában az egyén az IT-rendszerek használatára van utalva, miközben személyes adatait a rendszerre bízza vagy már csupán a rendszerek használata által kényszerűen kiszolgáltatja. Az a harmadik személy, aki egy ilyen rendszerhez hozzáfér, potenciális rendkívül széles és jelentőségteljes adatállományt képes megszerezni, anélkül hogy további adatgyűjtési vagy feldolgozási műveleteket kellene végeznie. Az ilyen hozzáférés súlya az érintett személyiségére nézve messze meghaladja az egyedi adatgyűjtésekét, melyekkel szemben az információs önrendelkezési jog védelmet nyújt.

201
d) Amennyiben a személyiséget fenyegető azon veszélyekkel szemben, amelyek abból adódnak, hogy személyisége kibontakoztatásában az egyén az IT-rendszerek használatára van utalva, nincs elegendő védelem, az általános személyiségi jog a védelem szükségességét hézagpótló, korábban már elismert megjelenési formájának funkciójában azáltal veszi számításba, hogy biztosítja az IT-rendszer integritását és bizalmas voltát. Ez a jog, akárcsak az információs önrendelkezési jog, az Alaptörvény 2. cikk (1) bekezdésében foglalt, azt az Alaptörvény 1. cikk 2. bekezdésével összefüggésben értelmezett rendelkezésén alapszik, védi a személyes szférát és a magánélet területét az információtechnika körében az állami hozzáféréssel szemben annyiban is, amennyiben az az IT-rendszerek összessége, s nem csupán egyedi kommunikációs folyamatok vagy tárolt adatok ellen irányul.

202
aa) Egyébként nem minden, személyes adatokat létrehozó, feldolgozó vagy tároló IT-rendszert szükséges önálló személyiségjogi biztosítékokkal sajátos védelemben részesíteni. Ha egy ilyen rendszer technikai konstrukciójának megfelelően csupán olyan adatokat tartalmaz, amelyek az érintett bizonyos életterületére vonatkoznak és egymással összefüggést nem mutatnak, mint pl. hálózatba nem kapcsolt elektronikus háztartási készülékek esetében, az adatállományhoz való állami hozzáférés kvalitatíve nem különbözik egyéb adatgyűjtésektől. Ilyen esetekben elegendő védelmet nyújt az információs önrendelkezési jog ahhoz, hogy az érintett titokhoz fűződő jogos érdekét biztosítsa.

203
Az IT-rendszerek integritásának és bizalmas voltának biztosítására vonatkozó alapjogot kell viszont alkalmazni, ha a hozzáférésre vonatkozó felhatalmazás olyan rendszereket érint, amelyek önmagukban vagy hálózattechnikai kapcsolataikban az érintett személyes adatainak akkora körét és olyan fajtáit tartalmazhatják, hogy a rendszerhez való hozzáféréssel lehetővé válik bepillantani egy személy életvitelének lényeges részébe vagy akár megbízható képet alkotni személyiségéről. Ez a lehetőség áll fenn például a személyi számítógéphez való hozzáférés esetében, függetlenül attól, használata helyhez kötött vagy mobilis. A használati magatartásból rendszerint nem csupán magáncélú, hanem foglalkozásbeli célokra való használat esetében is személyes tulajdonságokra vagy preferenciákra következtethetünk. A különös alapjogi védelem továbbá kiterjed olyan mobiltelefonokra és elektronikus előjegyzési naptárakra is, amelyek sok más funkcióval is rendelkeznek és többféle személyes adat létrehozására és tárolására alkalmasak.

204
bb) Az IT-rendszerek bizalmas voltának és integritásának biztosítására vonatkozó alapjog védi mindenekelőtt a használónak azt az érdekét, amely egy, a védelmi körbe tartozó IT-rendszerben létrehozott, feldolgozott és tárolt adatok bizalmas jellege megmaradásához fűződik. Az alapjogba való beavatkozást kell vélelmezni akkor is, ha a védett IT-rendszer integritását sértik, miközben a rendszerbe úgy avatkoznak bele, hogy annak szolgáltatásait, funkcióit és tárának tartalmát harmadik személyek felhasználhatják, mely esetben a rendszer kikémlelése, megfigyelése vagy manipulálása technikai akadályai elhárultak.

205
(1) Az általános személyiségi jog itt tárgyalt megjelenési formája különösen az olyan, titkos hozzáféréssel szemben nyújt védelmet, mely által a rendszerben tárolt adatok teljes egészben vagy jelentős részben kikémlelhetők. Az alapjogi védelem kiterjed a rendszer munkatárolójában és tároló eszközein ideiglenesen vagy tartósan rögzített adatokra egyaránt. Az alapjog véd továbbá az olyan eszközökkel végrehajtott adatgyűjtéssel szemben is, amelyek ugyan technikailag függetlenek az érintett IT-rendszer adatfeldolgozási folyamataitól, ám tárgyukat éppen ezek képezik. Ez a helyzet pl. egy un. billentyűzés-rögzítő hardver bevetése, valamint a képernyő vagy a billentyűzet elektromágneses sugárzásának mérése esetében.

206
(2) A bizalmassággal és az integritással kapcsolatos elvárások alapjogi védelme attól függetlenül fennáll, hogy az IT-rendszerhez való hozzáférés könnyen vagy csak nagy ráfordítással lehetséges. A bizalmassággal és az integritással kapcsolatos elvárások alapjogilag csak abban az esetben elismerendők, ha az IT-rendszert az érintett mint sajátját használja és ezért a körülményeket tekintve abból lehet kiindulni, hogy az IT-rendszer felett egyedül vagy a használatra feljogosított személyekkel együtt önállóan rendelkezik. Ha a saját IT-rendszer használata olyan IT-rendszereken keresztül történik, amelyek felett mások rendelkeznek, a használó védelme ezekre is kiterjed.

207
2. Az IT-rendszerek bizalmasságának és integritásának biztosítására vonatkozó alapjog nem korlátlan. A behatolást mind preventív, mind pedig bűnüldözési célok igazolhatják. Az egyén eközben jogának csak oly mértékű korlátozását kénytelen elviselni, amelynek alkotmányos törvényi alapja van. Az Alkotmányvédelmi Hatóság itt vizsgálandó felhatalmazása esetében ez hiányzik.

208
a) A támadott norma nem felel meg a normavilágosság és normaszabatosság követelményének.

209
aa) A szabatosság követelményének alapját az általános személyiségi jog – s annak különféle megjelenési formái – tekintetében is a jogállamiság elvében találjuk. Ez a feltétele annak, hogy a demokratikus legitim parlament mint törvényhozó az alapjogok korlátozásáról és e korlátok terjedelméről a lényeges döntéseket saját maga hozza meg úgy, hogy a kormány és a közigazgatás a cselekedeteit vezérlő és korlátozó szabályokat a törvény felölelje, s hogy a bíróságok a végrehajtás kontrollját elvégezhessék. A norma világos és egyértelmű volta továbbá azt is biztosítja, hogy az érintett a jogi helyzetet felismeri és magatartását az őt esetleg terhelő intézkedésekhez igazítja. A törvényhozó feladata, hogy a behatolás indítékait, célját és korlátait területspecifikusan, pontosan és szabatosan meghatározza.

210
A törvényhozónak a megoldandó feladatok szerint különféle lehetőségei vannak a beavatkozás előfeltételeinek szabályozására. A szabatosság követelményei is ezekre a szabályozási lehetőségekre irányulnak. Ha a törvényhozó meg nem határozott jogi fogalmakkal él, a fennmaradó bizonytalanság nem terjedhet addig, hogy az a norma által felhatalmazott állami szervek cselekvésének kiszámíthatóságát és igazságosságát veszélyeztesse.

211
bb) AZ ÉWA 5. § 2. bek. 11. pont 1. mondat 2. fordulata az előbbiek szerint azért nem felel meg a normavilágosság és normaszabatosság követelményének, mert a szabályozott intézkedés tényszerű előfeltételeit a törvény kielégítő módon nem tartalmazza.

212
(1) AZ ÉWA 5. § 2. bek. 11. pont 1. mondat 2. fordulatában megjelölt előfeltételeket két normára való utalással határozhatjuk meg. Egyikükre, az ÉWA 7. § 1. bekezdésére az ÉWA 5. § 2. bekezdése utal általában, amely viszont az ÉWA 3. § 1. bekezdését veszi figyelembe. Eszerint hírszerző-szolgálati

eszközök bevetése akkor megengedett, ha ily módon alkotmányvédelmi szempontból releváns információkat lehet szerezni. AZ ÉWA 5. § 2. bek. 11. pont 1. mondat 2. fordulata továbbá arra az esetre, ha az ÉWA 5. § 2. bek. 11. pont a levél-, posta- vagy távközlési titkot sért vagy egy ilyen sérelemmel jellegét és súlyát tekintve egyenértékű, az Alaptörvény 10. cikkéről szóló törvény erősebb előfeltételeire utal.

213
(2) A normavilágosság és normaszabatosság követelményével nem összeegyeztethető, hogy az ÉWA 5. § 2. bek. 11. pont 2. mondatában foglalt utalás az Alaptörvény 10. cikkéről szóló törvényre arra alapoz, hogy egy intézkedés az Alaptörvény 10. cikkéről szóló törvényt sérti. A válasz arra a kérdésre, hogy az Alkotmányvédelmi Hatóság nyomozási intézkedései milyen alapjogokat sértenek, komplex mérlegelést és értékelést igényel. Erre mindenekelőtt és elsősorban a törvényhozó hivatott. Az ő feladata, hogy a vonatkozó alapjogokat megfelelő törvényi rendelkezésekkel konkretizálja, miközben egy lehetséges vonatkozó alapjogra való puszta tényszerű hivatkozással a döntést arról, hogyan kell ezt az alapjogot kiteljesíteni és érvényesíteni, a normát végrehajtó közigazgatásra bízza. Egy ilyen „garanciális“ szabályozási technika nem felel meg a normaszabatosság követelményének az olyan norma esetében, mint az ÉWA 5. § 2. bek. 11. pont 1. mondat 2. fordulata, amelynek új technológiai fejlesztésekre kell reagálnia.

214
A normavilágosság követelményének hiányát még inkább elmélyíti az ÉWA 5. § 2. bek. 11. pont 2. mondatába foglalt kiegészítés, mely szerint az Alaptörvény 10. cikkéről szóló törvényre való utalás akkor is érvényes, ha a nyomozási intézkedés az Alaptörvény 10. cikkében foglaltak sérelmével „jellegét és súlyát tekintve egyenértékű”. Ily módon a szabályozott hozzáférés tényszerű előfeltétele e hozzáférés és egy olyan intézkedés összehasonlításának a kiértékelésétől függ, amelyet egy meghatározott alapjog sérelmeként kellene figyelembe venni. Ha már egy meghatározott alapjogra való puszta utalással a tényszerű előfeltételek megfelelő szabatossággal nem szabályozhatók, úgy érvényes ez arra a normára is, amely egy ilyen, normatíve tovább nem vezethető, a szabályozott intézkedésnek egy meghatározott alapjogi sérelemmel való összehasonlítását írja elő.

215
(3) AZ ÉWA 5. § 2. bek. 11. pont 2. mondatának utalása az Alaptörvény 10. cikkéről szóló törvényre továbbá azért sem felel meg a normavilágosság és normaszabatosság követelményének, mert az utalás terjedelme nincs megfelelő szabatossággal szabályozva.

216
AZ ÉWA 5. § 2. bek. 11. pont 2. mondata a titoktörvényben foglalt „előfeltételekre” utal. A norma így nyitva hagyja azt a kérdést, hogy az utalás a titoktörvény mely részére vonatkozik. Az sem világos, hogy e törvény előfeltételein csak a titoktörvény 3. §-ban szabályozott anyagi beavatkozási küszöböket kell érteni vagy egyéb előírásokat is figyelembe kell venni. Így a titoktörvény 9. és azt követő §-aiban foglalt eljárási szabályok is az e törvény szerinti beavatkozás előfeltételeinek tekinthetők. Sőt legalább azt is meg kellene gondolni, hogy az utalás kiterjedjen a titoktörvényben rögzített az anyagi beavatkozási küszöbökre és valamennyi eljárási óvintézkedésre is, ahogyan ezt az északrajna-westfáliai tartományi kormány javasolja. Eszerint megragadható lenne a titoktörvény 4. §-ban rögzített, a gyűjtött adatok kezelésére vonatkozó szabályozás és a titoktörvény parlamenti ellenőrzésről szóló 14. és azt követő §-ai normái, bár e normák olyan szabályokat tartalmaznak, amelyeket csak a beavatkozást követően kell figyelembe venni, és ezért szó szerint aligha lehet azokat a beavatkozás előfeltételeinek tekinteni.

217
Nem látható, hogy a törvény nem szabatos megfogalmazásában szabályozási nehézségek lennének vétkesek. A törvényhozónak minden további nélkül lehetősége lett volna arra, hogy az utalást tartalmazó norma a titoktörvény egyes olyan előírását felsorolja, melyre utalnia kell.

218

b) AZ ÉWA 5. § 2. bek. 11. pont 1. mondat 2. fordulata nem felel meg az arányosság alapelvének sem. Az arányosság megköveteli, hogy az alapjog korlátozása legitim célt szolgáljon, a cél elérésére alkalmas, szükséges és a célhoz mérhető legyen.

219
aa) A támadott normában előirányzott adatgyűjtések az Alkotmányvédelmi Hatóságnak az ÉWA 3. § (1) bekezdésében rögzített feladatai végrehajtását és ezáltal a konkrét veszély kialakulását megelőzően a szabad demokratikus alaprendet, a Szövetség és a tartományok fennállását, valamint a Szövetségi Köztársaság meghatározott külföldi kapcsolataira vonatkozó érdekeit védő biztonsági intézkedéseket szolgálják. AZ ÉWA módosítása az indokolása szerint azt a célt szolgálta, hogy az Alkotmányvédelmi Hatóság hatékony harcot folytathasson a terrorizmus újabb, különösen az Internet-kommunikációval összefüggésben jelentkező fenyegetéseivel szemben. Az új szabályozás alkalmazási területe egyébként sem kifejezetten, sem a terrorizmus elleni harccal való szisztematikus összefüggésének következményeként nincs korlátozva. A normát teljes alkalmazási területén igazolni kell.

220
Az államnak mint a béke és a rend fenntartásáért felelős hatalomnak a biztonsága és az általa a lakosságnak nyújtott biztonság a testet, az életet és a szabadságot fenyegető veszélyekkel szemben alkotmányos értékek, melyek rangja más, nagy értékű javakéval megegyezik. A védelmi kötelezettség alapja mind az Alaptörvény 2. cikk 2. bek. 1. mondatából, mind 1. cikk 1. bek. 2. mondatából levezethető. Az állam alkotmányjogi feladatait teljesíti, midőn terrorista vagy más törekvésekből adódó veszélyekkel szemben fellép. Az elektronikus és digitális kommunikációs eszközök növekvő használata és azok megjelenése az élet szinte minden területén, megnehezíti az Alkotmányvédelmi Hatóság feladatainak hatékony végrehajtását. A modern információtechnika számos lehetőséget kínál szélsőséges és terrorista törekvéseknek kapcsolatok kiépítésére és ápolására éppen úgy, mint a bűntettek megtervezésére, előkészítésére, sőt végrehajtására is. A törvényhozónak az IT-eszközök állami nyomozásban való használatára vonatkozó intézkedéseit mindenekelőtt annak a váltásnak a tükrében kell megítélni, melynek során a megszokott kommunikációs formák helyett egyre inkább az elektronikus hírközlés és az adatállományok titkosítása vagy elleplezése lehetőségeit veszik igénybe.

221
bb) Az IT-rendszerekhez való titkos hozzáférés alkalmas e célok szolgálatára (lásd 220.), általa kibővülnek az Alkotmányvédelmi Hatóság lehetőségei a fenyegetés felderítésére. Az alkalmasság megítélésére a törvényhozónak tág lehetősége van, s nem látható, hogy ezen a lehetőségen túllépett volna.

222
AZ ÉWA 5. § 2. bek. 11. pont 1. mondat 2. fordulatában foglalt felhatalmazás nem veszíti el alkalmasságát azáltal, hogy az érintettnek technikai önvédelmi lehetőségei vannak a hozzáférés hatékony megakadályozására, amikor is a célrendszerbe való betelepülést egy hozzáférési szoftverrel hajtják végre. Az alkalmassági vizsgálat keretében nem lehet megkívánni, hogy a támadott normával megengedett intézkedések mindig vagy csak főszabályként vezessenek sikerre. Az a törvényhozói prognózis, hogy a szabályozott módon végrehajtott hozzáférés egyedi esetben sikeres, legalábbis nem nyilvánvalóan hibás. Nem lehet magától értetődőnek venni, hogy minden lehetséges célszemély a hozzáférés ellen védő lehetőséget valóban és hibátlanul kihasználja. Egyébként az is elképzelhető, hogy az IT fejlődésével az Alkotmányvédelmi Hatóságnak olyan hozzáférési lehetősége is lesz, amely technikailag nem több vagy – éppen ellenkezőleg – aránytalan ráfordítást igényel.

223
A szabályozott felhatalmazás alkalmasságát továbbá azért sem lehet tagadni, mert annak az információnak a bizonyító ereje, melyhez a hozzáférés révén jutottak, korlátozott. E tekintetben megjegyzendő, hogy a megszerzett adatok valódiságának technikai igazolásához a célrendszernek a kérdéses időpontban való exklúzív kontrolljára lenne szükség. A bizonyító erő igazolásának ezek a nehézségei azonban nem jelentik azt, hogy a megszerzett adatoknak nincs információs értéke. A támadott norma szerinti online-hozzáférés ugyanis közvetlenül nem egy büntető eljárás számára

megdönthetetlen bizonyítékok megszerzésére szolgál, hanem az Alkotmányvédelmi Hatóságnak nyújt lehetőséget olyan információk gyűjtésére, melyek megbízhatóságával szemben – konkrét veszély bekövetkezésének megelőzésére irányuló, eltérő feladatai következtében – csekélyebb az igény, mint egy büntető eljárásban.

224
cc) Az IT-rendszerekbe való titkos hozzáférés nem sérti a szükségesség alapelvét sem. Mérlegelési jogkörében a törvényhozó feltételezheti, hogy nincs ugyanolyan hatékony, ám az érintettet kevésbé terhelő mód az ilyen rendszerekben tárolt adatok megszerzésére.

225
A célrendszernek az alkotmányvédelmi törvényben nem előírt nyílt átkutatása ugyan a titkos hozzáféréssel szemben elvileg enyhébb eljárásnak tekinthető, ha azonban az Alkotmányvédelmi Hatóságnak, feladatköréből adódóan elegendő oka van arra, hogy egy IT-rendszer tároló eszközeiben elhelyezett adatállományokat – ide értve a titkosított adatokat is – átfogóan megvizsgáljon, a módosításokat hosszabb időn át kövesse vagy a rendszer használatát átfogóan megfigyelje, úgy enyhébb eszközök ezen információk megszerzésére nem állnak rendelkezésre. Ugyanez áll az Internet-kommunikáció titkosított tartalmához való hozzáférésre, ha az ahhoz való hozzáférés az átviteli úton nem sikerülhet.

226
dd) ÉWA 5. § 2. bek. 11. pont 1. mondat 2. fordulata nem felel meg a szorosabb értelemben vett arányosság követelményének.

227
E követelmény szerint a beavatkozás súlya nem lehet aránytalan a beavatkozást igazoló okokhoz mérten. A törvényhozó az egyéni érdeket, melyet az alapjogba való beavatkozás sért, azokhoz a közösségi érdekekhez kell viszonyítania, vagyis megfelelőségét aszerint kell mérlegelni, amelyeket a beavatkozás szolgál. Az arányosság vizsgálata oda vezethet, hogy egy eszköz a közösségi érdekek érvényesítésére nem alkalmazható, mert az abból adódó alapjogi megfontolások nagyobb súllyal esnek latba, mint az érvényesíteni kívánt érdekek.

228
AZ ÉWA 5. § 2. bek. 11. pont 1. mondat 2. fordulata ennek nem felel meg. Az ebben a normában előírt intézkedések olyan intenzív alapjogi beavatkozással járnak, amely a beavatkozás szabályozott okából adódó közösségi nyomozati érdekekkel nem áll arányban. Szükség van további alkotmányjogi előírásra is, mely figyelembe veszi az érintett alapjogilag védett érdekeit.

229
(1) AZ ÉWA 5. § 2. bek. 11. pont 1. mondat 2. fordulata az alapjogba való nagy intenzitású beavatkozásra ad felhatalmazást.

230
Egy állami adatgyűjtés komplex IT-rendszerekből hallatlan lehetőséget kínál az érintett személyiségének kikutatására. Ez már olyan, egyszeri és célzott hozzáférésre is fennáll, amely például ilyen rendszerek tároló eszközeinek elkobzása vagy lemásolása.

231
aa) Egy ilyen titkos hozzáférés egy IT-rendszerbe olyan adatállományhoz nyit hozzáférést a cselekvő állami szervnek, amely a hagyományos információforrások terjedelmét és fajtáit messze felülmúlja. Ez annak a számos különféle használati lehetőségnek a következménye, amelyet a komplex IT-rendszerek nyújtanak a személyes adatok létrehozására, feldolgozására és tárolására nyújtanak. Ezeket az eszközöket a jelenlegi tipikus használati szokások szerint tudatosan fokozottan érzékeny személyes adatok – személyes szöveg-, kép- vagy hangfájlok – tárolására használják. A rendelkezésre álló adatállomány, amely felöleli a különféle kommunikációs csatornákon megvalósított magán- és üzleti

levelezést vagy még a naplószerű személyes feljegyzéseket is, részletes információval szolgál az érintett személyes körülményeire és életvitelére vonatkozóan.

232
Az állami hozzáférés egy ilyen átfogó adatállományhoz azzal a nyilvánvaló kockázattal jár, hogy a megszerzett adatok összességükben messzemenő következtetések levonását teszik lehetővé érintett személyiségére nézve, amely egészen a viselkedési és kommunikációs profilok összeállításáig terjedhet.

233
(bb) Ha olyan adatok megszerzésére kerül sor, amelyek az érintettnek harmadik személyekkel folytatott kommunikációjára vonatkozó információval szolgálnak, az alapjogi beavatkozás intenzitása tovább fokozódik azáltal, hogy a polgár lehetősége – ami egyébként a közjónak is eleme – abban is korlátozódik, hogy egy megfigyelésmentes távolsági kommunikációban részt vegyen. Ilyen adatok megszerzése közvetve csorbítja a polgár szabadságát, mert a megfigyeléstől való félelem, még ha csak utólag jelentkezik is, akadályozhatja az elfogulatlan egyéni kommunikációt. Ezenfelül az adatok ilyen megszerzése a beavatkozás súlyát növeli abban az esetben is, amikor a célszemély kommunikációs partnerével a megfigyelés szükségképpen harmadik személyekre is kiterjed, anélkül hogy felmerülne, fennállnak-e az ilyen hozzáférés előfeltételei.

234
(b) Az alapjogi beavatkozás különösen súlyos, ha – mint ahogyan ezt a támadott norma rögzíti – a titkos betelepülés a rendszer használatának tartós megfigyelését és a megfelelő adatok folyamatos gyűjtését teszi lehetővé.

235
(aa) Az ilyen hozzáféréssel nyerhető adatok volumene és sokfélesége jelentősen nagyobb, mint egy egyszeri és célzott adatgyűjtés esetében. A hozzáférés által a munkatárolóban csupán átmenetileg megjelenő adatok vagy a célrendszer tároló eszközeiben ideiglenesen tárolt adatok is hozzáférhetővé válnak. Ezenfelül lehetővé teszi az érintett Internet kommunikációjának tartós és teljes körű követését. Egyébként a nyomozás hatókörét az is növelheti, ha a célrendszer egy (helyi) hálózatra csatlakozik, mert a hozzáférés arra is kiterjed.

236
Az átmenetileg vagy csak ideiglenesen tárolt adatok különös relevanciát mutathatnak az érintett személyére nézve vagy további, különösen érzékeny adatokhoz való hozzáférést tehetnek lehetővé, így például a cache-tárban megjelenő adatokhoz, amelyeket kiszolgáló-programok, pl. web-böngészők helyeznek el, s melyek kiértékelése ilyen programok használatáról és ezáltal közvetve az érintett preferenciáiról és kommunikációs szokásairól nyújthat információt, vagy a jelszavakhoz, melyekkel az érintett saját rendszere vagy a hálózat technikailag védett tartalmaihoz férhet hozzá. Ezenfelül az Internet-kommunikáció tartós megfigyelése, amit a támadott norma lehetővé tesz, a kommunikáció tartalmának és körülményeinek egyszeri megfigyelésével szemben ugyancsak jelentősen intenzívebb beavatkozás. Végül figyelembe kell venni, hogy a szabályozott hozzáférés egyebek mellett arra is módot ad és arra is alkalmas, hogy a titkosítást megkerülje. Ily módon az érintett saját védelmi intézkedéseit is, amelyeket adatainak az általa nem kívánt hozzáférésével szemben foganatosított, ki lehet küszöbölni. Az ilyen információs önvédelem hatálytalanítása növeli az alapjogi beavatkozás súlyát.

237
A magatartási és kommunikációs profilok képzésének kockázata is növekszik azáltal, hogy a célrendszer használatát hosszabb időn keresztül átfogóan megfigyelik. A hatóság ily módon az érintett személyes körülményeit és kommunikációs magatartását messzemenően kikutathatja. A személyes adatok ilyen átfogó felvételét különösen nagy intenzitású alapjogi beavatkozásnak kell tekinteni.

238

(bb) A szabályozott hozzáféréssel végrehajtott beavatkozás intenzitását továbbá annak titkossága is meghatározza. Egy jogállamban az állami beavatkozás titkossága kivételes és ezért különös jogszabályi feltételei vannak. Ha az érintett egy őt terhelő állami intézkedésről annak végrehajtását megelőzően szerez tudomást, érdekeit azzal szemben eleve védheti. Egyrészt jogi eljárást kezdeményezhet ellene, például bírósági védelmet vehet igénybe. Másrészt egy nyíltan végrehajtott adatfelvétel esetében tényleges lehetősége van arra, hogy magatartásával a nyomozás folyamatára hatást gyakoroljon. E hatás lehetőségének kizárása fokozza az alapjogi beavatkozás súlyát.

239
(cc) A beavatkozás súlyát végül az is befolyásolja, hogy a hozzáférés következtében veszélyeztetve lesznek a célrendszer integritása, valamint az érintett, sőt harmadik személyek egyéb jogai is.

240
Szakértők szerint nem lehet kizárni, hogy a hozzáférés maga már kárt okoz a számítógépben. Így például az operációs rendszerrel való kölcsönhatás adatvesztéshez vezethet. Ezen felül figyelembe kell venni azt is, hogy egy kizárólag olvasó hozzáférést eredményező betelepülés nem létezhet. Mind a hozzáférést végrehajtó szerv, mind azok a harmadik személyek, akik a hozzáférést végrehajtó programmal alkalmasint visszaélnek, a célrendszerbe való betelepüléssel adatállományokat véletlenül vagy célzott manipuláció révén törölhetnek, módosíthatnak vagy másikra cserélhetnek. Mindez többféleképpen is kárt okozhat az érintettnek a nyomozással összefüggésben vagy attól akár függetlenül is.

241
A betelepülés alkalmazott technikájától függően a betelepülés további károkat is okozhat, melyeket egy állami intézkedés megfelelőségének vizsgálata során figyelembe kell venni. Ha például az érintettnek egy betelepülő programot egy vélhetően hasznos program formájában játszanak át, nem zárható ki, hogy ő ezt a programot harmadik személyeknek továbbadja, minek következtében ezek rendszerében is kár keletkezik. Ha pedig a betelepülésre az operációs rendszer eddig ismeretlen biztonsági hézagait használják ki, célkonfliktus keletkezhet a sikeres hozzáférés és az IT-rendszerek lehető legnagyobb biztonságához fűződő közérdek között. Ennek következtében fennáll a veszélye annak, hogy a nyomozó hatóság azt például elmulasztja, hogy más szerveket ilyen biztonsági hézagok kiküszöbölésére ösztönözzön, sőt ellenkezőleg, aktivitása arra irányul, hogy e hézagok ismeretlenek maradjanak. E célkonfliktus ezért csökkentheti a lakosság bizalmát, hiszen az államnak éppen oda kellene hatnia, hogy az IT-rendszerek biztonsági foka a lehető legnagyobb legyen.

242
(2) Az az alapjogi beavatkozás, amely egy IT-rendszerhez való titkos hozzáférés formáját ölti, intenzitását tekintve csak akkor felel meg a megfelelőség követelményének, ha az adott esetben bizonyos tények egy túlnyomóan jelentős jogtárgyat fenyegető veszélyre utalnak, még ha elegendő valószínűséggel nem is állapítható meg, hogy a veszély a közeli jövőben be is következik. Ezenfelül annak a törvénynek, amely az ilyen beavatkozásra felhatalmazást ad, az érintett alapjogi védelmére szolgáló eljárási előfeltételeket is biztosítania kell.

243
(a) Az államnak a jogi érdek védelmére vonatkozó kötelessége és az egyén alkotmányos jogai védelméhez fűződő érdeke közötti feszültség közepette a törvényhozó feladata az egymásnak ellentmondó érdekek absztrakt módon való egyensúlyának megteremtése. Ez oda vezethet, hogy bizonyos intenzív alapjogi beavatkozásoknak meghatározott jogi érdekek védelmét kell szolgálniuk, és azt is csak a gyanú és a veszély meghatározott fokával összhangban. A nem megfelelő alapjogi beavatkozás tilalma más jogi érdekek védelmére vonatkozó állami feladatoknak is határt szab. A beavatkozás megfelelő küszöbét törvényes szabályozásnak kell előírnia.

244
b) Egy nagy intenzitású alapjogi beavatkozás már akkor is aránytalan lehet, ha a beavatkozás törvényesen szabályozott indoka nem eléggé súlyos. Ha a vonatkozó jogszabály meghatározott

veszélyek elhárítását szolgálja, mint ez az alkotmányvédelmi törvényre nézve az ÉWA 1. §-ából következik, a beavatkozás indokának a súlyát tekintve azon védelmi érdekek veszélyeztetettségének a rangja és természete a mérvadó, amelyeket a mindenkori szabályzás figyelembe vett.

245
Ha a beavatkozásra vonatkozó felhatalmazás mint olyan által védendő érdek eléggé súlyos ahhoz, hogy a szabályozott módon végrehajtandó alapjogi beavatkozást igazolja, úgy éppen az arányosság alapelve vezet a beavatkozás tényleges előfeltételeivel szemben támasztott alkotmányjogi követelmények meghatározásához. A törvényhozónak ennyiben egyensúlyba kell hoznia az alapjog korlátozását a beavatkozást igazoló tényállás elemeivel. A valószínűségi fokkal és a prognózis tényadataival szemben támasztott követelményeknek az alapjog korlátozásának módjával és súlyával megfelelő arányban kell állniuk. Még a jogtárgyat fenyegető legsúlyosabb korlátozás esetében sem lehet az esemény bekövetkezése valószínűségi foka mérlegeléséről lemondani. Egy súlyos alapjogi beavatkozás előfeltételeként azt is garantálni kell, hogy a feltevések és következtetések konkrét tényekből indulnak ki.

246
(c) Az arányosság alapelve egy törvényes, IT-rendszerekhez való titkos hozzáférésre felhatalmazást adó szabályozásnak mindenekelőtt annyiban szab határt, amennyiben a beavatkozás indítékával szemben különös követelmények állnak fenn. Esetünkben ez az Alkotmányvédelmi Hatóságnak az ÉWA 1. §-ában meghatározott feladatai keretében mint veszélyek megelőzése jelenik meg.

247
(aa) Egy ilyen beavatkozás csak akkor tervezhető, ha a beavatkozásra vonatkozó felhatalmazás azt attól teszi függővé, ha tényleges támpontok merülnek fel egy túlnyomóan jelentős jogtárgy konkrét veszélyeztetésére vonatkozóan. Túlnyomóan jelentős mindenekelőtt a személy testi épsége, élete és szabadsága. Túlnyomóan jelentősek továbbá az olyan közösségi javak, melyek fenyegetése az állam alapjait vagy fennállását, vagy az ember egzisztenciájának alapjait érintik. Ide tartozik például a létezéshez elengedhetetlen közszolgáltatások lényeges elemeinek működőképessége is.

248
Egyéb egyéni vagy közösségi jogi érdekek védelmére azokban a helyzetekben, melyekben egzisztenciális fenyegetés nem áll fenn, egy olyan állami intézkedés elvileg nem megfelelő, mely által – mint esetünkben – az érintett személyisége a nyomozóhatóság által végrehajtott átfogó kikémlelésnek lesz kiszolgáltatva. Ilyen jogi érdek védelmére az államnak más nyomozati jogosultságokra kell korlátoznia magát, amelyeket számára a magánszférára mindenkor alkalmazható ágazati jog tartalmaz.

249
(bb) A törvényes felhatalmazás alapjául továbbá a titkos hozzáférés előfeltételeként kell figyelembe venni, hogy legalábbis tényleges támpontok álljanak fenn a normában szabályozott megfelelően súlyos jogtárgy tényleges veszélyeztetésére vonatkozóan.

250
() A tényleges támpontok követelménye oda vezet, hogy sejtések vagy általános tapasztalatok önmagukban nem elegendőek ahhoz, hogy a hozzáférést igazolják. Inkább bizonyos tényeket kell megállapítani, amelyek a veszélyt prognosztizálják.

251
E prognózisnak egy tényleges veszély bekövetkezésére kell mutatnia. Ez olyan helyzet, amelyben elegendő valószínűséggel következtetni lehet az adott esetben arra, hogy belátható időn belül az állam beavatkozása hiányában a normával védett érdekben bizonyos személyek kárt fognak okozni. A tényleges veszélyt három kritérium szerint kell meghatározni: az egyedi eset, a küszöbönálló veszély bekövetkezésével keletkező kár és az utalás adott személyre mint elkövetőre. Az IT-rendszerhez való hozzáférés iménti megítélését egyébként már az is igazolhatja, ha elegendő valószínűséggel még nem

állapítható meg, hogy a veszély a közeli jövőben már bekövetkezik, ha bizonyos tények az adott esetben egy túlnyomóan jelentős jogtárgyat fenyegető veszélyre utalnak. A tényeknek egyrészt meg kell engedniük a legalább módját tekintve konkrét és belátható időn belül bekövetkező eseményre való következtetést, másrészt a következtetést arra, hogy bizonyos személyek az eseménynek résztvevői lesznek, s azonosságukról legalább annyi ismert, hogy a megfigyelésre szolgáló intézkedés célzottan ellenük irányul és messzemenően rájuk korlátozható.

252
Az IT-rendszerbe való titkos hozzáférésben megnyilvánuló alapjogi beavatkozás súlyát azonban nem megfelelően veszik figyelembe akkor, ha a beavatkozás tényleges indítékának, a norma által védett érdek adott esetben belátható konkrét veszélyeztetésének előrejelzése még bizonytalan.

253
Alkotmányjogilag elfogadhatatlan, hogy a beavatkozás küszöbértékét bizonytalan előrejelzéshez kötik, amikor is csupán viszonylag bizonytalan támpontok merülnek fel egy lehetséges veszéllyel fenyegetett esemény bekövetkezésére vonatkozóan. A tényleges helyzetet ilyenkor egyedi megfigyelések jelentőségének magas ambivalenciája jellenzi. Az események éppúgy megmaradhatnak ártalmatlan összefüggésükben, mint ahogyan egy olyan folyamat kezdetét is képezhetik, amely veszélybe torkollik.

254
() A beavatkozás tényleges indítékával szemben támasztott alkotmányjogi követelményeket az IT-rendszerekhez való titkos hozzáférésre vonatkozó minden felhatalmazás esetében célként a megelőzést kell figyelembe venne. Minthogy a beavatkozással az érintettnek okozott sérelem mindezekben az esetekben azonos, követelményeit tekintve nincs ok különbséget tenni a hatóságok, pl. a rendőri és egyéb, megelőző feladatokkal megbízott hatóságok, s ilyen az Alkotmányvédelmi Hatóság, között. Az, hogy a rendőri és az Alkotmányvédelmi Hatóságok feladatai és felhatalmazásai különbözőek és ebből adódóan beavatkozásuk mélysége is eltérő, az IT-rendszerekhez való titkos hozzáférés súlyának mérlegelése szempontjából elvileg nincs jelentősége.

255
Ugyanakkor az is igaz, hogy létezhetnek alkotmányjogilag indokolt eltérések a megelőző feladatokat ellátó hatóságok felhatalmazásai között. Így igazolják a Szövetségi Hírszerző Szolgálat[22] sajátos céljai a távközlés stratégiai megfigyelése területén, hogy a beavatkozás előfeltételei másképp vannak meghatározva, mint a rendőri vagy a büntető eljárási jogban. Különféleképpen határozhatók meg továbbá a nyomozási intézkedésekkel kapcsolatos beavatkozás előfeltételei aszerint, mely hatóság és mely céllal cselekszik. Ily módon például az Alkotmányvédelmi Hatóság sajátos, alkotmányellenes törekvések felderítésével kapcsolatos feladatait figyelembe lehet venni már a konkrét veszély kialakulását megelőzően. Alkotmányjogilag tehát elvileg nem kifogásolható, ha az Alkotmányvédelmi Hatóságok hírszerző-szolgálati eszközöket is bevethetnek, hogy tudomást szerezzenek azokról a csoportosulásokról, amelyek az alkotmányvédelmi törvény jogi tárgyai ellen – még legalább – a törvényesség talaján állva küzdenek. Ilyen eszközök bevetésével kapcsolatban általában azt sem kell megkövetelni, hogy a mindenkor elengedhetetlen tényleges támpontokon felül konkrét gyanú merüljön fel.

256
A törvényhozót azoknak a biztonsági szolgálatoknak, amelyek feladata a megelőző felderítés, az egyedi felhatalmazásai szabályozásakor, azok az alkotmányjogi előírások is kötik, amelyek az arányosság alapelvéből következnek. Ez oda vezethet, hogy e hatóságok is csak akkor kaphatnak felhatalmazást egyes intenzív alapjogi beavatkozásokra, ha a beavatkozás indokának szabályozásával szemben szigorú követelményeket támasztanak. Különösen igaz ez az IT-rendszerhez való titkos hozzáférés esetében, amely a cselekvő hatóságtól függetlenül azt a kockázatot rejti, hogy az érintett személyisége egy mélyreható állami kikémlelés tárgyává válik. Még ha nem is sikerül olyan, a megelőzésben cselekvő hatóságokra igazított, a beavatkozás indokára vonatkozó törvényes

[22] Bundesnachrichtendienst

intézkedéseket meghatározni, amelyek az alapjogi veszélyeztetés súlyát és intenzitását ahhoz hasonló mértékben figyelembe veszi, mint ahogyan azt például a hagyományos veszélyeztetés esetében a rendőrségi jogszabályok teszik, az nem lenne alkotmányjogilag elfogadható indoka annak, hogy a tárgyalt jellegű beavatkozás tényleges feltételeit enyhítsék.

257
(d) Az IT-rendszerekhez való titkos hozzáférésre vonatkozó felhatalmazást továbbá alkalmas törvényes óvóintézkedésekhez kell kötni, amelyek az érintett érdekeit alkotmányjogilag biztosítják. Ha egy norma az állam titkos nyomozási tevékenységéről rendelkezik, s az – mint esetünkben – a magánszféra különösen védett területét érintik vagy egy különösen magas beavatkozási intenzitást mutatnak, az alapjogi beavatkozás súlyát alkalmas eljárási óvóintézkedésekkel összefüggésben kell figyelembe venni. A hozzáférés előírását elvileg bírósági rendelkezéshez kell kötni.

258
(aa) Egy ilyen előírással lehetővé válik, hogy a tervezett titkos nyomozási intézkedést egy független és semleges szerv előzetesen megvizsgálja. Egy efféle vizsgálat a hatékony alapjogi védelem jelentős elemét képezheti, jóllehet nem alkalmas arra, hogy egy bizonytalanul szabályozott vagy túl alacsonyra helyezett beavatkozási küszöböt kiegyenlítsen, mert a vizsgálatot végző független szerv is csak azt képes biztosítani, hogy a szabályozott beavatkozási feltételek teljesüljenek. Ez a szerv egyébként arról is gondoskodhat, hogy a titkos beavatkozásra vonatkozó intézkedést elrendelő határozat az érintett érdekeit megfelelően figyelembe veszi, amire az érintettnek magának az intézkedés titkos volta miatt nincs lehetősége. A vizsgálat ennyiben az államigazgatási eljárásban az érintett érdekeinek „kompenzációs képviseletét“ szolgálja.

259
(bb) Ha a titkos nyomozási intézkedés egy mélyreható alapjogi beavatkozással jár, a független szerv előzetes vizsgálata alkotmányjogilag kötelező, különben az érintett védtelen maradna. A törvényhozónak egyébként az egyedi vizsgálatok részleteinek meghatározására, pl. a vizsgálatot végző hatóság vagy az alkalmazandó eljárás tekintetében, elvileg tág tere van. Különösen nagy súlyú alapjogi beavatkozás esetében, mint amilyen egy IT-rendszerhez való titkos hozzáférés, ez a tér annyiban korlátozódik, hogy az intézkedést elvileg bírósági határozat előírásához kell kötni. Személyes és szakmai függetlenségük alapján, továbbá mert kizárólag a törvénynek vannak alárendelve, az érintett jogait az adott esetben a legjobban és a legbiztonságosabban a bírók képesek védelmezni. Ennek előfeltétele egyébként, hogy a tervezett intézkedés jogszerűségét behatóan megvizsgálják és az indokokat írásba foglalják.

260
A törvényhozó más szervet csak akkor bízhat meg az ellenőrzéssel, ha az ugyanolyan függetlenséggel és semlegességgel rendelkezik mint egy bíró. Jogszerűségét azonban e szervnek is igazolnia kell.

261
Sürgős esetben, ha a késlekedés veszéllyel járna, az arra alkalmas semleges szerv intézkedése előzetes ellenőrzésének követelményétől el lehet tekinteni, ha a semleges szerv az utólagos ellenőrzéséről gondoskodnak. A sürgősséget azonban ismét csak a tényleges és jogi előfeltételekkel szemben támasztott alkotmányos előírások tükrében kell megítélni.

262
(3) E kritériumok szerint a támadott norma nem tesz eleget az alkotmányjogi követelményeknek.

263
(a) AZ ÉWA 5. § 2. bek. a 7. § (1) bek. 1. pontjával és 3. § (1) bekezdéssel összefüggésben annak az előfeltétele, hogy az Alkotmányvédelmi Hatóság hírszerző-szolgálati eszközöket vessenek be csupán tényleges támpontjai annak a feltételezésnek, hogy ily módon tudomást lehet szerezni alkotmányellenes törekvésekről. Ez sem a beavatkozás tényleges előfeltételei, sem a védendő jogi érdek súlya tekintetében nem elegendő anyagi beavatkozási küszöb. Ugyanakkor hiányzik a független

szerv előzetes vizsgálatának elrendelése, vagyis az alkotmányjogilag megkövetelt eljárásjogi biztosíték.

264
(b) Ez a hiányosság akkor is fennáll, ha az ÉWA 5. § 2. bek. 11. pont 2. mondat hivatkozását a titoktörvény részletes előfeltételeire a vizsgálat nem meghatározott volta ellenére is figyelembe vesszük és az északrajna-westfáliai tartományi kormány tág értelmezésében úgy értjük, hogy az e törvény valamennyi formális és anyagi intézkedésére vonatkozik. AZ ÉWA 5. § 2. bek. 11. pont 1. mondat 2. fordulata az információtechnikai rendszerhez való titkos hozzáférést nem korlátozza a távközlés megfigyelésére, melynek előfeltételeit a titoktörvény 3. § (1) bek. szabályozza, hanem efféle hozzáférést elvileg minden rendelkezésre álló adat megszerzésére lehetővé teszi.

265
Sem a beavatkozási küszöb szabályozása, sem a titoktörvény 3. § (1) bekezdése beavatkozási tényállásaira vonatkozó eljárásjogi előírások nem felelnek meg az alkotmányjogi követelményeknek.

266
(aa) A titoktörvény 3. § (1) bek. 1. mondata szerint egy megfigyelésre irányuló intézkedés akkor megengedhető, ha a gyanú tényleges támpontokon nyugszik, amelyek arra utalnak, hogy valaki a normában szabályozott listában felsorolt bűncselekmények egyikét tervezi, követi el vagy követette el. A bűncselekménylistából egyrészt nem lehet felismerni olyan koncepciót, amely szerint igazolható lenne valamennyi, ott felsorolt bűncselekményt az ÉWA 5. § (2) bek. 11. pont 1. mondat 2. fordulatában foglalt intézkedés indokának tekinteni. Következésképpen nem minden tekintetbe vett norma esetében biztosítható, hogy a hozzáférés a konkrét esetben a fentebb (C I 2 b, dd <2> <c> <aa>) felsorolt túlnyomóan jelentős jogi érdek védelmét szolgálja. Másrészt titoktörvény 3. § (1) bek. 1. mondatára való utalás nem biztosítja, hogy az információtechnikai rendszerhez való hozzáférésre csak akkor kerül sor, ha ilyen jogi érdekek az adott esetben elegendő valószínűséggel (C I 2 b, dd <2> <c> <bb>) a közeli jövőben veszélyeztetve lesznek.

267
A titoktörvény 3. § (1) bek. 2. mondata szerint egy megfigyelési intézkedés akkor is elrendelhető, ha tényleges támpontja van annak a gyanúnak, hogy valaki egy olyan egyesület tagja, melynek célja vagy tevékenysége alkotmányosan védett jogi tárgyak elleni bűncselekmények elkövetésére irányul. A bűncselekmények egyébként csupán általánosan vannak körülírva, következésképpen egy kiterjesztő értelmezés kockázata áll fenn, hogy egy beavatkozás olyan jogi érdek védelmére is lehetővé válna, amely nem túlnyomóan jelentős. Ezen felül e rendelkezés szerint nem kellene minden olyan esetben fennállnia azoknak a titoktörvény 3. § (1) bek. 1. mondatában rögzített beavatkozási tényállást megvalósító tényleges támpontoknak, amelyek adott esetben ilyen személy vagy egyesület által fenyegető veszélyt jelentenek egy túlnyomóan jelentős jogtárgyra nézve.

268
(bb) AZ ÉWA 5. § 2. bek. 11. pont 1. mondat 2. fordulata továbbá akkor sem felel meg egy információtechnikai rendszerhez való titkos hozzáférés előzetes ellenőrzésére vonatkozó alkotmányjogi követelményeknek, ha a titoktörvényre való hivatkozást is tartalmazza.

269
A titoktörvény 10. § a megfigyelésre vonatkozó intézkedés előzetes elrendelését írja elő, melyet az Alkotmányvédelmi Hatóság kérelmére az arra illetékes legfelsőbb tartományi hatóság ad ki. Ez az eljárás nem elegendő ahhoz, hogy az Alaptörvény 2. § (1) bekezdésében az Alaptörvény 1. § (1) bekezdésével összefüggésben megkövetelt előzetes ellenőrzést biztosítsa. A törvény sem a bíróság kikötéséről, sem – minthogy Északrajna-Westváliának a titoktörvény végrehajtásáról szóló törvényének 3. § (6) bekezdésében rögzített, a G 10-bizottság előzetes ellenőrzésére vonatkozó szabályozást a hivatkozás nem tartalmazza – egy azzal egyenértékű ellenőrzési mechanizmusról nem rendelkezik. Az illetékes legfelsőbb tartományi hatóságnak, a bíróságoktól eltérően, ágazati struktúrájánál fogva, az alkotmányvédelemmel kapcsolatos hírszerző-szolgálati intézkedései

végrehajtásához sajátos érdeke fűződhet. A hatóság nem kínálja az ellenőrzési függetlenségének és semlegességének a bíróságokéval összehasonlítható biztosítékát.

270
c) Végül hiányzanak a megfelelő törvényes előfeltételek ahhoz, hogy ÉWA 5. § 2. bek. 11. pont 1. mondat 2. fordulata szerinti intézkedésekkel a magánéletvitel abszolút védett belső magjába való beavatkozás elkerülhető legyen.

271
aa) Az állami szervek titkos megfigyelésre irányuló intézkedéseinek meg kell óvnia a magánéletvitel sérthetetlen belső magját, melynek védelme az Alaptörvény 1. § (1) bekezdéséből adódik. Még túlnyomó közösségi érdekek sem igazolhatják a beavatkozást ebbe a területbe. A személyiségnek magánéletvitel belső magjában folyó kibontakoztatásához elengedhetetlen belső folyamatokat, például érzéseket és érzelmeket, valamint megfontolásokat, nézeteket és élményeket felettébb személyes módon kifejezni, nem félve attól, hogy állami szervek ezt megfigyelik.

272
Egy információtechnikai rendszerhez való titkos hozzáférés esetében fennáll a veszély, hogy a cselekvő állami szerv olyan személyes adatokhoz jut, amelyek a belső maghoz tartoznak. Az érintett ugyanis a rendszert arra használhatja, hogy felettébb személyes tartalmakat, például naplószerű feljegyzéseket vagy magánjellegű film- és hangdokumentumokat hozzon létre és tároljon. Ezek a dokumentumok, csakúgy, mint a felettébb személyes élmények írásos megtestesülése abszolút védelmet élveznek. A rendszert másrészt, ha távközlési célokra is szolgál, tartalmak továbbítására is használhatják, melyek szintén a belső maghoz tartoznak. Ez nem vonatkozik a beszédtelefonra, de például az e-mail-lel folytatott távközlésre vagy az Internet egyéb távközlési szolgáltatásaira igen. Az abszolút védelmet érdemlő adatokat a hozzáférés különféle módszereivel meg lehet szerezni, például az adathordozók áttekintésével, a folyó Internet-kommunikáció megfigyelésével, vagy akár a célrendszer használatának teljes megfigyelésével.

273
(bb) Az érintett információtechnikai rendszerének titkos megfigyeléséhez különös törvényes előfeltételekre van szükség, amelyek a magánéletvitel belső magját védik.

274
Személyes ügyeik kezelésére és közeli ismerőseikkel folytatott távközlési érintkezésre a polgárok egyre inkább komplex információtechnikai rendszereket használnak, amelyek lehetőséget kínálnak számukra a felettébb személyes területükben folyó kibontakozásra. Tekintettel erre egy olyan nyomozási intézkedés, mint az információtechnikai rendszerhez való hozzáférés, melynek révén a célrendszerben fellelhető adatokat kiterjedten meg lehet szerezni, egyéb olyan megfigyelési intézkedésekkel szemben, mint például a GPS (Globális Helymeghatározó Rendszer) felhasználása a technikai megfigyelés eszközeként, fokozza a felettébb személyes tartalmú adatok megszerzésének a veszélyét.

275
A hozzáférés titkos volta nem nyújt lehetőséget az érintettnek arra, hogy a megfigyelési intézkedés végrehajtását megelőzően vagy folyamán oda hasson, hogy a nyomozó állami szerv magánéletvitelének belső magját tiszteletben tartsa. Az ellenőrzésnek ezt a teljes elvesztését különös szabályozással kell ellensúlyozni, amely a belső mag sérelmének veszélyét alkalmas eljárási intézkedésekkel védi.

276
cc) A belső mag védelmét szolgáló konkrét megvalósításra vonatkozó alkotmányjogi követelmények az információszerzés módjától és az így megszerzett információtól függően különbözőek lehetnek.

277

Egy olyan megfigyelési intézkedés végrehajtására irányuló törvényes felhatalmazásnak, amely a magánéletvitel belső magját érintheti, a lehető legmesszebbmenően gondoskodnia kell arról, hogy a belső magra vonatkozó adatok megszerzésére ne kerüljön sor. Ha – mint egy információtechnikai rendszerhez való titkos hozzáférés esetében – gyakorlatilag elkerülhetetlen, hogy információ jusson tudomásra mielőtt még annak belső maghoz tartozása kiértékelhető lenne, a kiértékelés szakaszában kell a megfelelő védelemről gondoskodni. Mindenekelőtt haladéktalanul törölni kell a fellelt és megszerzett, belső maghoz tartozó adatokat és kiértékelésüket ki kell zárni.

278
(1) Egy információtechnikai rendszerhez való titkos hozzáférés keretében az adatgyűjtés már technikai okokból is legalább túlnyomóan automatizálva folyik. Az automatizálás azonban, eltérően egy személy által végzett adatgyűjtéstől, megnehezíti, hogy már az adatgyűjtés folyamán megkülönböztessék az adatokat aszerint, a belső maghoz tartoznak-e avagy nem. A Szenátus által meghallgatott szakértők egybehangzó véleménye szerint a személyes adatok belső maghoz tartozásának vizsgálatára szolgáló technikai kereső- és kizáró-mechanizmusok nem olyan megbízhatóak, hogy segítségükkel a belső mag hatékony védelmét el lehessen érni.

279
Még ha az adatokhoz való hozzáférést közvetlenül személyek végzik, s előzetesen technikai feljegyzéseket nem készítenek, mint például az Interneten folytatott beszédtelefon személyes megfigyelésekor, a belső mag védelme már az adatgyűjtés folyamán gyakorlati nehézségekbe ütközik. Egy ilyen intézkedés végrehajtása során rendszerint biztosan nem előrelátható, a gyűjtött adatok milyen tartalmat hordoznak. Az adatok tartalmának elemzése a gyűjtés folyamán ugyancsak nehézségekkel járhat, mint például idegen nyelvű szöveges dokumentumok vagy beszélgetések esetében. A megfigyelt folyamatok belső maghoz tartozását ilyen esetekben sem lehet mindig az adatgyűjtést megelőzően vagy annak során kiértékelni. Ilyen esetekben nem alkotmányjogi követelmény a belső mag sérelmének kockázata miatt a hozzáférést a gyűjtés szintjén eleve feladni, minthogy az IT-rendszerbe való hozzáférés alapját egy túlnyomóan jelentős védett érdek tényleges veszélyeztetésére mutató támpontok képezik.

280
(2) A belső mag alkotmányjogilag megkövetelt védelme egy kétfokozatú védelmi koncepció keretében valósítható meg.

281
(a) A törvényes szabályozásnak oda kell hatnia, hogy a belső maghoz tartozó adatok gyűjtésére, amennyire ezt az információtechnika és nyomozástechnika lehetővé teszi, ne kerüljön sor. Mindenekelőtt a rendelkezésre álló információtechnikai biztosítékokat kell alkalmazni. Ha adott esetben tényleges támpontok merülnek fel arra nézve, hogy egy meghatározott adatgyűjtés a magánéletvitel belső magját érinti, úgy annak végrehajtását elvileg fel kell adni. Más a helyzet, ha például tényleges támpontjai merülnek fel annak, hogy a belső magra vonatkozó kommunikációs tartalmak olyan tartalmakhoz kapcsolódnak, amelyek – hogy a megfigyelést megakadályozzák – a nyomozás célját képezik.

282
(b) Sok esetben a gyűjtött adatok belső maghoz tartozását az adatgyűjtés előtt vagy folyamán nem lehet tisztázni. A törvényhozónak alkalmas eljárási előírásokkal kell gondoskodnia arról, hogy amikor olyan adatokat gyűjtöttek, amelyek a magánéletvitel belső magjával kapcsolatosak, a belső mag sérelmének intenzitása és ennek hatása az érintett személyiségére és kibontakozására a lehető legcsekélyebb legyen.

283
A védelemre nézve döntő jelentőségű e tekintetben a gyűjtött adatok áttekintése egy arra alkalmas eljárással, hogy a belső maghoz tartoznak-e avagy nem, mely eljárás az érintett érdekét megfelelően

figyelembe veszi. Ha az áttekintés során kiderül, hogy a belső maghoz tartozó adatokat gyűjtöttek, úgy azokat haladéktalanul törölni kell. Továbbításukat vagy kiértékelésüket ki kell zárni.

284
dd) Az alkotmányvédelmi törvény a belső magot védő szükséges előírásokat nem tartalmazza. Ezen az sem változtat, hogy az ÉWA 5. § 2. bek. 11. pont 2. mondat hivatkozását a titoktörvényre nem meghatározott volta ellenére is figyelembe vesszük. Ez a törvény sem tartalmaz ugyanis a magánéletvitel belső magját védő előírásokat.

285
Az északrajna-westfáliai tartományi kormány felfogásával ellentétben a titoktörvény 4. § (1) bekezdése e tekintetben akkor sem vehető figyelembe, ha az ÉWA 5. § 2. bek. 11. pont 2. mondatát széles értelmezésben úgy értjük, hogy az erre az előírásra is kiterjed. A titoktörvény 4. § (1) bekezdése csupán azt szabályozza, hogy azokat a gyűjtött adatokat, amelyekre nincs vagy a továbbiakban nincs szükség, törölni kell, s ezzel a szükségességet mint főszabályt rögzíti. Az előírás másrészt semmiféle különös intézkedést nem tartalmaz azoknak az adatoknak a gyűjtésére, áttekintésére és törlésére nézve, amelyek kapcsolatba hozhatók a belső maggal. A szükségesség főszabályát a magánéletvitel belső magjának alkotmányjogilag elrendelt figyelembe vételével nem lehet azonosnak tekinteni. A belső mag még többnyire egymással ellentétes nyomozási érdekek, amikor azokat például a szükségesség főszabályának alkalmazásával implicite tekintetbe vennék, összevetésével sem közelíthető meg.

286
d) Az általános személyiségi jognak mint az IT-rendszerek bizalmas volta és sérthetetlensége védelme formája megsértése (Alaptörvény 2. § 1. bek. az 1. § (1) bekezdésével összefüggésben) az ÉWA 5. § 2. bek. 11. pont 1. mondat 2. fordulata semmisségéhez vezet.

287
e) Mindezek figyelembe vételével nincs szükség további vizsgálatra, milyen súlyosan sértenek azok az intézkedések, melyekre a norma felhatalmazást ad, egyéb alapjogokat vagy az Alaptörvény 19. § (1) bek. 2. mondatában előírt hivatkozást mint főszabályt.

II.
288
AZ ÉWA 5. § 2. bek. 11. pont 1. mondat 1. fordulatában adott felhatalmazás az Internet titkos felderítésére sérti az Alaptörvény 10. § 1. bekezdésében rögzített távközlési titkot. E norma szerinti intézkedések egyes esetekben ebbe az alapjogba való olyan beavatkozást valósíthatnak meg, amely alkotmányjogilag nem igazolható (1); sértik továbbá az Alaptörvény 19. § (1) bek. 2. mondatát (2). Az alkotmányellenesség a norma semmisségéhez vezet (3). Az Alkotmányvédelmi Hatóság egyébként továbbra is foganatosíthat az Internet felderítésére irányuló intézkedéseket, ha azok alapjogba való beavatkozásnak nem tekinthetők.

289
1. Az Internetnek az ÉWA 5. § 2. bek. 11. pont 1. mondat 1. fordulatában szabályozott titkos felderítése felöleli azokat az intézkedéseket, melyek révén az Alkotmányvédelmi Hatóság az Internet-kommunikáció tartalmáról az arra technikailag alkalmas módon tudomást szerez, így például a világháló egyes oldalainak egy böngészővel való kiválasztásával (lásd fentebb A I 1 a). Egyes esetekben ez a távközlési titokba való beavatkozással járhat. Egy ilyen beavatkozást a támadott norma alkotmányjogilag nem igazol.

290
a) Az Alaptörvény 10. § (1) bekezdésével védett terület felöleli az Internethez kapcsolt IT-rendszer igénybevételével folyó távolsági kommunikációt (v. ö. fentebb I 1 c, aa <1>). Ez az alapjog mindazonáltal csupán az egyén abba vetett bizalmát védi, hogy arról a távolsági kommunikációról, melynek résztvevője, harmadik személy nem szerez tudomást. Ezzel szemben a kommunikációban résztvevők egymás iránti bizalma nem tárgya az alapjog védelmének. Ha egy állami nyomozási

intézkedés nem a távközléshez való illetéktelen hozzáférésre irányul, hanem a kommunikációban résztvevő személy iránti bizalom megrendítése, akkor az Alaptörvény 10. § 1. bekezdése értelmében nem minősül beavatkozásnak. Ha az állam tudomást szerez egy távolsági kommunikáció tartalmáról, úgy azt csak arra való tekintettel kell a távközlési titok szerint megítélni, hogy az állami szerv a távközlési kapcsolatot kívülről figyeli-e meg anélkül, hogy maga a kommunikáció címzettje lenne. Az alapjog ugyanis nem véd attól, hogy egy állami szerv maga egy alapjog alanyával távközlési kapcsolatot létesítsen.

291
Ha egy állami szerv az arra technikailag alkalmas módon tudomást szerez az Internet távközlési szolgáltatásai igénybe vételével folytatott távközlési kommunikáció tartalmáról, úgy az csak akkor valósítja meg az Alaptörvény 10. § 1. bekezdése szerinti beavatkozást, ha az állami szervet erre a kommunikáció résztvevői nem hatalmazzák fel. Mivel a távközlési titok a kommunikációban résztvevők egymás iránt táplált bizalmát nem védi, az állami szerv a távközlés tartalmát már akkor is jogosult megismerni, ha számára ezt a hozzáférést több résztvevő közül csupán az egyik önként lehetővé tette.

292
Az Internet titkos felderítése eszerint csak akkor sérti az Alaptörvény 10. § 1. bekezdését, ha az Alkotmányvédelmi Hatóság hozzáférés ellen biztosított kommunikációs tartalmakat figyel meg, miközben a hozzáférésre olyan kulcsot használ, amelyet a kommunikáció résztvevői hozzájárulása nélkül vagy akarata ellenére szerzett meg. Erre szolgál például egy keylogging [23] segítségével megszerzett jelszó, mellyel egy e-mail postafiókba vagy egy zárt csevegésbe (chat) lehet belépni.

293
Ezzel szemben a beavatkozás nem sérti az Alaptörvény 10. § (1) bekezdését, ha például egy zárt csevegés egyik résztvevője hozzáférését önként az Alkotmányvédelmi Hatóságnak dolgozó személy rendelkezésére bocsátja és a hatóság ezt követően ezt a hozzáférést felhasználja. A távközlési titokba való beavatkozás nem valósul meg, ha a hatóság a nyilvánosság számára hozzáférhető tartalmakat gyűjt, például miközben betekint nyílt vitafórumokba vagy hozzáférés ellen nem védett Internet-oldalakba.

294
b) Az Alaptörvény 10. § (1) bekezdésébe való, az ÉWA 5. § 2. bek. 11. pont 1. mondat 1. fordulata szerint lehetséges beavatkozás alkotmányjogilag nem igazolható. A támadott norma nem felel meg az ilyen beavatkozásra vonatkozó felhatalmazások alkotmányjogi követelményeinek.

295
aa) AZ ÉWA 5. § 2. bek. 11. pont 1. mondat 1. fordulata nem felel meg a normavilágosság és normaszabatosság követelményének, mivel az előírás 2. mondata az egyértelműség hiánya következtében a beavatkozás előfeltételeit nem eléggé pontos szabályozza (v. ö. fentebb C I 2 a, bb).

296
bb) A támadott norma továbbá az Alaptörvény 10. § 1. bekezdéséhez mérten nincs összhangban az arányosság szoros értelemben vett követelményével.

297
A beavatkozás a távközlési titokba súlyos. A támadott norma szerint az Alkotmányvédelmi Hatóság olyan kommunikációs tartalmakhoz férhet hozzá, amelyek érzékenyek lehetnek és az érintett személyes ügyeibe és szokásaiba engednek betekinteni. Érintett nem csak az, aki a megfigyelési intézkedésre okot adott. A beavatkozás sokszor terjedelmes szórást mutathat, ha nemcsak annak a személynek a kommunikációs viselkedéséről szerezhető tudomás, aki ellen az intézkedés irányul,

[23] keylogging (eredetileg 'keystroke logging") szó szerint a billentyűlenyomások nyomon követése erre alkalmas szoftver vagy hardver eszköz segítségével.

hanem kommunikációs partneréről is. A hozzáférés titkossága növeli a beavatkozás intenzitását. Mi több, a beavatkozás előfeltételeinek az ÉWA 7. § (1) bek. 1. mondat 1. pontja a 3. § 1. bekezdésével összefüggésben való széles értelmezése következtében olyan személyek is megfigyelhetők, akik a beavatkozás okáért nem felelősek.

298
Az ilyen súlyos beavatkozás egy alapjogba az alkotmányvédelem céljainak súlyára való tekintettel elvileg legalább egy minősített anyagi beavatkozási küszöb elrendelésén alapulhat. Ez itt hiányzik. AZ ÉWA 7. § (1) bek. 1. mondat 1. pontja a 3. § 1. bekezdésével összefüggésben sokkal inkább széleskörű hírszerző-szolgálati intézkedésekre nyújt lehetőséget tényleges veszélyeztetések előzetes kialakulása alkalmával anélkül, hogy tekintettel lenne a lehetséges jogtárgy sérelmének súlyára, akár harmadik személyekkel szemben is. Egy ilyen széleskörű felhatalmazás a beavatkozásra az arányosság elvével nem egyeztethető össze.

299
cc) Az alkotmányvédelmi törvény az ÉWA 5. § (2) bek. 11. pont 1. mondat 1. fordulata szerinti beavatkozásokkal összefüggésben nem tartalmaz a magánéletvitel védelmét szolgáló óvintézkedéseket. Ilyen szabályokra azonban szükség van, ha az állami szerv a távközlés tartalmának gyűjtésére az Alaptörvény 10. § (1) bekezdése szerinti beavatkozásra felhatalmazást kap.

300
2. Végül az ÉWA 5. § (2) bek. 11. pont 1. mondat 1. pontja, amennyiben a norma az Alaptörvény 10. § 1. bekezdése szerinti beavatkozásra ad felhatalmazást, nem felel meg az Alaptörvény 19. § (1) bek. 2. mondatában előírt hivatkozás követelményének.

301
Az Alaptörvény 19. § (1) bek. 2. mondata értelmében egy törvényben paragrafusára való hivatkozással meg kell jelölni azt az alapjogot, melyet e törvény korlátoz vagy mely e törvény alapján korlátozva van. A hivatkozás előírása a figyelem felkeltését és a meggondolást szolgálja. A beavatkozás megnevezése a törvény szövegében biztosítja, hogy a törvényhozó csak olyan beavatkozásokat vesz tekintetbe, melyeknek mint ilyeneknek tudatában van és melyeknek az érintett alapjogokra gyakorolt hatásáról saját magának számot tud adni. A kifejezett megnevezés megkönnyíti továbbá a tervezett alapjogi beavatkozás szükségességének és terjedelmének nyilvános vitákban való tisztázását. Nem elégséges ezért, hogy a törvényhozó az alapjogi beavatkozásnak tudatában volt, ha a törvény szövege ezt nem tartalmazza.

302
A támadott norma, tekintettel az Alaptörvény 10. § 1. bekezdésére, nem felel meg a hivatkozás követelményének. Ellentétben az északrajna-westfáliai tartományi kormány véleményével a támadott norma már csak azért sem felel meg e követelményeknek, mert az ÉWA 5. § (2) bek. 11. pont 2. mondata a titoktörvényre való utalással arra mutathat, hogy a törvényhozó egy beavatkozást a távközlési titokba lehetségesnek tartott. A hivatkozás követelménye csak akkor teljesül, ha a törvény szövege az alapjogot mint korlátozott alapjogot kifejezetten megnevezi. Egyébként tekintettel arra, hogy az ÉWA 5. § (2) bek. 11. pont két különböző beavatkozásra ad felhatalmazást, a törvény szövegezése semmi esetre sem elegendően világos annak megállapítására, hogy törvényhozó melyikük esetében számolt legalábbis az Alaptörvény 10. §-ában rögzített beavatkozás lehetőségével.

303
3. AZ ÉWA 5. § (2) bek. 11. pont 1. mondat 1. fordulata ellentétes volta az Alaptörvény 10. § 1. bekezdésével és az Alaptörvény 19. § 1. bek. 2. mondatával az előírás semmisségét vonja maga után.

304
4. A felhatalmazás semmissége egyébként nem jár azzal, hogy a hatóság az Internet felderítésére irányuló intézkedéseket nem hozhat, ha azok az alapjogokba nem avatkoznak bele.

305
Az Internet titkos felderítése, ha az nem esik az Alaptörvény 10. § (1) bekezdés hatálya alá, kiváltképpen nem mindig minősül az Alaptörvény 2. § (1) bekezdésében az Alaptörvény 1. § (1) bekezdésével összefüggésben biztosított általános személyiségi jogba való beavatkozásnak.

306
a) Az IT-rendszereknek az általános személyiségi jog által biztosított bizalmas voltát és sérthetetlenségét az Internet felderítésére irányuló intézkedések nem érintik, ha az ÉWA 5. § (2) bek. 11. pont 1. mondat 1. fordulata szerinti intézkedések arra korlátozódnak, hogy olyan adatokat, melyeket a rendszer tulajdonosa – például egy Web-szerver üzemeltetője – az Internet-kommunikációhoz rendelt, az arra technikailag alkalmas módon gyűjtsenek. Ilyen adatgyűjtésre rendszerét technikailag az érintett maga nyitotta meg. Következésképpen nem bízhat abban, hogy ilyen intézkedésnek célpontja nem lesz.

307
b) Főszabályként legalább az Alaptörvény 2. § (1) bekezdésében az Alaptörvény 1. § (1) bekezdésével összefüggésben értelmezett információs önrendelkezési jog megjelenési formájába való beavatkozást kell elkerülni.

308
aa) Az állam tudomásszerzése nyilvánosan hozzáférhető információkról elvileg nem tiltott. Ez akkor is igaz, ha adott esetben személyes jellegű információk gyűjtésére kerül sor. Következésképpen nem minősül az általános személyiségi jogba való beavatkozásnak, ha egy állami szerv az Interneten rendelkezésre álló olyan kommunikációs tartalmakat gyűjt, amelyek címzettje bárki vagy legalább egy határozottan nem korlátozott személycsoport. Ez a helyzet például akkor, ha a hatóság egy nyilvánosan hozzáférhető Web-oldalt a világhálón megnyit, egy minden érdeklődőnek nyitva álló levelezési listára bejelentkezik vagy egy nyilvános csevegést megfigyel.

309
Az információs önrendelkezési jogba való beavatkozásról egyébként akkor lehet szó, ha célzatosan olyan információkat gyűjtenek össze, tárolnak és esetleg további adatok bevonásával kiértékelnek, melyeket a nyilvánosan hozzáférhető tartalmakból nyertek, és ebből az érintettek személyiségét különösen veszélyeztető helyzet adódik. Ehhez felhatalmazásra van szükség.

310
bb) Az információs önrendelkezési jogba való beavatkozás már akkor sem valósul meg, ha egy állami szerv álcázva az alapjog egy alanyával kommunikációs kapcsolatba lép, ellenben igen, ha közben az érintett védelemre méltó, a kommunikációs partner azonosságba és motivációba vetett bizalmát kihasználva olyan személyes adatokat gyűjt, melyekhez különben nem jutna hozzá.

311
Mindezért az Internet puszta felderítése főszabályként nem jelent alapjogba való beavatkozást. Az Internet kommunikációs szolgáltatásai széleskörű kommunikációs kapcsolatok kiépítését teszik lehetővé, melyek keretében a kommunikáció egy résztvevőjének a kommunikációs partnere azonossága és szavahihetősége iránt táplált bizalom védelemre nem méltó, mivel erre semmiféle ellenőrzési mechanizmus nem létezik. Igaz ez akkor is, ha meghatározott személyek – például egy vitafórum keretében – a kommunikációban hosszabb időn át részt vesznek és ily módon valamiféle „elektronikus társaságot“ alkotnak. Egy ilyen kommunikációs kapcsolat keretében egyébként minden résztvevő tudatában van annak, hogy partnere azonosságát nem ismeri vagy adatait semmi esetre sem ellenőrizheti. Abbéli bizalma tehát, hogy nem egy állami szervvel kommunikál, védelemre nem méltó.

III.
312
Minthogy az ÉWA 5. § (2) bek. 11. pontja teljes egészében semmis, az ÉWA 5. § (3) bekezdése és 17. §-a ellen benyújtott panaszt is elintéztük. Annyiban az indítványozók panaszai befogadhatók, hogy a

támadott normák alkotmányellenessége csupán semmis előírás intézkedéseire való tekintettel valósulnak meg.

IV.

313
AZ ÉWA 5a § (1) bekezdése összhangban van az Alaptörvénnyel, mert alkalmazási területe kiterjed az ÉWA 3. § (1) bekezdése értelmében vett törekvésekre. Ez az előírás különösen nem sérti az Alaptörvény 2. § (1) bekezdését az 1. § (1) bekezdésével összefüggésben.

314
1. AZ ÉWA 5a § (1) bekezdésében előírt számlatartalmak és számlamozgások gyűjtése beavatkozik az általános személyiségi jog információs önrendelkezési jogként való megjelenési formájába.

315
Efféle számlainformációk az érintett személyiségének védelme szempontjából jelentősek lehetnek és alapjogi védelemben részesülnek. A jelenlegi gyakorlat szerint azoknak a fizetéseknek a többségét, amelyek a mindennapi élet készpénzügyleteit meghaladják, számlán keresztül bonyolítják le. Ha egy meghatározott személy számláinak tartalmát célzatosan összehordják, betekintést nyerhetnek az érintett vagyoni viszonyaiba és társadalmi kapcsolataiba, ha ezeknek – például mint tagsági befizetéseknek vagy szórakozási szolgáltatásoknak – pénzügyi vonatkozása van. A számlatartalom egyes adatai, például fogyasztástól függő tartós pénzügyi kapcsolatok keretében folyó fizetések nagysága, további, az érintett viselkedésére vonatkozó következtetéseket tesz lehetővé.

316
AZ ÉWA 5a § (1) bekezdésében rögzített intézkedések az információs önrendelkezési jogba való beavatkozásnak minősülnek. Itt nem az a problematikus, hogy a támadott norma szabályozási tartalma kimerül abban az Alkotmányvédelmi Hatóságnak adott jogosultságban, hogy egy hitelintézettől felvilágosítást kérjen, vagy hogy implicite kötelezze az adott hitelintézetet a felvilágosítás megadására. Az előírás minden esetben olyan adatok gyűjtésére hatalmazza fel a hatóságot, amelyek már mint ilyenek egy alapjogba való beavatkozást valósítanak meg.

317
AZ ÉWA 5a § (1) bekezdésében előírt alapjogba való beavatkozások mindazonáltal tekintettel az ÉWA 3. § (1) bekezdés 1. pontjában foglalt nyomozati törekvésekre alkotmányjogilag helytállóak. A támadott norma így különösen megfelel az arányosság elvének.

318
a) AZ ÉWA 5a § (1) bekezdésében szabályozott intézkedések a norma alkalmazási területének kiterjesztése következtében a pénzügyi utak és pénzügyi viszonyok, valamint összefonódások felderítését szolgálja összhangban az ÉWA 3. § (1) bek. 1. pontja szerinti törekvésekkel. Ez az alkotmányvédelem törvényes célja.

319
A tág értelemben vett norma alkalmas e cél elérésére, ezért ehhez szükséges is. Az érintettet kevésbé terhelő, ám éppen ilyen hatékony eszköz a bankügyletek felderítésére tekintettel az ÉWA 3. § (1) bek. 1. pontja szerinti törekvésekre nem létezik.

320
b) AZ ÉWA 3. § (1) bekezdése megfelel a szorosabb értelemben vett arányosság követelményének is.

321
aa) Egyébként a norma az alapjogba való beavatkozásra felhatalmazza az Alkotmányvédelmi Hatóságot.

322

A számlatartalmakra és számlamozgásokra vonatkozó információk esetében érzékeny adatokról szerezhető tudomás, amelyek az érintett alapjogilag védett érdekeit jelentősen csorbíthatják. Ilyen információk gyűjtésének ezért főszabályként nagyobb az alapjogi súlya. Ezen túlmenően a beavatkozás intenzitását a titkosság is fokozza. AZ ÉWA 5a § (3) bek. 11. mondata szerint a felvilágosítást nyújtó hitelintézet az érintettnek a felvilágosításra irányuló megkeresésről és a továbbított adatokról nem adhat tájékoztatást. Az érintettnek végül az is hátrányt okozhat, hogy a számlavezető hitelintézet maga az adatgyűjtésről kényszerűen tudomást szerez és abból az érintettre nézve kedvezőtlen következtetéseket vonhat le

323
bb) AZ ÉWA 5a § (1) bekezdésében tekintetbe vett közösségi érdek azonban olyan súlyú, hogy az nem aránytalan a normában szabályozott alapjogba való beavatkozáshoz képest.

324
(1) A törvény a számlatartalmak és számlamozgások tudomásra jutását tényleges előfeltételekhez köti, amelyek az érintett alapjogába való beavatkozás jelentőségét kellően figyelembe veszik.

325
AZ ÉWA 5a § (1) bekezdése a gyűjtést mind az érintett jogi érdeke, mind a beavatkozás tényleges oka tekintetében minősített veszélyhelyzettől teszi függővé. AZ ÉWA 3. § (1) bekezdésében megnevezett védett érdekek súlyos veszélyeztetése megállapításának tényleges támpontokon kell nyugodnia. A súlyos veszély fogalma – éppen úgy, mint az ezzel e tekintetben egybehangzó szövetségi alkotmányvédelmi törvény 8a § (2) bekezdésében – a jogtárgy veszélyeztetésének fokozott intenzitására utal. A súlyos veszélyeztetésre mutató tényleges támpontok követelménye ezen felül minősíti a beavatkozás tényleges okát. Nem elegendő, hogy a szabályozott adatgyűjtés általában az Alkotmányvédelmi Hatóság feladatainak teljesítését szolgálja. Mindenekelőtt léteznie kell az arra a helyzetre utaló támpontoknak, melyben a védelmi érdek ténylegesen veszélyeztetve van.

326
Ez a kettős tekintetben minősített beavatkozási küszöb megfelel az általános személyiségi jogok követelményeinek. A beavatkozás tényleges előfeltételeinek további korlátozása alkotmányos okokból nem szükséges.

327
El kell utasítani különösen az 1b-ben megnevezett panaszosnak azt a véleményét, hogy az anyagi beavatkozási küszöböt az ÉWA 3. § (1) bek. 1. pontjában rögzített törekvésekre való tekintettel úgy állapítsák meg, hogy az ÉWA 5a § (1) bekezdés csak militáns és tömeguszító törekvésekre vonatkozzék. A súlyos veszélyeztetésre utaló tényleges támpontok követelménye elegendően biztosítja, hogy nem minden halvány gyanú, amely bizonyos csoportosulásoknak a szabad demokratikus rend ellen irányuló tevékenységére utal, elegendő ahhoz, hogy számlatartalmak vagy számlamozgások gyűjtésére adjon okot. Az ezzel kapcsolatos beavatkozás egyébként nem olyan súlyos, hogy olyan erőszakos vagy efféle csoportosulások puszta leküzdésére arányos lenne, amelyek tevékenysége tömeguszításra irányul.

328
Nem ad jelentős alkotmányjogi megfontolásokra okot, hogy az ÉWA 5a § (1) bekezdése az érintettek adatai gyűjtésének módja megválasztására vonatkozó különös követelményeket szabályozza. Ezért ugyan előfordulhat, hogy egy olyan személy számlaadatait gyűjtik, aki nem gyanúsítható azzal, hogy a veszélyeztetésért jogilag felelős. Tekintettel kell lenni ugyanis arra, hogy valaki, nem szándékosan, hanem mint eszköz, az érintett törekvésekkel megcélzott vagyoni ügyletekbe bekapcsolódik. Mindazonáltal alkotmányjogilag megengedhető, hogy ilyen személy ellen is az ÉWA 5a § (1) bekezdésében rögzített intézkedéseket foganatosítsanak, ha a fizetési mechanizmusok másképp nem deríthetők fel. A több lehetséges érintett közül való kiválasztást az ÉWA 5a § (1) bekezdése keretében érvényes arányossági elv alapján lehet megfelelően elvégezni. Olyan személyek számlatartalmáról felvilágosítást adni azonban, akik nem gyanúsíthatók azzal, hogy az érintett törekvésekkel megcélzott

vagyoni ügyletekben tudatosan vagy nem tudatosan részt vesznek, aligha szolgálhatják azt a törvényes célt, amely a fizetési mechanizmusok felderítésével egy súlyos veszély azonosításához vezet.

329
(2) A támadott norma ezen felül alkalmas eljárási óvintézkedésekkel tekintetbe veszi a szabályozott alapjogi beavatkozás súlyát is.

330
AZ ÉWA 5a § (3) bekezdés 3. mondat szerinti adatgyűjtést a belügyminiszter rendelheti el, melyet az alkotmányvédelmi osztály vezetője vagy helyettese indítványoz. A számlatartalmak és számlamozgások adatainak gyűjtésével kapcsolatos alapjogi beavatkozás ugyanis nem olyan súlyos, hogy éppenséggel egy semleges szerv ex-ante ellenőrzésére szükség lenne. Az adatgyűjtést megelőzően előírt belső hatósági ellenőrzés mindazonáltal az érintett érdekeinek előzetes védelmét szolgálja és a beavatkozás arányosságát segíti elő. Ezen felül az ÉWA 5a § (3) bek. 4-8. mondatai a G 10-bizottság ex-post ellenőrzését is tartalmazzák, amely éppen úgy az érintett alapjogilag védett érdekeinek védelmét szolgálják.

331
A gyűjtött adatok feldolgozását és továbbítását az ÉWA 5a § (3) bek. 9. mondata az Északrajna-Westfália tartománynak a titoktörvény végrehajtásáról szóló törvénye 4. §-ával összefüggésben szabályozza, amelyek különösen megfelelnek a szükségesség és célhoz kötöttség követelményének.

332
AZ ÉWA 5a § (3) bek 11. mondata az Északrajna-Westfália tartománynak a titoktörvény végrehajtásáról szóló törvénye 5. §-ával összefüggésben végül az érintett értesítését írja elő, mihelyt a korlátozás célját már nem veszélyezteti. Ily módon az érintettnek messzemenően lehetősége nyílik arra, hogy érdekeinek legalább utólag érvényt szerezzen.

333
A költségekre vonatkozó határozat Szövetségi Alkotmánybíróságról szóló törvény 34. §-án nyugszik.

Papier	Hohmann-Dennhardt	Hoffmann-Riem
Bryde	Gaier	Eichberger
Schluckebier		Kirchhof

eof

Hivatkozás: BVerfG, 1 BvR 370/07, 2008.2.27, (1 - 333) bekezdés*

* BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz-Nr. (1 - 333)
Forrás: http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html