I

(Állásfoglalások, ajánlások és vélemények)

VÉLEMÉNYEK

EURÓPAI ADATVÉDELMI BIZTOS

Az európai adatvédelmi biztos véleménye „A személyes adatok Európai Unión belüli védelmének átfogó megközelítése" című, az Európai Parlamenthez, a Tanácshoz, az Európai Gazdasági és Szociális Bizottsághoz és a Régiók Bizottságához intézett bizottsági közleményről

(2011/C 181/01)

AZ EURÓPAI ADATVÉDELMI BIZTOS,

tekintettel az Európai Unió működéséről szóló szerződésre és különösen annak 16. cikkére,

tekintettel az Európai Unió Alapjogi Chartájára és különösen annak 7. és 8. cikkére,

tekintettel a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló, 1995. október 24-i 95/46/EK európai parlamenti és tanácsi irányelvre [1],

tekintettel a személyes adatok közösségi intézmények és szervek által történő feldolgozása tekintetében az egyének védelméről, valamint az ilyen adatok szabad áramlásáról szóló, 2000. december 18-i 45/2001/EK európai parlamenti és tanácsi rendeletre [2] és különösen annak 41. cikkére,

ELFOGADTA A KÖVETKEZŐ VÉLEMÉNYT:

A. **ÁLTALÁNOS RÉSZ**

1. **Bevezetés**

1.1. *Első, általános értékelés*

1. Az Európai Bizottság 2010. november 4-én „A személyes adatok Európai Unión belüli védelmének átfogó megközelítése" címmel közleményt fogadott el (a „közlemény") [3]. A közleményt konzultáció céljából elküldték az európai adatvédelmi biztosnak. Az európai adatvédelmi biztos üdvözli azt a tényt, hogy az Európai Bizottság a 45/2001/EK rendelet 41. cikkének megfelelően konzultált vele. Az európai adatvédelmi biztosnak már a közlemény elfogadása előtt lehetősége nyílt arra, hogy előterjessze nem hivatalos észrevételeit. Ezen észrevételek közül néhányat figyelembe vettek a dokumentum végleges változatának elkészítésekor.

2. A közlemény célja, hogy – elsősorban a globalizációból és az új technológiákból származó kihívásokat szem előtt tartva – meghatározza a személyes adatoknak az Unió valamennyi cselekvési területén történő védelmére vonatkozó uniós jogi keret felülvizsgálatára irányuló bizottsági megközelítést [4].

3. Az európai adatvédelmi biztos összességében üdvözli a közleményt, mivel meg van győződve arról, hogy szükséges a jelenlegi uniós adatvédelmi jogi keret felülvizsgálata annak érdekében, hogy az EU hatékony védelmet biztosítson egy folyamatosan fejlődő információs társadalomban. Az adatvédelmi biztos már az adatvédelmi irányelv végrehajtásáról szóló, 2007. július 25-i véleményében [5] megállapította, hogy hosszú távon elkerülhetetlennek tűnik a 95/46/EK irányelv megváltoztatása.

4. A közlemény fontos lépcső e jogszabályi változás felé, amely az uniós adatvédelem területén a legfontosabb fejlemény lenne a 95/46/EK irányelv elfogadása óta; ez utóbbi irányelvet tartják az Európai Unión belül (és tágabb értelemben véve az Európai Gazdasági Térségben) az adatvédelem sarokkövének.

5. A közlemény megfelelő keretet biztosít egy jól célzott felülvizsgálat számára – azért is, mert meghatározza – általánosságban szólva – a legfontosabb kérdéseket és kihívásokat. Az európai adatvédelmi biztos osztja az Európai Bizottság nézetét, miszerint a jövőben is szükség lesz erős adatvédelmi rendszerre azon az alapon, hogy az adatvédelem jelenlegi általános elvei továbbra is indokoltak egy olyan társadalomban, amely a gyors technológiai fejlődés és a globalizáció miatt jelentős változásokon megy át. Ez szükségessé teszi a meglévő jogalkotási intézkedések felülvizsgálatát.

(1) HL L 281., 1995.11.23., 31. o.
(2) HL L 8., 2001.1.12., 1. o.
(3) COM(2010) 609 végleges.
(4) Lásd a közlemény 5. oldalának első bekezdését.
(5) Az európai adatvédelmi biztos 2007. július 25-i véleménye az adatvédelmi irányelv jobb végrehajtását célzó munkaprogram nyomon követéséről szóló, az Európai Parlamenthez és a Tanácshoz címzett bizottsági közleményről, (HL C 255., 2007.10.27., 1. o.).

6. A közlemény helyesen hangsúlyozza, hogy a kihívások óriásiak. Az európai adatvédelmi biztos teljes mértékben egyetért ezzel a kijelentéssel, és kiemeli azt a következményt, hogy a tervezett megoldásoknak ennek megfelelően ambiciózusnak kell lenniük, és fokozniuk kell a védelem hatékonyságát.

1.2. *A vélemény célja*

7. Ez a vélemény a következő két kritérium alapján értékeli a közleményben javasolt megoldásokat: ambíció és hatékonyság. A vélemény várt távlati hatása általánosságban véve pozitív. Az európai adatvédelmi biztos támogatja a közleményt, ugyanakkor kritikát fogalmaz meg olyan pontokon, ahol álláspontja szerint a több ambíció hatékonyabb rendszert eredményezne.

8. Az európai adatvédelmi biztos célja, hogy ezzel a véleménnyel hozzájáruljon az adatvédelmi jogi keret továbbfejlesztéséhez. Várakozással tekint az Európai Bizottság 2011 közepére várható javaslata elé és reméli, hogy a javaslat szövegezése során figyelembe veszik indítványait. Megjegyzi továbbá, hogy úgy tűnik, a közlemény bizonyos területeket – például az uniós intézmények és szervek általi adatfeldolgozást – kizár az általános jogi aktus hatálya alól. Ha az Európai Bizottság valóban úgy döntene, hogy egyes területeket ebben a stádiumban kihagy – amit az európai adatvédelmi biztos sajnálna –, a biztos sürgeti az Európai Bizottságot, hogy kötelezze el magát egy teljesen átfogó architektúra rövid és meghatározott időn belül történő megvalósítása mellett.

1.3. *E vélemény építőelemei*

9. Ez a vélemény nem önmagában áll. Az európai adatvédelmi biztos és az európai adatvédelmi hatóságok különféle korábbi álláspontjain alapul. Különösen ki kell emelni, hogy az európai adatvédelmi biztos már említett, 2007. július 25-i véleményében meghatározták és kidolgozták a jövőbeli változás egyes főbb elemeit ([6]). E vélemény alapját képezik továbbá a magánélet védelme és az adatvédelem területén működő más érdekelt felekkel folytatott megbeszélések is. Az említettek hozzájárulása igen hasznos hátteret nyújtott a közleményhez és ehhez a véleményhez egyaránt. Ezzel kapcsolatban megállapítható, hogy valamilyen szintű együtthatás létezik a tekintetben, hogy hogyan növelhető az adatvédelem hatékonysága.

10. E vélemény másik fontos építőeleme „A magánélet védelmének jövője" című dokumentum, amely a 29. cikk alapján létrehozott adatvédelmi munkacsoport, illetve a rendőrségi és igazságügyi munkacsoport közös hozzájárulása az Európai Bizottság által 2009-ben indított konzultációhoz („a magánélet védelmének jövőjéről szóló munkacsoport-dokumentum") ([7]).

11. Az európai adatvédelmi biztos a közelmúltban, a 2010. november 15-én tartott sajtókonferencián reagált először a jelen közleményre. Ez a vélemény az említett sajtókonferencián elhangzott általános nézeteket fejti ki bővebben ([8]).

12. Végül ez a vélemény az európai adatvédelmi biztos számos korábbi véleményére és a 29. cikk alapján létrehozott adatvédelmi munkacsoport dokumentumaira is támaszkodik. Az említett véleményekre és dokumentumokra mutató hivatkozások e vélemény különböző releváns pontjain megtalálhatók.

2. **Háttér**

13. Az adatvédelmi szabályok felülvizsgálatára kritikus történelmi pillanatban kerül sor. A közlemény alaposan és meggyőzően írja le a hátteret. A leírás alapján az európai adatvédelmi biztos azonosítja azt a négy fő hajtóerőt, ami meghatározza a környezetet, amelyben a felülvizsgálati eljárás zajlik.

14. Az első ilyen tényező a technológiai fejlődés. A mai technológia nem azonos a 95/46/EK irányelv megfogalmazásának és elfogadásának idején létezett technológiával. Az olyan technológiai újítások, mint például a számítási felhő, a viselkedésalapú reklám, a közösségi hálózatok, az útdíj beszedés és a földrajzi helymeghatározó eszközök, alapjaiban megváltoztatták az adatok feldolgozásának módját, és hatalmas kihívásokat állítanak az adatvédelem elé. Az európai adatvédelmi szabályok felülvizsgálatának hatékonyan kell kezelnie ezeket a kihívásokat.

15. A második tényező a globalizáció. A kereskedelmi akadályok fokozatos eltörlése egyre inkább világméretű dimenziót ad a vállalkozásoknak. A határokon átnyúló adatfeldolgozás és a nemzetközi adattovábbítások száma rendkívüli mértékben emelkedett az elmúlt években. Továbbá az információs és kommunikációs technológiák miatt az adatfeldolgozás ma már mindenhol előfordul: az internet és a számítási felhő világszerte lehetővé tette nagy mennyiségű adat más helyen történő feldolgozását. Az utolsó évtized a nemzetközi rendőrségi és igazságügyi tevékenységek növekedését is hozta a terrorizmus és

([6]) Különösen (lásd a vélemény 77. pontját) nincs szükség új elvekre, egyértelműen szükség van viszont egyéb igazgatási intézkedésekre; a személyes adatok mindennemű felhasználására alkalmazandó adatvédelmi jogszabályok széles körű hatályát nem kell módosítani; az adatvédelmi jogszabályoknak konkrét esetekben lehetővé kell tenniük a kiegyensúlyozott megközelítést, az adatvédelmi hatóságok számára pedig azt, hogy prioritásokat határozzanak meg; a rendszert teljes körűen kell alkalmazni a személyes adatok bűnüldözési célú felhasználására, habár az e területen jelentkező különleges problémák kezeléséhez megfelelő kiegészítő intézkedésekre lehet szükség.

([7]) WP 168. sz. dokumentum (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf). A dokumentum fő üzenete, hogy a jogszabályi változás jó alkalom néhány fontos szabály és elv pontosítására (pl. hozzájárulás, átláthatóság), bizonyos új elvek bevezetésére (pl. „beépített adatvédelem", elszámoltathatóság), a hatékonyság növelésére az intézkedések modernizálásával (pl. a meglévő tájékoztatási követelmények korlátozásával), és arra, hogy mindezeket egyetlen átfogó jogi keretbe foglalják (beleértve a rendőrségi és igazságügyi együttműködést is).

([8]) A sajtókonferencián érintett témakörök elérhetők az európai adatvédelmi biztos honlapján a következő címen: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-11-15_Press_conf_speaking_points_PHBG_EN.pdf

a nemzetközi szervezett bűnözés más formái elleni küzdelemben, amit hatalmas mennyiségű bűnüldözési célú információcsere támogatott. Mindezek miatt alaposan át kell gondolni, hogyan biztosítható hatékonyan a személyes adatok védelme a globalizált világban a nemzetközi adatfeldolgozási tevékenység jelentős akadályozása nélkül.

16. A harmadik tényező a Lisszaboni Szerződés. A Lisszaboni Szerződés hatálybalépése új korszakot nyit az adatvédelem szempontjából. Az EUMSZ 16. cikke nemcsak az érintett egyén jogát tartalmazza, hanem közvetlen jogalapot is nyújt egy erős uniós adatvédelmi jogszabály számára. A pillérszerkezet eltörlése továbbá kötelezi az Európai Parlamentet és a Tanácsot, hogy az uniós jog minden területén intézkedjen az adatvédelemről. Más szóval, lehetővé teszi a tagállamokban a magán- és az állami szektorra, valamint az uniós intézményekre és szervekre egyaránt alkalmazandó átfogó adatvédelmi jogi keret kialakítását. A Stockholmi Program ([9]) következetesen állítja ezzel kapcsolatban, hogy az Uniónak átfogó stratégiát kell alkalmaznia a saját területén és a harmadik országokkal fennálló kapcsolatai során megvalósuló adatvédelem érdekében.

17. A negyedik tényezőt nemzetközi szervezetekkel kapcsolatos párhuzamos fejlemények alkotják. Különféle viták folynak a jelenlegi adatvédelmi jogi eszközök modernizációjáról. Ezzel kapcsolatban fontos megemlíteni az Európa Tanács 108. egyezménye ([10]) és a magánélet védelmével foglalkozó OECD-iránymutatás ([11]) jövőbeli felülvizsgálatával kapcsolatos jelenlegi megfontolásokat. Egy másik fontos fejlemény a személyes adatok és a magánélet védelmére vonatkozó nemzetközi normák elfogadása, ami egy kötelező erejű globális adatvédelmi eszköz elfogadásához is elvezethet. Mindezek a kezdeményezések teljes körű támogatást érdemelnek. Közös céljuk a hatékony és következetes védelem biztosítása egy technológiavezérelt és globalizált környezetben.

3. **Fő perspektívák**

3.1. *Az adatvédelem erősíti a bizalmat, és más (köz)érdekeket is támogatnia kell*

18. Az erős adatvédelmi keret szükségszerű következménye annak, hogy a Lisszaboni Szerződés – különösen az Európai Unió Alapjogi Chartájának 8. cikke és az EUMSZ 16. cikke alapján, szorosan kapcsolódva továbbá a Charta 7. cikkéhez – nagy fontosságot tulajdonít az adatvédelemnek ([12]).

19. Az erős adatvédelmi keret szélesebb körű állami és magánérdekeket is szolgál egy olyan információs társadalomban, ahol az adatfeldolgozás mindenütt jelen van. Az adatvédelem erősíti a bizalmat, és a bizalom társadalmunk megfelelő működésének egyik alapvető fontosságú eleme. Fontos, hogy az adatvédelmi intézkedéseket úgy értelmezzék, hogy azok – amennyire lehetséges – aktívan támogassák, ne pedig akadályozzák az egyéb törvényes jogokat és jogos érdekeket.

20. Fontos példák az egyéb jogos érdekekre az erős európai gazdaság, az egyének biztonsága, valamint a kormányok elszámoltathatósága.

21. Az Európai Unió gazdasági fejlődése együtt jár új technológiák és szolgáltatások bevezetésével és piaci értékesítésével. Az információs társadalomban az információs és kommunikációs technológiák és szolgáltatások felbukkanása és sikeres kiépítése a bizalmon múlik. Ha az emberek nem bíznak az IKT-kban, ezek a technológiák kudarcra vannak ítélve. ([13]) Az emberek viszont csak akkor fognak bízni az IKT-kban, ha adataikat hatékonyan megvédik. Az adatvédelemnek tehát a technológiák és szolgáltatások szerves részét kell képeznie. Az erős adatvédelmi keret előmozdítja az európai gazdaságot, feltéve, hogy ez a keret nemcsak erős, de jól is van kialakítva. A további harmonizáció az Európai Unión belül, valamint az adminisztratív terhek minimalizálása ebben a perspektívában elengedhetetlen (lásd a vélemény 5. fejezetét).

22. Az elmúlt években sokat beszéltek a magánélet védelme és a biztonság közötti egyensúly megteremtésének szükségességéről, különösen az adatvédelmi eszközök, valamint a rendőrségi és igazságügyi együttműködés területén zajló információcsere tekintetében. ([14]) Az adatvédelemre elég gyakran – helytelenül – az egyének fizikai biztonsága teljes körű védelmének akadályaként tekintettek ([15]), vagy legalábbis olyan elkerülhetetlen feltételként, amit a bűnüldöző hatóságoknak tiszteletben kell tartani. Ez azonban nem a teljes kép. Az erős adatvédelmi keret fokozhatja és erősítheti a biztonságot. Az adatvédelmi elvek alapján – ha jól alkalmazzák azokat – az adatkezelők kötelesek biztosítani, hogy a tájékoztatás pontos és naprakész legyen, és hogy a bűnüldözés számára nem szükséges, felesleges személyes adatokat távolítsák el a rendszerekből.

([9]) A Stockholmi Program – A polgárokat szolgáló és védő, nyitott és biztonságos Európa; (HL C 115., 2010.5.4., 1. o.), a 10. oldalon.

([10]) Az Európa Tanács 108. egyezménye az egyének személyes adataik gépi feldolgozása során való védelméről, ETS 108. sz., 1981. január 28.

([11]) OECD-iránymutatás a magánélet védelméről és személyes adatok határokon átnyúló továbbításáról; közzétették a http://www.oecd.org oldalon.

([12]) Az adatvédelem fontosságát és a Chartában a magánélet védelméhez való kapcsolódását a Bíróság 2010. november 9-i ítéletében is kiemelte; a C-92/09. és C-93/09. sz. egyesített ügyek, *Schecke*, még nem tették közzé az EBHT-ben

([13]) Lásd az európai adatvédelmi biztos 2010. március 18-i véleményét az információs társadalom iránti bizalomnak az adatok és a magánélet védelme elősegítése révén történő erősítéséről, (HL C 280., 2010.10.16., 1. o.), 113. pont.

([14]) Lásd az európai adatvédelmi biztos 2009. július 10-i véleményét a szabadságon, a biztonságon és a jog érvényesülésén alapuló, a polgárok szolgálatában álló térségről szóló, a Tanácshoz és az Európai Parlamenthez intézett bizottsági közleményről; (HL C 276., 2009.9.17., 8. o.).

([15]) A biztonság a fizikai biztonságnál tágabb értelmű fogalom, de a szóban forgó érvek illusztrálására itt korlátozottabb értelemben értendő.

Ez arra enged következtetni, hogy a rendszerek biztonsága érdekében technológiai és szervezeti intézkedéseket kell végrehajtani, például védeni kell a rendszereket a jogosulatlan közzététellel vagy hozzáféréssel szemben, ahogyan az adatvédelem területén már kidolgozták ezeket.

23. Az adatvédelmi elvek tiszteletben tartása biztosíthatja továbbá, hogy a bűnüldöző hatóságok jogállami keretek között működnek, ami bizalmat kelt a magatartásuk iránt, és ezzel tágabb értelemben fokozza a társadalmainkba vetett bizalmat. Az Emberi Jogok Európai Egyezményének 8. cikke alapján álló ítélkezési gyakorlat biztosítja, hogy a rendőrég és az igazságügyi hatóságok a munkájukhoz szükséges összes adatot feldolgozhatják, de nem korlátlan módon. Az adatvédelemhez elengedhetetlenek az egyensúlyt biztosító eszközök (a rendőrségről és az igazságszolgáltatásról lásd a vélemény 9. fejezetét).

24. A demokratikus társadalmakban a kormányok minden tevékenységükért elszámolással tartoznak, beleértve a személyes adatok különböző közérdekű felhasználását is. Ez az adatok – átláthatóság céljából – interneten történő közzétételétől egészen az adatok közegészségügyi, közlekedési vagy adópolitikák támogatásához való felhasználásáig, illetve magánszemélyek bűnüldözési célú megfigyeléséig terjed. Az erős adatvédelmi keret lehetővé teszi, hogy a kormányok – a felelősségteljes kormányzás részeként – tiszteletben tartsák feladataikat, és elszámoltathatók legyenek.

3.2. *Az adatvédelem jogi keretének következményei*

3.2.1. További harmonizációra van szükség

25. A közlemény helyesen állapította meg, hogy a jelenlegi keret egyik legalapvetőbb hiányossága, hogy túlságosan nagy mérlegelési jogkört biztosít a tagállamoknak az európai rendelkezések nemzeti jogba való átültetésének területén. A harmonizáció hiányának számos negatív következménye van egy olyan információs társadalomban, ahol a tagállamok közötti fizikai határoknak egyre kisebb a jelentősége (lásd a vélemény 5. fejezetét).

3.2.2. Az adatvédelem általános elvei továbbra is érvényben maradnak

26. Az egyik első és formálisabb ok, amiért az adatvédelem általános elveit nem szabad és lehet megváltoztatni, jogi jellegű. Ezeket az elveket az Európa Tanács 108. egyezménye tartalmazza, amely minden tagállamra kötelező erejű. Ez az egyezmény jelenti az adatvédelem alapját az Európai Unióban. Sőt, a legfontosabb alapelvek közül néhányat az Európai Unió Alapjogi Chartájának 8. cikke is kifejezetten említ. Ezen elvek megváltoztatásához tehát az említett Szerződéseket is módosítani kellene.

27. Ez azonban így még nem teljes. Más lényeges okok is vannak arra, hogy miért ne változtassák meg az általános elveket. Az európai adatvédelmi biztos határozottan úgy véli, hogy az információs társadalom nem működhet az egyének magánéletének és személyes adatainak megfelelő védelme nélkül. Ha több adatot dolgoznak fel, jobb védelem is szükséges. Az információs társadalomnak, ahol mindenkiről hatalmas mennyiségű információ feldolgozása folyik, az egyén általi ellenőrzés koncepciójára kell épülnie, lehetővé téve, hogy a személy egyénként járjon el, és élhessen a demokratikus társadalomban létező szabadságaival, mint például a vélemény- és szólásszabadsággal.

28. Nehezen képzelhető el továbbá az egyén általi ellenőrzés anélkül, hogy az adatkezelők ne lennének kötelesek az adatfeldolgozást a szükségesség, az arányosság és a célhoz kötöttség elvének megfelelően korlátozni. Ugyanilyen nehezen képzelhető el az egyén általi ellenőrzés az érintettek elismert jogainak hiányában (pl. az adatokhoz való hozzáférés, helyesbítés, törlés és zárolás joga).

3.2.3. Az alapvető jogok perspektívája

29. Az európai adatvédelmi biztos kiemeli, hogy az adatvédelem alapvető jogként elismert jog. Ez nem azt jelenti, hogy az adatvédelem minden esetben irányadó a demokratikus társadalomban létező más fontos jogokkal és érdekekkel szemben, hanem azt, hogy valóban következményekkel jár az uniós jogi keret értelmében biztosítandó védelem jellegére és terjedelmére – így biztosítva, hogy az adatvédelmi követelményeket mindenkor megfelelően figyelembe veszik.

30. Ezek a főbb következmények az alábbiak szerint határozhatók meg:

— A védelemnek hatékonynak kell lennie. A jogi keretnek olyan eszközökről kell gondoskodnia, amelyek lehetővé teszik, hogy az egyének a gyakorlatban is élhessenek jogaikkal.

— A keretnek hosszú ideig stabilnak kell lennie.

— A védelmet minden körülmények között biztosítani kell, az nem függhet bizonyos időkeretek között a politikai preferenciáktól.

— Szükség lehet a jog gyakorlásának korlátozására, de erre csak kivételesen kerülhet sor, megfelelő indokok alapján, és a korlátozás semmilyen körülmények között nem sértheti magának a jognak az alapvető elemeit ([16]).

Az európai adatvédelmi biztos ajánlja, hogy az Európai Bizottság vegye figyelembe ezeket a következményeket, amikor jogalkotási megoldásokat javasol.

3.2.4. Új jogalkotási intézkedések szükségesek

31. A közlemény helyesen összpontosít az adatvédelmi jogalkotási eszközök erősítésének szükségességére. Ezzel kapcsolatban érdemes felidézni, hogy a magánélet védelmének jövőjéről szóló munkacsoport-dokumentumban ([17]) az adatvédelmi hatóságok hangsúlyozták,

([16]) Lásd még az európai adatvédelmi biztos 2007. július 25-i véleményét az adatvédelmi irányelv jobb végrehajtását célzó munkaprogram nyomon követéséről szóló, az Európai Parlamenthez és a Tanácshoz címzett bizottsági közleményről; a vélemény 17. pontját, amely az Emberi Jogok Európai Bírósága és a Bíróság ítélkezési gyakorlatára épül.

([17]) L. 7. lábjegyzetet.

hogy az adatvédelem különböző szereplőinek – nevezetesen az érintetteknek, az adatkezelőknek és maguknak a felügyelő hatóságoknak – erősebb szerepet kell biztosítani.

32. Úgy tűnik, széles körű konszenzus uralkodik az érdekelt felek között abban, hogy – figyelemmel a technológiai fejlődésre és a globalizációra – az erősebb jogalkotási intézkedések meghozatala az ambiciózus és hatékony adatvédelem megteremtésének kulcsfontosságú eleme. A 7. pontban említetteknek megfelelően ezek azok a kritériumok, amelyeket az európai adatvédelmi biztos a javasolt megoldások értékeléséhez használ.

3.2.5. Átfogó jelleg, mint elengedhetetlen feltétel

33. Ahogyan a közlemény is emlékeztet rá, a 95/46/EK irányelv a tagállamok állami és magánszektoraiban végzett valamennyi személyesadat-feldolgozási tevékenységre alkalmazandó, kivéve azokat a tevékenységeket, amelyek kívül esnek a korábbi közösségi jog ([18]) hatályán. Míg az előző Szerződésben szükség volt erre a kivételre, a Lisszaboni Szerződés hatálybalépése után már nem ez a helyzet. Sőt, a kivétel ellentétes az EUMSZ 16. cikkével – annak szövegével, de a szellemével mindenképpen.

34. Az európai adatvédelmi biztos szerint az átfogó adatvédelmi jogi eszközre – beleértve a büntetőügyekben folytatott rendőrségi és igazságügyi együttműködést is – úgy kell tekintetni, mint az egyik legfőbb előrelépésre, amit egy új jogi keret megvalósíthat. Ez a hatékony adatvédelem egyik elengedhetetlen feltétele a jövőben.

35. Az európai adatvédelmi biztos – állításának alátámasztására – kiemeli a következő érveket:

— A magánszektor és a bűnüldözési szektor tevékenységei közötti határvonal elmosódóban van. A magánszektorbeli intézmények feldolgozhatnak olyan adatokat, amelyeket végül bűnüldözési célokra használnak fel (példa: utasnyilvántartási adatok (PNR-adatok ([19])), míg más esetekben kötelesek megőrizni az adatokat bűnüldözési célokra (példa: adatmegőrzési irányelv ([20])).

— Nincs alapvető különbség a rendőrségi és igazságügyi hatóságok és a bűnüldözéssel foglalkozó egyéb hatóságok (adó-, vám-, csalás elleni, bevándorlási hatóságok) között, amelyek a 95/46/EK irányelv hatálya alá tartoznak.

— Ahogyan a közlemény pontosan leírja, a rendőrségre és az igazságügyi hatóságokra alkalmazandó jelenlegi adatvédelmi jogi eszköz (2008/977/IB kerethatározat ([21])) nem megfelelő.

— A legtöbb tagállam beemelte a 95/46/EK irányelvet és a 108. egyezményt nemzeti jogába, azaz ezek a jogi aktusok saját rendőrségére és igazságügyi hatóságaira is alkalmazandók lettek.

36. A rendőrség és az igazságszolgáltatás felvétele az általános jogi eszközbe nemcsak több garanciát nyújtana a polgároknak, hanem a rendőri hatóságok feladatát is megkönnyítené. Ha különféle szabályrendszereket kell alkalmazni, az fáradságos, feleslegesen időrabló, és útjában áll a nemzetközi együttműködésnek (lásd még a vélemény 9. fejezetét). Ez a nemzetbiztonsági szolgálatok adatfeldolgozó tevékenységének belefoglalása mellett is szól, amennyiben az uniós jog jelenlegi állása szerint ez lehetséges.

3.2.6. Technológiai semlegesség

37. A 95/46/EK irányelv 1995-ös elfogadása óta eltelt időszakot viharos technológiai változások jellemzik. Gyakran vezettek be új technológiai fejlesztéseket és alkalmazásokat. Ez sok esetben alapvető változásokat eredményezett az egyének személyes adatai feldolgozásának módjában. Az információs társadalom már nem tekinthető párhuzamos környezetnek, amelyben az egyének önként részt vehetnek, hanem mindennapi életünk szerves részévé vált. Például a „tárgyak internete" fogalom ([22]) kapcsolatokat létesít fizikai objektumok és a rájuk vonatkozó online információk között.

38. A technológia fejlődik tovább. Ennek megvannak a következményei az új jogi keretre vonatkozóan. Annak több évre hatékonynak kell lennie, ugyanakkor nem állhat a további technológiai fejlesztések útjában. Ehhez az szükséges, hogy a jogi intézkedések technológiailag semlegesek legyenek. A keretnek azonban nagyobb jogbiztonságot kell nyújtania a vállalatoknak és az egyéneknek egyaránt. Tudniuk kell, mit várnak tőlük, és biztosítani kell számukra, hogy élhessenek jogaikkal. Ehhez viszont a jogi intézkedéseknek pontosnak kell lenniük.

39. Az európai adatvédelmi biztos szerint az általános adatvédelmi jogi eszközt – amennyire lehetséges – technológiailag semleges módon kell megszövegezni. Ez azt jelenti, hogy a különböző szereplők jogait és kötelezettségeit általános és semleges módon kell megfogalmazni, hogy a személyes adatok feldolgozásához választott technológiától függetlenül is általában érvényesek és kikényszeríthetők maradjanak. A mai technológiai haladás gyors üteme miatt nincs más lehetőség. Az európai adatvédelmi biztos javasolja olyan új, „technológiailag semleges" jogok

([18]) Ez a vélemény elsősorban a korábbi harmadik pillérre összpontosít (rendőrségi és igazságügyi együttműködés büntető ügyekben), mivel a korábbi második pillér nemcsak az uniós jog egyik bonyolultabb területe (ahogyan ezt az EUMSZ. 16. cikke és az Európai Unióról szóló szerződés 39. cikke is elismeri), hanem kevésbé lényeges is az adatfeldolgozás szempontjából.

([19]) Lásd pl. az utasnyilvántartási adatállomány (PNR) adatainak harmadik országok részére történő továbbításával kapcsolatos általános megközelítésről szóló bizottsági közleményt, COM(2010) 492 végleges.

([20]) Az Európai Parlament és a Tanács 2006. március 15-i 2006/24/EK irányelve a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtása, illetve a nyilvános hírközlő hálózatok szolgáltatása keretében előállított vagy feldolgozott adatok megőrzéséről és a 2002/58/EK irányelv módosításáról (HL L 105., 2006.4.13., 54. o.).

([21]) A Tanács 2008. november 27-i 2008/977/IB kerethatározata a büntetőügyekben folytatott rendőrségi és igazságügyi együttműködés keretében feldolgozott személyes adatok védelméről (HL L 350., 2008.12.30., 60. o.).

([22]) A fogalom meghatározása „A tárgyak internete – Cselekvési terv Európáért" című dokumentumban található, COM(2009) 278 végleges.

bevezetését a meglévő adatvédelmi elveken felül, amelyek különösen fontosak lehetnek a gyorsan változó elektronikus környezetben (lásd elsősorban a 6. és 7. fejezetet).

3.2.7. Hosszú távon: jogbiztonság hosszabb időre

40. Az elmúlt tizenöt évben a 95/46/EK irányelv volt az adatvédelem központi jogi aktusa az Európai Unióban. Beemelték a tagállamok jogába, és a különböző szereplők alkalmazták. Az évek során az alkalmazás tanult a gyakorlati tapasztalatokból és az Európai Bizottság, az adatvédelmi hatóságok (nemzeti szinten, illetve a 29. cikk alapján létrehozott munkacsoport keretében), valamint a nemzeti és az európai bíróságok további iránymutatásaiból.

41. Hangsúlyozandó, hogy ezekhez a fejlesztésekhez idő kell, és – különösen mivel alapvető jogot életbe léptető általános keretről van szó – ez az idő szükséges a jogbiztonság és a stabilitás megteremtéséhez. Az új jogi eszközt azzal az ambícióval kell megszövegezni, hogy hosszabb időre képes legyen megteremteni a jogbiztonságot és stabilitást, szem előtt tartva, hogy nehezen megjósolható, hogyan fejlődik tovább a technológia és a globalizáció. Mindenesetre az európai adatvédelmi biztos teljes körűen támogatja a hosszú távú jogbiztonság megteremtésének célját, hasonlóan a 95/46/EK irányelv perspektívájához. Röviden, ahol a technológia gyors ütemben fejlődik, a jognak stabilnak kell maradnia.

3.2.8. Rövid távon: a meglévő eszközök jobb kihasználása

42. Rövid távon elengedhetetlen a meglévő jogi intézkedések hatékonyságának biztosítása – középpontban a szabályok érvényesítésével – nemzeti és uniós szinten egyaránt (lásd e vélemény 11. fejezetét).

B. AZ ÚJ KERET ELEMEI

4. Átfogó megközelítés

43. Az európai adatvédelmi biztos teljes mértékben támogatja az adatvédelemmel kapcsolatos átfogó megközelítést, ami nemcsak a közlemény címe, hanem kiindulópontja is, és szükségképpen tartalmazza az adatvédelem általános elveinek kiterjesztését a büntetőügyekben folytatott rendőrségi és igazságügyi együttműködésre ([23]).

44. Megjegyzi azonban, hogy az Európai Bizottság nem kívánja belevenni az összes adatfeldolgozási tevékenységet ebbe az általános jogi eszközbe. Különösen az uniós intézmények, szervek és hivatalok általi adatfeldolgozás fog kimaradni. Az Európai Bizottság csak annyit mond, hogy „megvizsgálja, hogy más jogi aktusokat is hozzá kell-e igazítani az adatvédelmi keret új generációjához".

([23]) Lásd a közlemény 14. oldalát és e vélemény 3.2.5. szakaszát.

45. Az európai adatvédelmi biztos egyértelmű preferenciája, hogy az európai uniós szintű adatfeldolgozást vegyék bele az általános jogi keretbe. Arra emlékeztet, hogy ez volt a korábbi EK-Szerződés 286. cikkének eredeti szándéka, amely először említette az adatvédelmet a Szerződés szintjén. Az EK-Szerződés 286. cikke egyszerűen kimondta, hogy a személyes adatok feldolgozásával kapcsolatos jogi eszközök az intézményekre is alkalmazandók. Ami még fontosabb: egyetlen jogi szöveg kivédi a rendelkezések közötti ellentmondások kockázatát, és ez lenne a legmegfelelőbb az uniós szintű, illetve a tagállami köz- és magánintézmények közötti adatcserére vonatkozóan. Azt a kockázatot is elkerülné, hogy a 95/46/EK irányelv módosítása után megszűnne a politikai érdek a 45/2001/EK rendelet módosítására vagy arra, hogy e módosítás elegendő prioritást kapjon a hatálybalépés dátumaival kapcsolatos ellentmondások elkerülése érdekében.

46. Az európai adatvédelmi biztos sürgeti, hogy az Európai Bizottság – amennyiben úgy vélné, hogy az uniós szintű adatfeldolgozás felvétele az általános jogi eszközbe nem lenne megvalósítható – kötelezze el magát amellett, hogy a lehető legrövidebb időn belül, lehetőleg 2011 végéig javaslatot tesz a 45/2001/EK rendelet hozzáigazítására (nem arra, hogy „megvizsgálja, hogy hozzá kell-e igazítani").

47. Ugyanilyen fontos, hogy az Európai Bizottság biztosítsa, hogy más területek nem szorulnak háttérbe, különösen:

— Adatvédelem a közös kül- és biztonságpolitikában az Európai Unióról szóló szerződés 39. cikke alapján ([24]).

— Ágazatspecifikus adatvédelmi rendszerek az Európai Unió intézményei (pl. Europol, Eurojust) és nagyléptékű információs rendszerek számára, amennyiben ezeket a rendszereket hozzá kell igazítani az új jogi eszközhöz.

— Az elektronikus hírközlési adatvédelmi irányelv (2002/58/EK), amennyiben hozzá kell igazítani az új jogi eszközhöz.

48. Végül az adatvédelem általános jogi eszközét valószínűleg ki kell egészíteni további ágazati és speciális előírásokkal, például a rendőrségi és igazságügyi együttműködésre vonatkozóan, de más területeken is ([25]). Ha szükséges – és összhangban a szubszidiaritás elvével –, ezeket a kiegészítő előírásokat uniós szinten kell elfogadni. A tagállamok kiegészítő szabályokat is kidolgozhatnak olyan speciális területeken, ahol ez indokolt (lásd az 5.2. szakaszt).

([24]) Lásd még az európai adatvédelmi biztos 2010. november 24-i véleményét „Az EU terrorizmusellenes politikája: legfőbb eredmények és jövőbeni kihívások" című, az Európai Parlamentnek és a Tanácsnak szóló bizottsági közleményről, 31. pont.

([25]) Lásd még a magánélet védelmének jövőjéről szóló munkacsoportdokumentum (7. lábjegyzet) 18–21. pontját.

5. **További harmonizáció és egyszerűsítés**

5.1. *A harmonizáció szükségessége*

49. A harmonizáció kiemelkedően fontos az Európai Unió adatvédelmi joga szempontjából. A közlemény helyesen emelte ki, hogy az adatvédelemnek erős belső piaci dimenziója van, mivel biztosítania kell a személyes adatok szabad áramlását a tagállamok között a belső piacon. A jelenlegi irányelv szerinti harmonizáció szintje azonban a megítélések szerint nem kielégítő. A közlemény elismeri, hogy ez az egyik ismétlődő aggodalom az érdekelt felek részéről. Az érdekelt felek különösen kiemelik a jogbiztonság fokozásának, az adminisztratív teher csökkentésének szükségességét, valamint azt, hogy azonos versenyfeltételeket kell biztosítani a gazdasági szereplők számára. Ahogyan az Európai Bizottság – helyesen – megjegyzi, különösen ez a helyzet a több tagállamban működő adatkezelők esetében, akiknek a nemzeti adatvédelmi jogszabályok (adott esetben eltérő) követelményeit kell betartaniuk ([26]).

50. A harmonizáció nemcsak a belső piac szempontjából, hanem a megfelelő adatvédelem biztosítása céljából is fontos. Az EUMSZ 16. cikke úgy rendelkezik, hogy „mindenkinek" joga van a rá vonatkozó személyes adatok védelméhez. E jog hatékony tiszteletben tartása érdekében az egész Európai Unióban azonos szintű védelmet kell garantálni. A magánélet védelmének jövőjéről szóló munkacsoport-dokumentum kiemelte, hogy az érintettek pozíciójával kapcsolatban számos rendelkezést nem hajtottak végre, illetve nem egységesen értelmeztek az összes tagállamban ([27]). Egy globalizált és összekapcsolódó világban ezek a különbözőségek alááshatják vagy korlátozhatják az egyének védelmét.

51. Az európai adatvédelmi biztos úgy véli, a további és jobb harmonizáció a felülvizsgálati eljárás egyik legfőbb célkitűzése. Az európai adatvédelmi biztos üdvözli az Európai Bizottság elkötelezettségét aziránt, hogy megvizsgálja az adatvédelem további, uniós szintű harmonizációjának módját. Némileg meglepődve jegyzi meg azonban, hogy a közlemény ezen a ponton semmiféle konkrét lehetőséget nem vet fel. Ezért maga jelez néhány területet, ahol a jobb konvergencia a legsürgetőbb (lásd az 5.3. szakaszt). Ezeken a területeken a további harmonizációt nemcsak a nemzeti jog mozgásterének korlátozásával kell elérni, hanem a helytelen tagállami végrehajtás megakadályozásával (lásd a 11. fejezetet is), valamint a következetesebb és összehangoltabb érvényesítés biztosítása által (lásd a 10. fejezetet is).

([26]) A közlemény, 10. oldal.

([27]) Lásd A magánélet védelmének jövőjéről szóló munkacsoport-dokumentum (7. lábjegyzet) 70. pontját. A dokumentum említi különösen a felelősséggel kapcsolatos rendelkezéseket, valamint a nem vagyoni kártérítés követelésének lehetőségét.

5.2. *A mozgástér csökkentése az irányelv végrehajtása tekintetében*

52. Az irányelv számos olyan rendelkezést tartalmaz, amelyeket tág értelemben fogalmaztak meg, ezért helyet hagynak az eltérő értelmezésnek. Az irányelv (9) preambulumbekezdése kifejezetten megerősíti, hogy a tagállamok rendelkeznek bizonyos mozgástérrel, és e mozgástér keretein belül különbségek merülhetnek fel az irányelv végrehajtása során. A tagállamok számos rendelkezést, köztük döntő fontosságúakat is, különbözőképpen hajtottak végre ([28]). Ez a helyzet nem megfelelő, nagyobb konvergenciára kell törekedni.

53. Ez nem jelenti azt, hogy a sokszínűséget teljesen ki kell zárni. Bizonyos területeken rugalmasságra lehet szükség egyes indokolt sajátosságok, fontos közérdekek vagy a tagállamok intézményi autonómiája megőrzése érdekében. Az európai adatvédelmi biztos szerint a tagállamok közötti eltérések lehetőségét különösen a következő konkrét helyzetekben kell korlátozni:

— Szólásszabadság: a jelenlegi jogi keret szerint (9. cikk) a tagállamok felmentésről, illetve eltérésről kizárólag a személyes adatoknak újságírás, vagy irodalmi, illetve művészi kifejezés céljából történő feldolgozása esetén rendelkezhetnek. Ez a rugalmasság – tekintve az e téren a tagállamokban létező eltérő hagyományokra és kulturális különbségekre – megfelelőnek tűnik, figyelemmel természetesen az EU Alapjogi Chartájában és az emberi jogok európai egyezményében található korlátozásokra. Ez azonban nem állna a jelenlegi 9. cikk lehetséges frissítésének útjában, amelyet az internettel kapcsolatos fejlemények figyelembevételével szövegeznének meg.

— Konkrét közérdekek: a jelenlegi keret szerint (13. cikk) a tagállamok jogszabályokat fogadhatnak el a jogok és kötelezettségek körének korlátozására, amennyiben a korlátozás fontos közérdek (például a nemzetbiztonság, a honvédelem, a közbiztonság, stb.) biztosításához szükséges. A tagállamok e hatásköre továbbra is indokoltan áll fenn. A kivételek értelmezését azonban lehetőség szerint még jobban harmonizálni kell (lásd a 9.1. szakaszt). Ezenkívül a 6. cikk (1) bekezdése alóli kivétel jelenlegi hatóköre túlzottan szélesnek tűnik.

— Jogorvoslatok, szankciók és adminisztratív eljárások: az európai keretnek meg kell határoznia a fő feltételeket, de az uniós jog jelenlegi állása szerint a nemzeti szinten alkalmazandó szankciók, jogorvoslatok, eljárási szabályok és az ellenőrzés részletes szabályai meghatározását a tagállamokra kell hagyni.

([28]) Bizonyos eltérő megközelítések a manuális adatokkal kapcsolatban is léteznek.

5.3. *A további harmonizáció területei*

54. *Fogalommeghatározások* (a 95/46/EK irányelv 2. cikke). A fogalommeghatározások a jogrendszer sarokkövét alkotják; ezeket minden tagállamban egységesen kell értelmezni, végrehajtási eltérés nélkül. Eltérések merültek fel a jelenlegi keret szerint, mint például az adatkezelő fogalmával kapcsolatban. ([29]) Az európai adatvédelmi biztos a nagyobb jogbiztonság biztosítása érdekében javasolja további tételek hozzáadását a 2. cikkben szereplő jelenlegi listához, mint például anonim adatok, álnéven szereplő adatok, bírósági adatok, adattovábbítás és adatvédelmi tisztviselő.

55. Az *adatfeldolgozás jogszerűsége* (5. cikk). Az új jogi eszköznek a lehető legpontosabbnak kell lennie – figyelemmel az adatfeldolgozás jogszerűségét eldöntő alapelemekre. Ezért az irányelv 5. cikkére (és (9) preambulumbekezdésére), amely megbízza a tagállamokat, hogy részletesen határozzák meg, hogy a személyes adatok feldolgozása milyen feltételek mellett jogszerű, a jövőbeli keretben már nem lesz szükség.

56. Az *adatfeldolgozás jogalapja* (7. és 8. cikk). Az adatfeldolgozás feltételeinek meghatározása minden adatvédelmi jogszabály nélkülözhetetlen eleme. Nem szabad megengedni, hogy a tagállamok további vagy módosított jogalapokat vezessenek be az adatfeldolgozásra, vagy egyes jogalapokat kizárjanak. Az eltérések lehetőségét ki kell zárni vagy korlátozni kell (különösen az érzékeny adatok tekintetében ([30])). Az új jogi eszközben pontosan meg kell fogalmazni az adatvédelem jogalapjait, ez csökkenti a megítélésbeli különbségeket a végrehajtás vagy érvényesítés során. Különösen a hozzájárulás fogalmát kell részletesebben meghatározni (lásd a 6.5. szakaszt). Ezenfelül az adatkezelő jogszerű érdekén alapuló jogalap (7. cikk f) pontja) – rugalmas jellege miatt – igen eltérő értelmezésekre ad módot. További körülírásra van szükség. Egy másik rendelkezés, amit lehetőség szerint jobban körül kell írni, a 8. cikk (2) bekezdésének b) pontja, amely engedélyezi érzékeny adatok feldolgozását, ha az az adatkezelő kötelezettségei és meghatározott jogai gyakorlása érdekében szükséges a foglalkoztatási jogszabályok területén ([31]).

57. Az *érintett jogai* (10–15. cikk). Ez az egyik olyan terület, ahol a tagállamok az irányelv nem minden elemét hajtják végre és értelmezik egységesen. Az érintettek jogai a hatékony adatvédelem egyik központi elemét alkotják. Ezért ebben a tekintetben a mérlegelési mozgásteret jelentősen csökkenteni kell. Az európai adatvédelmi biztos ajánlja, hogy az adatkezelő által az érintetteknek adott információk legyenek egységesek az egész Európai Unióban.

58. *Nemzetközi adattovábbítások* (25–26. cikk). Ez olyan terület, amely az egységes uniós gyakorlat hiánya miatt széles körben kritikára adott okot. Az érdekelt felek kritizálták, hogy a tagállamok igen eltérően értelmezik és hajtják végre az Európai Bizottság megfelelőségi határozatait. A kötelező erejű vállalati szabályok egy másik olyan elem, ahol az európai adatvédelmi biztos további harmonizációt javasol (lásd a 9. fejezetet).

59. *Nemzeti adatvédelmi hatóságok* (28. cikk) A nemzeti adatvédelmi hatóságokra igen eltérő szabályok vonatkoznak a 27 uniós tagállamban, különösen jogállásuk, erőforrásaik és hatáskörük tekintetében. A 28. cikk pontatlanságával részben hozzájárult ehhez a különbözőséghez ([32]), ezért további pontosításra szorul, összhangban az Európai Bíróság C-518/07. számú ügyben hozott ítéletével ([33]) (lásd még a 10. fejezetet).

5.4. *Az értesítési rendszer egyszerűsítése*

60. Az értesítési követelmények (a 95/46/EK irányelv 18–21. cikke) egy másik olyan terület, ahol a tagállamok eddig jelentős szabadsággal rendelkeztek. A közlemény helyesen ismeri fel, hogy egy harmonizált rendszer csökkentené az adatkezelők költségeit és adminisztratív terheit ([34]).

61. Ezen a területen az egyszerűsítés legyen a fő célkitűzés! Az adatvédelmi keret felülvizsgálata egyedülálló lehetőség a jelenlegi értesítési követelmények további egyszerűsítésére és/vagy hatókörének csökkentésére. A közlemény felismeri, hogy az érdekelt felek között általános az egyetértés, hogy a jelenlegi értesítési rendszer meglehetősen terhes, és önmagában véve nem biztosít hozzáadott értéket az érintettek személyes adatainak védelme terén ([35]). Az európai adatvédelmi biztos ezért üdvözli az Európai Bizottság elkötelezettségét aziránt, hogy megvizsgálja a jelenlegi bejelentési rendszer egyszerűsítésének különféle lehetőségeit.

62. Álláspontja szerint az egyszerűsítés kiindulópontja az áttérés lenne egy olyan rendszerről, ahol a főszabály – ellenkező rendelkezés hiányában (azaz a „kivételek rendszere") – a bejelentés, egy célzottabb rendszerre. A kivételek rendszere nem bizonyult hatékonynak, mivel a tagállamok egyeztetés nélkül, egymásnak ellentmondóan hajtották végre. ([36]) Az európai adatvédelmi biztos a következő alternatívák mérlegelését javasolja:

([29]) Lásd a 29. cikk alapján létrehozott munkacsoport 1/2010. sz. véleményét az „adatkezelő" és az „adatfeldolgozó" fogalmának meghatározásáról (WP 169).

([30]) A 8. cikk (4) és (5) bekezdése jelenleg bizonyos feltételek mellett felhatalmazza a tagállamokat, hogy további eltéréseket állapítsanak meg az érzékeny adatokkal kapcsolatban.

([31]) Ezzel kapcsolatban lásd az Európai Bizottság fent hivatkozott első jelentését az adatvédelmi irányelv végrehajtásáról, 14. o.

([32]) A magánélet védelmének jövőjéről szóló munkacsoport-dokumentum, 87. pont.

([33]) A C-518/07. sz. ügy, *Európai Bizottság kontra Németország*, még nem tették közzé az EBHT-ben.

([34]) L. 26. lábjegyzet.

([35]) L. 26. lábjegyzet.

([36]) A 29. cikk alapján létrehozott munkacsoport jelentése a nemzeti felügyelő hatóságok értesítésének kötelezettségéről, a kivételek és egyszerűsítések legjobb felhasználásáról, valamint az adatvédelmi tisztviselők szerepéről az Európai Unióban, WP 106., 2005, 7. o.

— a kötelezettség korlátozása meghatározott típusú, speciális kockázatokkal járó adatfeldolgozási műveletek bejelentésére (a bejelentés további lépéseket indíthatna el, mint például az adatfeldolgozás előzetes ellenőrzése);

— egyszerű regisztrációs kötelezettség, amelynek keretében az adatkezelő köteles az adatfeldolgozást nyilvántartásba venni (ellentétben az összes adatfeldolgozási művelet széles körű nyilvántartásba vételével).

Ezenfelül be lehetne vezetni az általános páneurópai bejelentési formanyomtatványt, így biztosítva az összehangolt megközelítést a kért információk tekintetében.

63. A jelenlegi bejelentési rendszer felülvizsgálata nem lehet joghatással egyes, valószínűsíthetően speciális kockázatot jelentő adatfeldolgozási kötelezettségek (pl. nagyléptékű információs rendszerek) előzetes ellenőrzési kötelezettségének javítására. Az európai adatvédelmi biztos támogatná, ha az új jogi eszközbe felvennének egy nem teljes listát azokról az esetekről, amikor az előzetes ellenőrzés kötelező. A személyes adatok közösségi intézmények és szervek által történő feldolgozása tekintetében az egyének védelméről, valamint az ilyen adatok szabad áramlásáról szóló 45/2001/EK rendelet hasznos mintát ad erre ([37]).

5.5. *Rendelet, nem pedig irányelv*

64. Végezetül, az európai adatvédelmi biztos úgy véli, a felülvizsgálati eljárás jó alkalom annak átgondolására, milyen típusú jogi eszközre lenne szükség az adatvédelem szabályozásához. A rendelet – azaz egy olyan egységes eszköz, amely közvetlenül alkalmazandó a tagállamokban – a leghatékonyabb eszköz az adatvédelemhez való alapvető jog megvédésére, és egy olyan valódi belső piac létrehozására, ahol a személyes adatok szabadon áramolhatnak, és a védelem szintje az adatfeldolgozás helye szerinti országtól vagy ágazattól függetlenül azonos.

65. A rendelet csökkentené az egymásnak ellentmondó értelmezések és az indokolatlan különbségek esélyét a jogszabály végrehajtása és alkalmazása során. Csökkentené továbbá az Európai Unión belüli adatfeldolgozási műveletekre alkalmazandó jog meghatározásának fontosságát, ami a jelenlegi rendszer egyik legellentmondásosabb oldala (lásd a 9. fejezetet).

66. Az adatvédelem területén a rendelet annál is inkább indokolt, mivel

— az EUMSZ 16. cikke a Szerződés szintjére emelte a személyes adatok védelméhez való jogot, és az egész Európai Unióban egységes szintű védelmet irányoz elő – sőt rendel el – az egyének tekintetében.

— Az adatfeldolgozás elektronikus környezetben történik, ahol a tagállamok közötti belső határok egyre kevésbé lényegesek.

67. Ha a rendeletet, mint általános eszközt választják, azzal szükség esetén lehetővé válik, hogy – ahol rugalmasság szükséges – bizonyos rendelkezéseket közvetlenül a tagállamokhoz intézzenek. A rendelet választása nem befolyásolja továbbá a tagállamok azon hatáskörét, hogy szükség esetén – az uniós jogszabályokkal összhangban – kiegészítő szabályokat fogadjanak el az adatvédelemre vonatkozóan.

6. **Az egyének jogainak erősítése**

6.1. *A jogok erősítésének szükségessége*

68. Az európai adatvédelmi biztos teljes mértékben támogatja a közleményt, amikor az az egyének jogainak erősítését javasolja, mivel a meglévő jogi eszközök nem teljesen biztosítják azt a hatékony védelmet, amelyre az egyre összetettebb digitalizált világban szükség van.

69. Egyfelől a digitalizált világ fejlődése együtt jár a személyes adatok – rendkívül bonyolult és nem átlátható módon történő – gyűjtésének, felhasználásának és továbbításának erőteljes növekedésével. Az egyének sokszor nem tudják vagy nem értik, hogyan történik mindez, ki gyűjti az adataikat, illetve hogyan gyakorolhatnának ellenőrzést efölött. Jól szemlélteti a jelenséget az egyének internetes böngésző tevékenységét – a célzott hirdetés érdekében – sütik és más hasonló eszközök segítségével nyomon követő hirdetési hálózatok tevékenysége. Amikor a felhasználó felkeres weboldalakat, nem számít rá, hogy egy kívülálló fél naplózza a kattintásait és felhasználói rekordokat hoz létre olyan információk alapján, amelyek megmutatják életstílusát, vagy azt, hogy mit szeret és mit nem.

70. Másfelől a fejlődés arra ösztönzi az egyéneket, hogy proaktívan megosszák egymással személyes információikat, például a közösségi hálózatok weboldalain. Egyre fiatalabb emberek vesznek részt a közösségi hálózatokban, és tartanak fenn kapcsolatot társaikkal. Kétséges, hogy a (fiatal) emberek tisztában vannak kitárulkozásuk mélységével, és cselekedetük hosszú távú hatásaival.

6.2. *Növekvő átláthatóság*

71. Az átláthatóság minden adatvédelmi rendszerben rendkívül fontos, nemcsak a hozzá tartozó érték miatt, hanem azért is, mert lehetővé teszi más adatvédelmi elvek érvényesülését. Az egyének csak akkor tudják jogaikat gyakorolni, ha tudnak az adatfeldolgozásról.

72. A 95/46/EK irányelvben számos rendelkezés foglalkozik az átláthatósággal. A 10. és 11. cikk azt a kötelezettséget tartalmazza, hogy tájékoztatni kell az egyént, ha adatot gyűjtenek róla. Sőt a 12. cikk elismeri az egyén arra vonatkozó jogát, hogy érthető formában másolatot kapjon saját személyes adatairól (adathozzáféréshez való jog). A 15. cikk elismeri a hozzáférési jogot a jogi hatással járó automatizált döntések meghozatala során alkalmazott logikához. Végül, de nem utolsósorban a 6. cikk (1) bekezdésének a) pontja, amely előírja, hogy az adatok feldolgozását tisztességesen kell végezni, szintén maga után vonja az átláthatóság követelményét. Személyes adatok nem dolgozhatók fel rejtett vagy titkos okból.

([37]) Lásd a rendelet 27. cikkét, (HL L 8., 2001.1.12., 1. o.).

73. A közlemény javasolja az átláthatóság általános elvének hozzáadását. Erre a javaslatra válaszul az európai adatvédelmi biztos kiemeli, hogy az átláthatóság fogalma már a jelenlegi adatvédelmi jogi keretnek is szerves részét képezi, jóllehet hallgatólagosan. Ez az átláthatósággal foglalkozó, az előző bekezdésben említett különféle rendelkezésekből is látható. Az európai adatvédelmi biztos szerint hozzáadott értéket jelentene, ha *kifejezetten* kimondanák az átláthatóság elvét – akár a tisztességes adatfeldolgozás meglévő rendelkezésével összekapcsolva, akár attól függetlenül. Ez növelné a jogbiztonságot és megerősítené, hogy az adatkezelő köteles a személyes adatokat minden körülmények között átlátható módon feldolgozni – nemcsak kérésre vagy akkor, ha konkrét jogi rendelkezés kötelezi erre.

74. Még fontosabb azonban ennél az átláthatósággal kapcsolatos meglévő rendelkezések –például a 95/46/EK irányelv 10. és 11. cikke – megerősítése. Az említett rendelkezések azokat az információelemeket határozzák meg, amelyeket kötelező megadni, de nem írják le pontosan ennek részletes szabályait. Konkrétabban, az európai adatvédelmi biztos javasolja, hogy a következőkkel erősítsék a meglévő rendelkezéseket:

— Az adatkezelőkre vonatkozó azon követelmény, hogy egyszerűen hozzáférhető és könnyen érthető módon, világos és közérthető nyelven adjanak tájékoztatást az adatfeldolgozásról ([38]). A tájékoztatásnak egyértelműnek, tisztán láthatónak és szembetűnőnek kell lennie. A rendelkezés magában foglalhatná a tájékoztatás könnyen érthetőségének biztosítására irányuló kötelezettséget is. E kötelezettség meg nem engedetté tenné a homályos vagy nehezen érthető adatvédelmi politikákat.

— Az a követelmény, hogy a tájékoztatás könnyen elérhető legyen, és azt közvetlenül az érintetteknek nyújtsák. A tájékoztatásnak állandóan elérhetőnek kell lennie, nem szabad, hogy rövid idő után eltűnjön az adott elektronikus médiumból. Ez segítené a felhasználókat az információk jövőbeli tárolásában és újraelőállításában, lehetővé téve a további hozzáférést.

6.3. *A biztonság megsértésének bejelentésére irányuló kötelezettség támogatása*

75. Az európai adatvédelmi biztos támogatja egy olyan rendelkezés bevezetését a személyes adatok megsértése esetén fennálló tájékoztatási kötelezettséggel kapcsolatban, amely a felülvizsgált elektronikus hírközlési adatvédelmi irányelvben egyes szolgáltatókra vonatkozó kötelezettséget az összes adatkezelőre kiterjeszti, ahogyan azt a közlemény javasolja. A felülvizsgált elektronikus hírközlési adatvédelmi irányelv értelmében a kötelezettség csak az elektronikus hírközlési szolgáltatásokat nyújtó szolgáltatókra vonatkozik (telefonszolgáltatók (az internetalapú beszédhívásokat (VoIP) is beleértve) és internet-hozzáférést kínáló szolgáltatók). Más adatkezelőkre ez a kötelezettség nem vonatkozik. A kötelezettséget alátámasztó okok teljes mértékben vonatkoznak azokra az adatkezelőkre is, amelyek nem elektronikus hírközlési szolgáltatásokat nyújtó szolgáltatók.

76. A biztonság megsértésének bejelentése különböző célokat szolgál. A legnyilvánvalóbb, amit a közlemény is hangsúlyoz, hogy a bejelentés tájékoztatási eszköz legyen, amely ráébreszti az egyéneket arra, hogy személyes adataik sérülése milyen kockázatokkal jár. Ez segíthet abban, hogy e kockázatok csökkentésére megtegyék a szükséges intézkedéseket. Ha például valakit pénzügyi információinak sérüléséről értesítenek, ez a személy többek között megváltoztathatja a jelszavát vagy megszüntetheti a bankszámláit. Ezenkívül a biztonság megsértésének bejelentése az irányelvben szereplő más elvek és kötelezettségek hatékony alkalmazásához is hozzájárul. Például a biztonság megsértésének bejelentésére vonatkozó követelmények arra ösztönzik az adatkezelőket, hogy erősebb biztonsági intézkedéseket hajtsanak végre a jogsértések megelőzése érdekében. A biztonság megsértésének bejelentése az adatkezelők felelőssége erősítésének, sőt az elszámoltathatóság fokozásának is eszköze (lásd a 7. fejezetet). Végül az adatvédelmi hatóságok számára is eszközként szolgál a szabályok érvényesítéséhez. A jogsértés adatvédelmi hatóságoknak történő bejelentése nyomán az adatkezelő teljes gyakorlatát megvizsgálhatják.

77. Az elektronikus hírközlési adatvédelmi irányelvben található, a biztonság megsértésére vonatkozó konkrét szabályokat a szabályozási háttér parlamenti fázisában, még az elektronikus hírközlési adatvédelmi irányelv elfogadása előtt átfogóan megvitatták. Ebben a vitában a 29. cikk alapján létrehozott munkacsoport és az európai adatvédelmi biztos véleményét, továbbá más érdekelt felek álláspontját is áttekintették. A szabályokban különböző érdekelt felek álláspontja tükröződik. Megjelenik az érdekek egyensúlya: bár a bejelentési kötelezettséget megalapozó kritériumok általában biztosítják az egyének védelmét, ezt anélkül teszik, hogy túlzottan terhes, nem hasznos követelményeket írnának elő.

6.4. *A hozzájárulás megerősítése*

78. Az adatvédelmi irányelv 7. cikke hat jogalapot sorol fel személyes adatok feldolgozására. A személy hozzájárulása az egyik ezek közül. Az adatkezelő olyan mértékig dolgozhat fel személyes adatokat, amennyire az egyének tájékoztatáson alapuló beleegyezésüket adták ahhoz, hogy adataikat összegyűjtsék és feldolgozzák.

79. A gyakorlatban a felhasználók gyakran csak korlátozott ellenőrzéssel rendelkeznek adataik felett, különösen technológiai környezetekben. Az egyik olykor használt módszer a hallgatólagos hozzájárulás; ez olyan hozzájárulást jelent, amelynek megléte feltételezésen alapul. A hozzájárulás kikövetkeztethető az egyén cselekvéséből (pl. ha a cselekvés egy weboldal használatában áll, ez hozzájárulásnak minősül a felhasználó adatainak

([38]) Lásd a közleményt, 6. o.

marketing célokra történő naplózásába). Kikövetkeztethető továbbá hallgatásból vagy a cselekvés elmulasztásából is (ha valaki egy kattintással nem oldja fel a kockába tett pipát, az hozzájárulásnak minősül).

80. Az irányelv szerint ahhoz, hogy a hozzájárulás érvényes legyen, tájékoztatáson kell alapulnia, önkéntesnek és kifejezettnek kell lennie. A hozzájárulásnak az érintett kívánsága tájékozott kinyilvánításának kell lennie, amellyel beleegyezését adja az őt érintő személyes adatok feldolgozásához. A hozzájárulást egyértelműen kell megadni.

81. Az a hozzájárulás, amelyre cselekvésből, főképpen pedig hallatásból vagy a cselekvés elmulasztásából következtettek, sokszor nem jelent egyértelmű beleegyezést. Nem mindig egyértelmű azonban, mi számít valódi, kétséget kizáró hozzájárulásnak. Néhány adatkezelő ezt a bizonytalanságot használja ki, amikor olyan módszerekre épít, amelyekkel nem nyerhető valódi, egyértelmű hozzájárulás.

82. A fentiekre figyelemmel az európai adatvédelmi biztos támogatja az Európai Bizottság azon törekvését, hogy pontosítani kell a hozzájárulás korlátait és biztosítani kell, hogy csak a szoros értelemben vett hozzájárulás minősül egyértelmű beleegyezésnek. Ezzel kapcsolatban az európai adatvédelmi biztos a következőket javasolja ([39]):

— Azon helyzetek szélesebb értelmezésének mérlegelése, ahol kifejezett hozzájárulás szükséges; jelenleg ez az érzékeny adatok körére korlátozódik.

— Kiegészítő szabályok elfogadása az online környezetben adott hozzájárulásra vonatkozóan.

— Kiegészítő szabályok elfogadása a másodlagos célokra történő adatfeldolgozáshoz való hozzájárulás tekintetében (azaz amikor az adatfeldolgozás a fő feldolgozáshoz képest másodlagos vagy nem nyilvánvaló).

— A szükséges hozzájárulás típusának meghatározása – például a fogyasztói termékeken lévő rádiófrekvenciás azonosító címkékből történő adatfeldolgozással vagy más speciális technikákkal kapcsolatos hozzájárulás szintjének megjelölése – a kiegészítő jogalkotási aktusban, függetlenül attól, hogy az Európai Bizottság az EUMSZ 290. cikke alapján elfogadta-e azt vagy sem.

6.5. *Adathordozhatóság és a személyes adatok tárolásának megszüntetéséhez való jog*

83. Az adathordozhatóság és a személyes adatok tárolásának megszüntetéséhez való jog („right to be forgotten") két egymáshoz kapcsolódó fogalom, amelyet a közlemény felvet az érintettek jogainak erősítése érdekében. Kiegészítik az irányelvben már említett elveket, jogot biztosítanak az érintettnek arra, hogy kifogásolja személyes adatainak további feldolgozását, és arra kötelezik az adatkezelőt, hogy törölje az információkat, amint azok az adatfeldolgozáshoz már nem szükségesek.

84. Ez a két új fogalom főként az információs társadalommal összefüggésben jelent hozzáadott értéket, ahol egyre több adatot tárolnak automatikusan és őriznek határozatlan ideig. A gyakorlat azt mutatja, hogy még akkor is, ha az adatokat maga az érintett tölti fel, az adott személy által a saját személyes adatai felett gyakorolt ellenőrzés foka igen korlátozott. Ez annál inkább igaz arra a hatalmas memóriára tekintettel, amit ma az internet képvisel. Ezenkívül gazdasági szempontból az adatok törlése sokkal költségesebb az adatkezelő számára, mint azok további tárolása. Az egyén jogainak gyakorlása tehát ellenkezik a természetes gazdasági trenddel.

85. Mind az adathordozhatóság, mind pedig a személyes adatok tárolásának megszüntetéséhez való jog hozzájárulhat az egyensúly elmozdításához az érintett javára. Az adathordozhatóság célja az lenne, hogy az egyén számára nagyobb ellenőrzést biztosítsanak az adatai felett, a személyes adatok tárolásának megszüntetéséhez való jog pedig azt biztosítaná, hogy bizonyos idő után az információ automatikusan eltűnik még akkor is, ha az érintett semmit nem tesz vagy nem is tud arról, hogy adatait valaha is tárolták.

86. Konkrétabban, az adathordozhatóság a felhasználók azon képessége, hogy megváltoztassák az adataik feldolgozásával kapcsolatos preferenciájukat, különösen új technológiai szolgáltatásokkal kapcsolatban. Ez mindinkább vonatkozik azokra a szolgáltatásokra, amelyek információk – köztük személyes adatok – tárolásával járnak (például mobiltelefon-szolgáltatás), valamint amelyek képeket, elektronikus leveleket és más információkat tárolnak, gyakran számítási felhő szolgáltatások felhasználásával.

87. Az egyéneknek könnyen és szabadon kell tudniuk szolgáltatót váltani, és személyes adataikat egy másik szolgáltatóhoz továbbítani. Az európai adatvédelmi biztos úgy véli, hogy a 95/46/EK irányelvben rögzített meglévő jogok erősíthetők, ha felveszik a szövegbe a hordozhatóság jogát, különösen az információs társadalommal összefüggő szolgáltatások tekintetében, amely abban segíti az egyéneket, hogy a szolgáltatók és más lényeges adatkezelők biztosítsanak számukra hozzáférést személyes adataikhoz, ugyanakkor azt is biztosítsák, hogy a régi szolgáltatók vagy más adatkezelők akkor is töröljék a szóban forgó információkat, ha saját jogszerű céljaikra szeretnék azokat megtartani.

88. Az újonnan kodifikált jog, a személyes adatok tárolásának megszüntetéséhez való jog biztosítaná a személyes adatok törlését vagy további felhasználásuk tiltását anélkül, hogy bármilyen cselekvésre szükség lenne az érintett részéről, azzal a feltétellel viszont, hogy az adatokat már bizonyos ideig tárolták. Más szóval, az adatoknak bizonyos „lejárati idejük" lenne. Ezt az elvet nemzeti bíróságokon zajló ügyekben már megerősítették, illetve speciális ágazatokban

([39]) A 29. cikk alapján létrehozott munkacsoport jelenleg dolgozik a „beleegyezés" fogalmával kapcsolatos vélemény kialakításán. E vélemény nyomán további javaslatok várhatók.

(például rendőrségi akták, bűnügyi nyilvántartások, fegyelmi akták) már alkalmazták: egyes nemzeti jogszabályok alapján a magánszemélyekre vonatkozó információkat – különösen egy meghatározott idő eltelte után – automatikusan törlik, illetve azok további felhasználása vagy terjesztése tiltott anélkül, hogy esetenkénti előzetes elemzésre lenne szükség.

89. Ebben az értelemben a személyes adatok tárolásának megszüntetéséhez való új jogot össze kell kapcsolni az adathordozhatósággal. Ez azzal a hozzáadott értékkel járna, hogy az érintettnek nem kellene lépéseket tennie adatainak töröltetésére vagy követelnie azt, mivel a törlést objektív, automatizált módon kellene elvégezni. Csak igen kivételes körülmények között, ha különleges igény állapítható meg az adatok hosszabb ideig tartó megőrzésére, lehetne jogosult az adatkezelő az adatok megtartására. Ennek megfelelően a személyes adatok tárolásának megszüntetéséhez való jog megfordítja a bizonyítási terhet: a teher az egyénről az adatkezelőre hárul, és a személyes adatok feldolgozásakor alapértelmezés szerint kell biztosítani az adatvédelmi beállításokat.

90. Az európai adatvédelmi biztos úgy véli, hogy a személyes adatok tárolásának megszüntetéséhez való jog különösen hasznos az információs társadalommal összefüggő szolgáltatások tekintetében. Annak a kötelezettségnek, hogy meghatározott idő eltelte után törölni kell az információkat, illetve azok további terjesztése nem megengedett, elsősorban a médiumokban és az interneten van értelme, különösen a közösségi hálózatokban. A végberendezésekkel kapcsolatban hasznos lenne az is, ha a mobil eszközökön vagy számítógépeken tárolt adatokat meghatározott idő eltelte után automatikusan törölnék vagy zárolnák, amikor azok már nincsenek az egyén birtokában. Ebben az értelemben a személyes adatok tárolásának megszüntetéséhez való jog „beépített adatvédelmi kötelezettségként” is értelmezhető.

91. Összegezve, az európai adatvédelmi biztos azon a véleményen van, hogy az adathordozhatóság és a személyes adatok tárolásának megszüntetéséhez való jog hasznos fogalmak. Érdemes lenne beépíteni őket a jogi eszközbe, de talán az elektronikus környezetre korlátozva.

6.6. Gyermekekre vonatkozó személyes adatok feldolgozása

92. A 95/46/EK irányelv szerint nincsenek sajátos szabályok a gyermekek személyes adatainak feldolgozására vonatkozóan. Az irányelv nem ismeri fel, hogy különleges helyzetekben különleges védelmet kell biztosítani a gyermekeknek – sebezhetőségük miatt és amiatt is, hogy ez jogbizonytalanságot okoz, különösen a következő területeken:

— gyermekek adatainak gyűjtése és a gyermekek tájékoztatásának módja az adatgyűjtésről;

— a gyermekek hozzájárulása megszerzésének módja. Mivel nincsenek speciális szabályok arra vonatkozóan, hogy hogyan kell megszerezni a gyermek hozzájárulását, és milyen életkor alatt minősül a személy gyermeknek, ezekkel a témákkal a nemzeti jogszabályok foglalkoznak, vagyis a szabályozás tagállamonként eltérő ([40]);

— a joggyakorlás módja és feltételei, ahogyan a gyermekek vagy jogi képviselőik gyakorolhatják az irányelv alapján fennálló jogaikat.

93. Az európai adatvédelmi biztos úgy véli, hogy a gyermekek speciális érdekei jobb védelemben részesülnének, ha az új jogi eszköz kiegészítő rendelkezéseket tartalmazna külön a gyermekek adatainak gyűjtésére és további feldolgozására vonatkozóan. Ezek a speciális rendelkezések jogbiztonságot is nyújtanának ezen a speciális területen, és az adatkezelők számára is hasznosak lennének, akiknek jelenleg különféle jogi követelményeknek kell megfelelniük.

94. Az európai adatvédelmi biztos javasolja a következő rendelkezések beépítését a jogi eszközbe:

— A tájékoztatás gyermekekre szabásának követelménye, hogy megkönnyítsék a gyermekek számára annak megértését, hogy mit jelent, amikor adatokat gyűjtenek tőlük.

— Más tájékoztatási követelmények gyermekekre szabása – a tájékoztatás megadásának módjára és esetleg a hozzájárulásra vonatkozóan is.

— Speciális rendelkezés, ami védi a gyermekeket a viselkedésalapú hirdetéssel szemben.

— Meg kell erősíteni a célhoz kötöttség elvét a gyermekek adataival kapcsolatban.

— Bizonyos kategóriába tartozó adatokat soha nem szabad gyűjteni gyermekektől.

— Életkori küszöb. A küszöb alatt – általánosan szólva – kizárólag kifejezett és ellenőrizhető szülői beleegyezéssel szabad információt gyűjteni gyermekektől.

— Ha szülői beleegyezés szükséges, meg kellene állapítani szabályokat a gyermek életkorának igazolására, más

([40]) A hozzájárulást általában ahhoz az életkorhoz kötik, amikor a gyermek szerződéses kötelezettséget vállalhat. Ez az az életkor, amikor a gyermekek feltételezhetően már elértek bizonyos fokú érettséget. A spanyol jog például 14 éven aluli gyermekek adatainak gyűjtéséhez előírja a szülői beleegyezés megszerzését. Ezen életkor felett azt vélelmezik, hogy a gyermek képes maga dönteni a hozzájárulásról. Az Egyesült Királyságban az adatvédelmi törvény nem tartalmaz konkrét életkort vagy küszöböt. Az Egyesült Királyság adatvédelmi hatósága azonban úgy értelmezte, hogy a 12 éven felüli gyermekek képesek megadni hozzájárulásukat. Ellenben a 12 éven aluli gyermekek nem tudnak hozzájárulást adni, és személyes adataik megszerzéséhez előbb be kell szerezni az egyik szülő vagy a gyám engedélyét.

szóval arra nézve, hogy honnan tudható, hogy a gyermek kiskorú, és hogyan kell ellenőrizni a szülői beleegyezést. Ez olyan terület, ahol az Európai Unió más országok – például az Amerikai Egyesült Államok – gyakorlatából is meríthet ([41]).

6.7. *Kollektív jogorvoslati mechanizmusok*

95. Az egyének jogai érdemi részének erősítése értelmetlen, ha nem párosul az ilyen jogok érvényesítésére szolgáló hatékony eljárási mechanizmusokkal. Ezzel kapcsolatban az európai adatvédelmi biztos ajánlja kollektív jogorvoslati mechanizmusok bevezetését az uniós jogban az adatvédelmi szabályok megsértésének esetére. Különösen azok a kollektív jogorvoslati mechanizmusok jelenthetnek igen erős eszközt az adatvédelmi szabályok érvényesítése területén, amelyek polgárok csoportjait hatalmazzák fel arra, hogy egyetlen keresetben egyesítsék követeléseiket ([42]). Ezt az újítást az adatvédelmi hatóságok is támogatják a magánélet védelmének jövőjéről szóló munkacsoport-dokumentumban.

96. Kisebb hatású ügyekben nem valószínű, hogy az adatvédelmi szabályok megszegésének sértettjei egyénenként keresetet nyújtanának be az adatkezelők ellen – figyelemmel az ezzel kapcsolatos költségekre, késedelemre, bizonytalanságra, kockázatra és terhekre. Ezek a nehézségek leküzdhetők vagy jelentősen enyhíthetők, ha kollektív jogorvoslati rendszer létezik, amely felhatalmazza a jogsértések sértettjeit, hogy egyéni követeléseiket egyetlen keresetben egyesítsék. Az európai adatvédelmi biztos is minősített szervezetek (például fogyasztói szövetségek vagy közszervezetek) felhatalmazását részesítené előnyben arra, hogy kártérítési pert indítsanak az adatvédelmi jogsértések sértettjei nevében. Ezek a perek nem érintenék az érintett egyéni keresetindítási jogát.

97. A kollektív keresetek nemcsak azért fontosak, mert teljes körű kártalanítást vagy más jogorvoslati fellépést biztosítanak, közvetve az elrettentő funkciót is erősítik. Az ilyen perekben a drága kollektív kártérítés megítélésének kockázata megsokszorozza az adatkezelők arra irányuló törekvéseit, hogy biztosítsák a jogszabályok betartását. Ebből a szempontból egy továbbfejlesztett magánjogi végrehajtási rendszer, amely kollektív jogorvoslati mechanizmusok segítségével valósul meg, kiegészítené az állami érvényesítést.

98. A közlemény ezzel kapcsolatban nem foglal állást. Az európai adatvédelmi biztosnak tudomása van arról, hogy jelenleg európai szinten vita folyik a kollektív fogyasztói jogorvoslat bevezetéséről. Tudatában van továbbá a túlzásokkal kapcsolatos kockázatnak, amelyet ezek a mechanizmusok előidézhetnek, ahogyan az más jogrendszerek tapasztalatai alapján látszik. Ezek a tényezők azonban – álláspontja szerint – nem jelentenek elégséges érvet az említett mechanizmusok adatvédelmi jogba történő bevezetésének elutasításához vagy elhalasztásához – tekintettel a haszonra, amivel járnának ([43]).

7. **A szervezetek/adatkezelők szerepének erősítése**

7.1. *Általános észrevételek*

99. Az európai adatvédelmi biztos azon a véleményen van, hogy az egyének jogainak megerősítésén felül egy modern adatvédelmi jogi aktusnak tartalmaznia kell azokat a szükséges eszközöket, amelyek fokozzák az adatkezelők felelősségét. Konkrétabban, a keretnek tartalmaznia kell ösztönzőket a magán- és állami szektorban működő adatkezelők számára, hogy eljárásaikba proaktív módon illesszenek be adatvédelmi intézkedéseket. Ezek az eszközök elsősorban azért lennének hasznosak, mert – mint korábban említettük – a technológiai fejlesztések jelentős növekedést eredményeztek a személyes adatok gyűjtésében, felhasználásában és további feldolgozásában; ez növeli a magánélet és az egyének személyes adatai védelmével kapcsolatos kockázatokat, amit hatékonyan ellensúlyozni kell. Másodsorban a jelenlegi keretből – néhány jól definiált rendelkezést kivéve (lásd alább) – hiányoznak az ilyen eszközök, és az adatkezelők *reaktív* megközelítést alkalmazhatnak az adatvédelemmel és a magánélet védelmével kapcsolatban, és csak akkor cselekednek, ha probléma merül fel. Ez a megközelítés a statisztikákban is tükröződik, amelyekben a gyenge megfelelőségi gyakorlat és az adatvesztések visszatérő problémaként jelennek meg.

100. Az európai adatvédelmi biztos szerint a meglévő keret a jelenlegi és jövőbeli körülmények között nem elegendő a személyes adatok hatékony védelméhez. Minél nagyobb a kockázat, annál nagyobb szükség van olyan konkrét intézkedések végrehajtására, amelyek gyakorlati szinten védik az információkat, és hatékony védelmet nyújtanak. Amíg ténylegesen végre nem hajtják ezeket a proaktív intézkedéseket, addig a hibák, kellemetlenségek és a gondatlanság minden valószínűség szerint tovább folytatódik, veszélyeztetve az egyének magánéletének védelmét ebben az egyre inkább digitalizálódó társadalomban. Ennek elérése érdekében az európai adatvédelmi biztos a következő intézkedéseket javasolja:

7.2. *Az adatkezelők elszámoltathatóságának megerősítése*

101. Az európai adatvédelmi biztos azt ajánlja, hogy a jogi aktusba illesszenek be egy új rendelkezést, amely megfelelő és hatékony intézkedések végrehajtására kötelezi az adatkezelőket a jogi aktusban foglalt elvek és kötelezettségek életbe léptetése érdekében, valamint arra, hogy kérésre mutassák is be ezeket az intézkedéseket.

([41]) Az Amerikai Egyesült Államokban a gyermekek személyes adatainak online védelméről szóló törvény (COPPA) előírja, hogy a 13 évesnél fiatalabb gyermekeknek szóló kereskedelmi weboldalak vagy online szolgáltatások üzemeltetői kötelesek szülői beleegyezést beszerezni, mielőtt személyes adatokat gyűjtenek, az általános kereskedelmi közönségnek szóló weboldalak üzemeltetői pedig kötelesek aktuálisan meggyőződni arról, hogy egyes meghatározott látogatók gyermekek.

([42]) Lásd még az európai adatvédelmi biztos 2007. július 25-i véleményét az adatvédelmi irányelv jobb végrehajtását célzó munkaprogram nyomon követéséről szóló, az Európai Parlamenthez és a Tanácshoz címzett bizottsági közleményről, (HL C 255., 2007.10.27., 10. o.).

([43]) Egyes nemzeti jogszabályok már előírnak hasonló mechanizmusokat.

102. Az ilyen típusú rendelkezés nem teljesen újdonság. A 95/46/EK irányelv 6. cikkének (2) bekezdése utal az adatminőséggel kapcsolatos elvekre és megemlíti, hogy „az adatkezelő feladata gondoskodni arról, hogy az (1) bekezdés rendelkezései teljesüljenek". Ugyanígy a 17. cikk (1) bekezdése is intézkedések végrehajtására kötelezi az adatkezelőket – technikai és szervezési jellegűekre egyaránt. E rendelkezések hatóköre azonban korlátozott. Az elszámoltathatóságra vonatkozó általános rendelkezés beillesztése arra ösztönözné az adatkezelőket, hogy proaktív intézkedéseket léptessenek életbe az adatvédelmi jogszabályok összes elemének teljesítése érdekében.

103. Az elszámoltathatósággal kapcsolatos rendelkezésnek az lenne a következménye, hogy az adatkezelőknek belső mechanizmusokat és ellenőrzési rendszereket kellene életbe léptetniük, amelyek biztosítanák a jogi keretben foglalt elvek és kötelezettségek betartását. Ez a rendelkezés előírná például az adatvédelmi politikák legmagasabb szintű irányítását, megfeleltetési eljárások bevezetését az összes adatfeldolgozási művelet megfelelő azonosításának biztosítására, kötelező erejű adatvédelmi politikák meglétét, amelyeket folyamatosan felül kell vizsgálni és aktualizálni, hogy az új adatvédelmi műveletekre is vonatkozzanak – az adatminőség, bejelentés, biztonság, hozzáférés, stb. elvének betartásával. Kötelezővé tenné továbbá, hogy az adatkezelők rendelkezzenek olyan bizonyítékokkal, hogy kérésre igazolni tudják a fentiek betartását a hatóságok felé. Egyes esetekben a megfelelőség nyilvánosság felé való igazolását is kötelezővé kell tenni. Ez történhet például úgy, hogy kötelezővé teszik az adatkezelők számára az adatvédelem feltüntetését a nyilvános (éves) jelentésekben, ha ezek a jelentések más jogcímen kötelezőek.

104. A végrehajtandó belső és külső intézkedések típusának nyilván megfelelőnek kell lennie, és mindenkor az adott eset tényállásához és körülményeihez kell igazodnia. Nagy a különbség, ha az adatkezelő csupán nevekből és címekből álló, néhány száz fős ügyfélnyilvántartást dolgoz fel, vagy több millió beteg információit dolgozza fel, kórtörténetüket is beleértve. Ugyanez vonatkozik azokra a speciális módszerekre is, amelyekkel az intézkedések hatékonyságát értékelni kell. Szükséges a méretezhetőség.

105. Az általános átfogó adatvédelmi jogi eszköznek nem kell meghatároznia az elszámoltathatóság konkrét követelményeit, csupán alapvető elemeit. A közlemény előirányoz bizonyos, az adatkezelők felelősségének erősítését célzó elemeket, amelyek nagyon is üdvözlendők. Konkrétabban, az európai adatvédelmi biztos teljes mértékben támogatja, hogy bizonyos küszöbfeltételek mellett tegyék kötelezővé az adatvédelmi tisztviselők kinevezését és a magánélet-védelmi hatásvizsgálatokat.

106. Ezenfelül az európai adatvédelmi biztos ajánlja, hogy az EUMSZ 290. cikke alapján ruházzanak hatásköröket az Európai Bizottságra – az elszámoltathatósági norma teljesítéséhez szükséges alapkövetelmények kiegészítése céljából. E hatáskörök felhasználása fokozná az adatkezelők jogbiztonságát, és harmonizálná a normák betartását az egész Európai Unióban. A fenti speciális jogi aktusok kidolgozása során konzultálni kell a 29. cikk alapján létrehozott munkacsoporttal és az európai adatvédelmi biztossal.

107. Végül az adatkezelők által az elszámoltathatósággal kapcsolatban végrehajtandó konkrét intézkedéseket adatvédelmi hatóságok is előírhatnák végrehajtási hatásköreikben. Ehhez új hatásköröket kell adni az adatvédelmi hatóságoknak, amelyek lehetővé teszik, hogy ezek a hatóságok jogorvoslati intézkedéseket vagy szankciókat rójanak ki. A példák közé fel kell venni belső megfelelési programok létrehozását, a beépített adatvédelem megvalósítását egyes meghatározott termékeken és szolgáltatásokon stb. Jogorvoslatot csak olyan mértékben kell kiszabni, ami megfelelő, arányos és hatékony, hogy biztosítsák az alkalmazandó és kikényszeríthető jogi normáknak való megfelelést.

7.3. *Beépített adatvédelem*

108. A beépített adatvédelem fogalma az adatvédelemnek és a magánélet védelmének beépítése a személyes adatok feldolgozásával járó új termékekbe, szolgáltatásokba és eljárásokba már azok kialakításától kezdve. Az európai adatvédelmi biztos szerint a beépített adatvédelem az elszámoltathatóság egyik eleme. Ennek megfelelően az adatkezelőknek – indokolt esetben – igazolniuk is kell, hogy megvalósították a beépített adatvédelmet. A közelmúltban az adatvédelmi biztosok 32. nemzetközi konferenciája kiadott egy állásfoglalást, amely az alapvető adatvédelem elengedhetetlen alkotóelemének ismeri el a beépített adatvédelmet ([44]).

109. A 95/46/EK irányelv tartalmaz néhány rendelkezést a beépített adatvédelem elősegítésére ([45]), de kifejezetten nem ismeri el azt kötelezettségként. Az európai adatvédelmi biztos örömmel veszi, hogy a közlemény támogatja a beépített adatvédelmet mint az adatvédelmi szabályok betartásának biztosítására szolgáló eszközt. Javasolja egy olyan kötelező érvényű rendelkezés felvételét a

([44]) Állásfoglalás a beépített adatvédelemről, elfogadta az adatvédelmi biztosok 32. nemzetközi konferenciája, Jeruzsálem, 2010. október 27.–29.

([45]) Az irányelv tartalmaz olyan rendelkezéseket, amelyek különböző helyzetekben közvetve megkövetelik a beépített adatvédelem megvalósítását. Különösképpen a 17. cikk előírja, hogy a jogellenes adatfeldolgozás megelőzése érdekében az adatkezelők hajtsanak végre megfelelő technikai és szervezési intézkedéseket. Az elektronikus hírközlési adatvédelmi irányelv ennél nyíltabban fogalmaz. A 14. cikk (3) bekezdése előírja, hogy „Szükség esetén intézkedések fogadhatók el annak biztosítására, hogy a végberendezések konstrukciója olyan legyen, amely az 1999/5/EK irányelvvel, valamint az információtechnológia és a távközlés terén történő szabványosításról szóló, 1986. december 22-i 87/95/EGK tanácsi határozattal összhangban összeegyeztethető a felhasználóknak a személyes adataik védelmére és felhasználása ellenőrzésére vonatkozó jogával."

jogi aktusba, amely „beépített adatvédelmi kötelezettséget" ír elő, és ez a 95/46/EK irányelv (46) preambulumbekezdésének szövegére is épülhet. Konkrétabban, a rendelkezés kifejezetten kötelezné az adatkezelőket technikai és szervezési intézkedések végrehajtására az adatfeldolgozó rendszer megtervezésekor és az adatfeldolgozás időpontjában egyaránt, különösen a személyes adatok védelmének biztosítása és az engedély nélküli adatfeldolgozás megakadályozása érdekében ([46]).

110. Egy ilyen rendelkezés alapján az adatkezelők kötelesek – többek között – biztosítani, hogy az adatfeldolgozó rendszereket úgy tervezik meg, hogy a lehető legkevesebb személyes adatot dolgozzák fel; már alapértelmezés szerint adatvédelmi beállításokat alkalmazni, például közösségi hálózatok esetében; a magánszemélyek profiljait már alapértelmezés szerint másokétól elkülönítve tartani; továbbá olyan eszközöket megvalósítani, amelyek lehetővé teszik, hogy a felhasználók jobban megvédjék személyes adataikat (pl. hozzáférés-ellenőrzések, titkosítás).

111. A beépített adatvédelem kifejezettebb említésének előnyei az alábbiakban összegezhetők:

— Kiemelné önmagában az elv, mint eszköz fontosságát abban a tekintetben, hogy az eljárásokat, termékeket és szolgáltatásokat már kezdetben úgy tervezik, hogy szem előtt tartják az adatvédelmet.

— Csökkentené az adatvédelemmel kapcsolatos visszaélések számát, minimalizálná a felesleges adatgyűjtéseket, és felhatalmazná az egyéneket, hogy valós választás keretében hozzanak döntéseket személyes adataikról.

— Nem lenne szükség utólagos „foldozgatásra" a nehezen vagy egyáltalán nem kezelhető problémák megoldása érdekében.

— Elősegítené, hogy az adatvédelmi hatóságok hatékonyan alkalmazzák és érvényesítsék ezt az elvet.

112. E kötelezettség kombinált hatása azt eredményezné, hogy nagyobb kereslet lenne a beépített adatvédelmet tartalmazó termékek és szolgáltatások iránt, ez viszont tovább ösztönözné az ipart e kereslet kielégítésére. Ezenfelül mérlegelni kell egy külön kötelezettség létrehozását olyan új termékek és szolgáltatások tervezőire és gyártóira vonatkozóan, amelyeknek valószínűsíthetően adat- és magánélet-védelmi kihatása van. Az európai adatvédelmi biztos ajánlja, hogy vegyenek fel a szövegbe ilyen külön kötelezettséget, amely még inkább előmozdíthatná, hogy az adatkezelők tartsák be saját kötelezettségüket.

113. A beépített adatvédelem kodifikálását egy általános „beépített adatvédelmi követelményt" rögzítő rendelkezéssel lehetne kiegészíteni, amely minden szektorra, termékre és szolgáltatásra alkalmazható lenne, mint például a felhasználó felhatalmazására irányuló intézkedések biztosítása, és amelyet az elvnek megfelelően fogadnának el.

([46]) A jelenlegi keretben a (46) preambulumbekezdés bátorítja az adatkezelőket ilyen intézkedések végrehajtására, de egy preambulumbekezdésnek természetesen nincs kötelező ereje.

114. Ezenfelül az európai adatvédelmi biztos ajánlja, hogy az EUMSZ 290. cikke alapján – indokolt esetben – ruházzanak hatásköröket az Európai Bizottságra egyes kiválasztott termékekre és szolgáltatásokra vonatkozóan a beépített adatvédelem alapkövetelményeinek kiegészítése céljából. E hatáskörök felhasználása fokozná az adatkezelők jogbiztonságát, és harmonizálná a normák betartását az egész Európai Unióban. A fenti speciális jogi aktusok kidolgozása során konzultálni kell a 29. cikk alapján létrehozott munkacsoporttal és az európai adatvédelmi biztossal (hasonlóan az elszámoltathatóságról szóló 106. ponthoz).

115. Végül az adatvédelmi hatóságoknak hatáskört kell adni jogorvoslati intézkedések vagy szankciók kiszabására, a 107. pontban már említett korlátozó feltételekhez hasonló feltételekkel, ha az adatkezelők egyértelműen elmulasztottak konkrét lépéseket tenni olyan esetekben, ahol kötelező lett volna.

7.4. *Tanúsítási szolgáltatások*

116. A közlemény elismeri, hogy meg kell vizsgálni annak lehetőségét, hogy a magánélet védelmét tiszteletben tartó termékekre és szolgáltatásokra vonatkozó európai uniós tanúsítási rendszereket hívjon életre. Az európai adatvédelmi biztos teljes mértékben támogatja ezt a célt, és javasolja egy rendelkezés beillesztését a szövegbe az említett rendszerek létrehozásáról és lehetséges hatásáról az Európai Unióban; ez a rendelkezés később egy kiegészítő jogszabályban tovább is fejleszthető. A rendelkezésnek ki kell egészítenie az elszámoltathatósággal és a beépített adatvédelemmel kapcsolatos rendelkezéseket.

117. Az önkéntes tanúsítási rendszerek lehetővé tennék annak ellenőrzését, hogy az adatkezelő életbe léptetett-e intézkedéseket a jogi aktusnak való megfelelés érdekében. Ezenkívül a hitelesítő jelzéssel rendelkező adatkezelők – sőt termékek vagy szolgáltatások – valószínűleg versenyelőnyre tesznek szert másokkal szemben. Az ilyen rendszerek segítenék az adatvédelmi hatóságokat felügyeleti és végrehajtási szerepük ellátásában.

8. **Globalizáció és alkalmazandó jog**

8.1. *Nyilvánvalóan következetesebb védelemre van szükség*

118. Ahogy korábban a 2. fejezetben említésre került, az új technológiák kifejlesztése, a multinacionális vállalatok szerepe, valamint a személyes adatok nemzetközi méretekben történő feldolgozása és megosztása terén a kormányok növekvő befolyása következtében egyre fokozódó ütemben növekszik a személyes adatok továbbítása az Unión kívülre. Ez az egyik ok, amiért indokolt a jelenlegi jogi keret felülvizsgálata. Ezért ez az egyik olyan terület, ahol az európai adatvédelmi biztos ambíciót és hatékonyságot kér, mivel nyilvánvaló szükség van a következetesebb védelemre, amennyiben az adatok feldolgozása az Európai Unión kívül történik.

8.2. *Nemzetközi szabályok alkotására tett erőfeszítések*

119. Az európai adatvédelmi biztos szerint nagyobb erőfeszítések szükségesek a nemzetközi szabályok létrehozására. A személyes adatok védelmének szintje tekintetében a nagyobb harmonizáció világszerte jelentősen tisztázná a betartandó elvek lényegét és az adattovábbítás feltételeit. Ezekre a globális szabályokra azért lenne szükség, hogy egyeztessék a magas szintű adatvédelem követelményét (beleértve a legfontosabb európai uniós adatvédelmi elemeket) a regionális jellemzőkkel.

120. Az európai adatvédelmi biztos támogatja az adatvédelmi biztosok nemzetközi konferenciájának keretében eddig végzett ambiciózus munkát, amely az ún. madridi szabványok kidolgozására és terjesztésére irányult, és célja e szabványoknak egy kötelező erejű jogi aktusba történő integrálása, és lehetőség szerint egy kormányközi konferencia kezdeményezése ([47]). Felhívja az Európai Bizottságot, hogy tegye meg a szükséges kezdeményezéseket annak érdekében, hogy elősegítse e célkitűzés megvalósulását.

121. Az európai adatvédelmi biztos megítélése szerint az is fontos, hogy biztosítsák az összhangot a nemzetközi szabványokkal kapcsolatos fenti kezdeményezés, az uniós adatvédelmi keret jelenlegi felülvizsgálata és más fejlemények között; utóbbira példa az OECD adatvédelmi iránymutatása és az Európa Tanács 108. egyezményének jelenlegi felülvizsgálata, amely egyezmény harmadik országok számára is nyitva áll aláírásra (lásd a 17. pontot). Az európai adatvédelmi biztos úgy véli, hogy itt az Európai Bizottságnak speciális szerepet kell játszania – meg kell határoznia, hogyan segíti elő az összhang megteremtését az OECD-ben és az Európa Tanácsban folytatott tárgyalások során.

8.3. *Az alkalmazandó jogi kritériumok pontosítása*

122. Mivel a teljes konzisztencia nem érhető el könnyen, maradni fog – legalábbis a közeljövőben – némi eltérés az uniós és főként az Európai Unió határain túli jogszabályok között. Az európai adatvédelmi biztos úgy véli, hogy egy új jogi aktusnak pontosítania kell az alkalmazandó jog megállapítására vonatkozó kritériumokat, és egyszerűsített mechanizmusokat kell biztosítania az adatáramlásra, valamint biztosítania kell az adatáramlásban részt vevő szereplők elszámoltathatóságát.

123. Először is a jogi aktusnak biztosítania kell, hogy az uniós jogszabályok legyenek alkalmazandók, amikor a személyes adatok feldolgozása az Európai Unió határain kívül történik, de indokolt az uniós jog alkalmazása. Az EU lakosaira célzott, nem európai számítási felhő alapú szolgáltatások jól szemléltetik, miért van erre szükség. Egy olyan környezetben, ahol az adatokat nem fizikailag tárolják és nem egy meghatározott helyen tartják, ahol a különböző országokban lévő szolgáltatók és felhasználók egymást keresztező befolyással lehetnek az adatok fölött, igen nehezen azonosítható, ki a felelős az adatvédelmi elvek betartásáért. Iránymutatásokat adnak ki – különösen az adatvédelmi hatóságok – arra vonatkozóan, hogy ilyen esetekben hogyan kell értelmezni és alkalmazni a 95/46/EK irányelvet, de az iránymutatás önmagában nem elegendő ahhoz, hogy jogbiztonságot nyújtson ebben az új környezetben.

124. A 29. cikk alapján létrehozott munkacsoport a közelmúltban kiadott véleményében hangsúlyozta, hogy az Európai Unió területén a jogi keret pontosítására, valamint egyszerűsített kritériumra van szükség az alkalmazandó jog meghatározására vonatkozóan ([48]).

125. Az európai adatvédelmi biztos szerint a legjobb megoldás a jogi eszköz rendeletben történő rögzítése lenne, aminek nyomán azonos szabályok vonatkoznának minden tagállamra. A rendelettel az alkalmazandó jog meghatározása bizonyos mértékig elveszíti fontosságát. Ez az egyik ok, amiért az európai adatvédelmi biztos határozottan a rendelet elfogadását pártolja. Egy rendelet is hagy azonban némi mozgásteret a tagállamoknak. Ha jelentősebb mozgástér marad az új jogi eszközben, az európai adatvédelmi biztos támogatná a munkacsoport javaslatát, hogy térjenek át a különböző nemzeti jogszabályok elhatároláson alapuló alkalmazásáról egyetlen jogszabály központi alkalmazására az összes tagállamban, ahol az adatkezelő szervezeti egységekkel rendelkezik. Szót emel továbbá a nagyobb együttműködésért és koordinációért az adatvédelmi hatóságok között transznacionális ügyekben és panaszok esetén (lásd a 10. fejezetet).

8.4. *Az adatáramlási mechanizmusok egyszerűsítése*

126. A következetesség és a magas referenciaszint iránti igényt nemcsak a globális adatvédelmi elvek, hanem a nemzetközi adattovábbítások tekintetében is figyelembe kell venni. Az európai adatvédelmi biztos teljes mértékben támogatja az Európai Bizottság célkitűzését a nemzetközi adattovábbítás jelenlegi eljárásainak egyszerűsítésére, valamint egységesebb és koherensebb megközelítés biztosítására harmadik országokkal és nemzetközi szervezetekkel szemben.

127. Az adattovábbítási mechanizmusba a magánszektorbeli továbbítások – különösen a szerződéses feltételek vagy kötelező erejű vállalati szabályok alapján történő továbbítások – és a hatóságok közötti továbbítások egyaránt beletartoznak. A kötelező erejű vállalati szabályok az egyik olyan elem, ahol koherensebb és egyszerűsítettebb megközelítés lenne kívánatos. Az európai adatvédelmi biztos ajánlja, hogy az új jogi aktusban kifejezetten foglalkozzanak a kötelező erejű vállalati szabályokra vonatkozó feltételekkel ([49]) – a következők szerint:

— a kötelező erejű vállalati szabályok, mint megfelelő garanciákat nyújtó eszközök kifejezett elismerése;

— rendelkezés a kötelező erejű vállalati szabályok elfogadásának főbb elemeiről/feltételeiről;

([47]) Az adatvédelmi biztosok 32. nemzetközi konferenciáján (Jeruzsálem, 2010. október 27.–29.) elfogadott, a nemzetközi szabványokról szóló állásfoglalás javaslata alapján.

([48]) A 29. alapján létrehozott munkacsoport 8/2010. sz. véleménye az alkalmazandó jogról, WP 179.

([49]) A nemzetközi adattovábbításokkal kapcsolatban lásd még a vélemény 8. fejezetét.

— együttműködési eljárások rögzítése a kötelező erejű vállalati szabályok elfogadására vonatkozóan, beleértve egy vezető felügyelő hatóság kiválasztásának kritériumait (egyablakos ügyintézés).

9. **A rendőrség és igazságügy területe**

9.1. *Az általános eszköz*

128. Az Európai Bizottság ismételten kiemelte az adatvédelem erősítésének fontosságát a bűnüldözés és a bűnmegelőzés tekintetében, ahol a személyes adatok kicserélése és felhasználása jelentősen felerősödött. Az Európai Tanács által jóváhagyott Stockholmi Program is említi az erős adatvédelmi rendszert mint az uniós információkezelési stratégia legfontosabb előfeltételét ezen a területen ([50]).

129. Az általános adatvédelmi keret felülvizsgálata tökéletes alkalom arra, hogy előrehaladást érjenek el ezzel kapcsolatban, különösen mivel a közlemény helyesen minősíti a 2008/977/IB kerethatározatot nem megfelelőnek ([51]).

130. Az európai adatvédelmi biztos e vélemény 3.2.5. pontjában érvekkel támasztotta alá, miért kell belefoglalni a rendőrségi és igazságügyi együttműködést az általános jogi eszközbe. A rendőrség és az igazságügy szerepeltetése számos további előnnyel is jár. Azt jelenti, hogy a szabályok már nemcsak a határokon átnyúló adatcserére ([52]), hanem a hazai adatfeldolgozásra is alkalmazandók. Jobban garantálják a megfelelő védelmet a személyes adatok harmadik országokkal folytatott cseréje területén, a nemzetközi megállapodásokra is figyelemmel. Ezenkívül az adatvédelmi hatóságok ugyanazokkal a kiterjedt és harmonizált hatáskörökkel rendelkeznek majd a rendőrséggel és az igazságügyi hatóságokkal, mint más adatkezelőkkel szemben. Végül a jelenlegi 13. cikket, amely a tagállamok azon hatásköréről rendelkezik, hogy konkrét jogszabályokat fogadhatnak el az általános jogi eszközben foglalt jogok és kötelezettségek közérdekből való korlátozása tárgyában, ugyanolyan korlátozó módon kell alkalmazni, mint más területeken. Az általános eszközben meghatározott, ezen a területen érvényes konkrét garanciákat különösen tiszteletben kell tartani a rendőrségi és igazságügyi együttműködés területén elfogadott nemzeti jogszabályokban is.

9.2. *Konkrét kiegészítő szabályok a rendőrségre és az igazságügyre vonatkozóan*

131. A fenti rendelkezés beillesztése azonban nem zárja ki azokat a speciális szabályokat és eltéréseket, amelyek kellően figyelembe veszik az ágazat jellemzőit, összhangban a Lisszaboni Szerződéshez csatolt 21. nyilatkozattal. Előírhatók korlátozások az érintettek jogaival kapcsolatban, de ezeknek szükségesnek és arányosnak kell lenniük, és magának a jognak az alapvető elemeit nem módosíthatják. Ezzel kapcsolatban hangsúlyozni kell, hogy a 95/46/EK irányelv – beleértve 13. cikkét – jelenleg különféle olyan területeken (pl. adózás, vámügy, csalás elleni fellépés) alkalmazandó a bűnüldözésre, amelyek alapvetően nem különböznek a rendőrség és igazságügy területének számos tevékenységétől.

132. Ezenkívül konkrét garanciákat is életbe kell léptetni annak érdekében, hogy kiegészítő védelem nyújtásával kárpótolják az érintettet egy olyan területen, ahol a személyes adatok feldolgozása tolakodóbb jellegű lehet.

133. A fentiekre figyelemmel, az európai adatvédelmi biztos úgy véli, hogy az új keretnek legalább a következő elemeket tartalmaznia kell, összhangban a 108. egyezménnyel és az R (87) 15. sz. ajánlással:

— különböző adat- és adatállomány-kategóriák megkülönböztetése pontosságuk és megbízhatóságuk szerint, elfogadva azt az elvet, hogy a tényeken alapuló adatokat meg kell különböztetni a véleményen vagy személyes értékelésen alapuló adatoktól.

— Az érintettek (gyanúsítottak, áldozatok, tanúk, stb.) és adatállományok (átmeneti, állandó és információs) különböző kategóriáinak megkülönböztetése. Egyedi feltételeket és garanciákat kell előírni a nem gyanúsítottak adatainak feldolgozására vonatkozóan.

— Rendszeres ellenőrzés és helyesbítés biztosítására irányuló mechanizmusok, amelyek célja a feldolgozás alatt álló adatok minőségének biztosítása.

— Egyedi rendelkezéseket és/vagy garanciákat lehet kidolgozni a (növekvő fontosságú) biometrikus és genetikai adatok feldolgozásával összefüggésben a bűnüldözés területén. Felhasználásukat kizárólag azokra az esetekre kell korlátozni, amikor nem áll rendelkezésre más, kevésbé beavatkozó jellegű eszköz, amellyel ugyanaz a hatás elérhető lenne ([53]).

— A személyes adatok nem illetékes hatóságoknak és magánfeleknek történő továbbítására, valamint magánfelek által gyűjtött személyes adatok bűnüldöző hatóságok általi hozzáférésére és további felhasználására vonatkozó feltételek.

([50]) Ezzel kapcsolatban lásd az európai adatvédelmi biztos 2010. szeptember 30-i véleményét a szabadságon, a biztonságon és a jog érvényesülésén alapuló térségben folytatott információkezelés áttekintéséről szóló, az Európai Parlamenthez és a Tanácshoz intézett bizottsági közleményről; 9–19. pont.

([51]) Lásd a fenti 3.2.5. pontot.

([52]) Jelenleg ez a 2008/977/IB kerethatározat korlátozott hatálya.

([53]) Ezzel kapcsolatban lásd a magánélet védelmének jövőjéről című munkacsoport-dokumentum 112. pontját.

9.3. *Ágazatspecifikus adatvédelmi rendszerek*

134. A közlemény kimondja, hogy „a kerethatározat nem helyettesítheti a büntetőügyekben folytatott rendőrségi és igazságügyi együttműködésre vonatkozó, uniós szinten elfogadott különféle ágazatspecifikus jogi aktusokat, kiváltképpen azokat, amelyek az Europol, az Eurojust, a Schengeni Információs Rendszer (SIS), és a váminformációs rendszer (VIR) működését szabályozzák. Az említett jogszabályok saját adatvédelmi szabályozást tartalmaznak és/vagy rendszeresen hivatkoznak az Európa Tanács adatvédelmi jogi aktusaira".

135. Az európai adatvédelmi biztos álláspontja szerint az új jogi keretnek a lehető legnagyobb mértékig egyértelműnek, egyszerűnek és következetesnek kell lennie. Ha elterjed, hogy különböző rendszerek alkalmazandók például az Europolra, az Eurojustra, a SIS-re és a Prümre, a szabályok betartása továbbra is bonyolult marad, vagy még bonyolultabbá válik. Ez az egyik ok, amiért az európai adatvédelmi biztos egy minden ágazatra alkalmazandó, átfogó jogi eszközt pártol.

136. Az európai adatvédelmi biztos azonban megérti, hogy a különböző rendszerekből származó szabályok összehangolása jelentős munkát igényel, amit gondosan kell elvégezni. Az európai adatvédelmi biztos úgy véli, hogy a közleményben is említett fokozatos megközelítésnek van értelme, feltéve, hogy a következetesen és hatékonyan biztosított magas szintű adatvédelem iránti elkötelezettség egyértelmű és nyilvánvaló marad. Konkrétabban:

— Első lépésben az általános adatvédelmi jogi eszköznek alkalmazandónak kell lennie az összes adatfeldolgozásra a rendőrségi és igazságügyi együttműködés területén, beleértve a rendőrség és az igazságügy tekintetében elvégzett módosításokat is (lásd a 9.2. pontot).

— A második lépésben az ágazatspecifikus adatvédelmi rendszereket össze kell hangolni ezzel az általános eszközzel. Az Európai Bizottságnak kötelezettséget kell vállalnia arra, hogy meghatározott – és rövid – időn belül javaslatokat fogad el ehhez a második lépéshez.

10. **Az adatvédelmi hatóságok és együttműködés az adatvédelmi hatóságok között**

10.1. *Az adatvédelmi hatóságok szerepének megerősítése*

137. Az európai adatvédelmi biztos teljes mértékben támogatja az Európai Bizottság azon célkitűzését, hogy az adatvédelmi hatóságok jogállásának kérdésével foglalkozni kell, sőt konkrétabban: erősíteni kell azok függetlenségét, erőforrásait és végrehajtási hatáskörét.

138. Az európai adatvédelmi biztos sürgeti továbbá, hogy pontosítsák az új jogi eszközben az adatvédelmi hatóságok függetlenségének alapfogalmát. Az Európai Bíróság a közelmúltban hozott határozatot erről a kérdésről a C-518/07. sz. ügyben ([54]), amelyben hangsúlyozta, hogy a függetlenség mindenfajta külső befolyástól való mentességet jelent. Az adatvédelmi hatóság senkitől nem kérhet és nem fogadhat el utasítást. Az európai adatvédelmi biztos javasolja, hogy kifejezetten nevesítsék a függetlenség ezen elemeit a jogszabályban.

139. Az adatvédelmi hatóságoknak elégséges emberi és pénzügyi erőforrást kell biztosítani feladataik elvégzéséhez. Az európai adatvédelmi biztos javasolja, hogy foglalják bele ezt a követelményt a jogszabályba. ([55]) Végül kiemeli, hogy biztosítani kell, hogy a hatóságoknak teljes körűen harmonizált hatáskörük legyen a vizsgálódásra, valamint eléggé elrettentő és korrekciós intézkedések és szankciók kiszabására. Ez az érintettek és az adatkezelők számára egyaránt fokozná a jogbiztonságot.

140. Az adatvédelmi hatóságok függetlenségének, erőforrásainak és hatáskörének együtt kell járnia a multilaterális szintű fokozott együttműködéssel, különös tekintettel az adatvédelmi kérdések növekvő számára Európa-szerte. Az együttműködéshez felhasználható elsődleges infrastruktúra nyilvánvalóan a 29. cikk alapján létrehozott munkacsoport.

10.2. *A munkacsoport szerepének erősítése*

141. A munkacsoport történetének tanúsága szerint a csoport működése az 1997-es indulástól kezdve a mai napig fejlődik. Működése során a csoport egyre nagyobb függetlenségre tett szert, így gyakorlatilag többé már nevezhető az Európai Bizottság egyszerű tanácsadó munkacsoportjának. Az európai adatvédelmi biztos további előrelépéseket javasol a munkacsoport működése tekintetében, beleértve a csoport infrastruktúráját és függetlenségét.

142. Az európai adatvédelmi biztos úgy véli, a csoport erőssége valójában függetlenségével és tagjainak hatáskörével függ össze. A munkacsoport autonómiáját biztosítani kell az új jogi keretben, összhangban az adatvédelmi hatóságok teljes függetlenségére kidolgozott, az Európai Bíróság által a C-518/07. sz. ügyben megállapított kritériumokkal. Az európai adatvédelmi biztos megítélése szerint elegendő erőforrást és költségvetést, valamint megerősített titkárságot is biztosítani kell a munkacsoport részére, hozzájárulásának támogatása céljából.

143. A munkacsoport titkárságával kapcsolatban az európai adatvédelmi biztos nagy fontosságot tulajdonít annak, hogy a titkárság a Jogérvényesülési Főigazgatóság Adatvédelmi Osztályához tartozik, aminek megvan az az előnye, hogy a munkacsoportnak hasznára lehetnek a hatékony és rugalmas kapcsolatok, valamint az adatvédelmi fejlemények kapcsolatos naprakész információk. Másrészről vitatja a tényt, miszerint az Európai Bizottság (konkrétabban az Osztály) tagja a munkacsoportnak, a titkárságot is ő adja, és ugyanakkor ő a munkacsoport véleményeinek címzettje is egyben. Ez indokolná a titkárság nagyobb függetlenségét. Az európai adatvédelmi biztos arra bátorítja az Európai Bizottságot, hogy az érdekelt felekkel konzultálva mérje fel, hogyan lehetne a legjobban biztosítani ezt a függetlenséget.

([54]) A C-518/07. sz. ügy, *Európai Bizottság* kontra *Németország*, még nem tették közzé az EBHT-ben.

([55]) Lásd például a 45/2001/EK rendelet 43. cikkének (2) bekezdését, amely tartalmazza ezt a követelményt az európai adatvédelmi biztos tekintetében.

144. Végül az adatvédelmi hatóságok hatáskörének megerősítéséhez a munkacsoport erősebb hatásköre is szükséges – jobb szabályokat és garanciákat, valamint nagyobb átláthatóságot biztosító struktúrával együtt. Ezt a munkacsoport tanácsadó és végrehajtó szerepe érdekében kell kidolgozni.

10.3. *A munkacsoport tanácsadó szerepe*

145. A munkacsoport álláspontjait – az Európai Bizottság felé betöltött tanácsadó szerepével kapcsolatban – hatékonyan kell végrehajtani, különösen az irányelv és más adatvédelmi eszközök elveinek értelmezése és alkalmazása tekintetében, más szóval biztosítani kell a munkacsoport álláspontjainak irányadó jellegét. További vitára van szükség az adatvédelmi hatóságok között, hogy megállapítsák, hogyan foglalják ezt bele a jogi eszközbe.

146. Az európai adatvédelmi biztos olyan megoldásokat ajánl, amelyek a munkacsoport véleményeit még inkább irányadóvá tennék anélkül, hogy alapjaiban megváltoztatnák a munkacsoport működésének módját. Az európai adatvédelmi biztos javasolja, hogy a szövegben írjanak elő kötelezettséget az adatvédelmi hatóságok és az Európai Bizottság számára, hogy vegyék kellően figyelembe a munkacsoport által elfogadott véleményeket és közös álláspontokat, az Európai Elektronikus Hírközlési Szabályozók Testületének (BEREC) álláspontjaira vonatkozóan elfogadott modell alapján ([56]). Ezenkívül az új jogi eszköz azt a kifejezett feladatot adhatná a munkacsoportnak, hogy fogadjon el „értelmező ajánlásokat". Ezek az alternatív megoldások erősebb szerepet biztosíthatnának a munkacsoport ajánlásainak – a bíróság előtt is.

10.4. *Összehangolt érvényesítés a munkacsoport részéről*

147. A jelenlegi keret szerint az adatvédelmi jogszabályok érvényesítése a tagállamokban 27 adatvédelmi hatóságra marad, amelyek konkrét esetek kezelésében kevéssé vannak összehangolva egymással. Amikor egynél több tagállamot érintő vagy egyértelműen globális ügyről van szó, ez megsokszorozza a költségeket a vállalkozások számára, amelyek ugyanazon tevékenység kapcsán különböző hatóságokhoz kénytelenek fordulni, és ez fokozza az egymásnak ellentmondó alkalmazás kockázatát: kivételes esetekben előfordulhat, hogy ugyanazt az adatfeldolgozási tevékenységet az egyik adatvédelmi hatóság jogszerűnek minősíti, míg egy másik tiltja.

148. Egyes eseteknek stratégiai dimenziója van, amit központilag kell megközelíteni. A 29. cikk alapján létrehozott munkacsoport elősegíti a koordinációs és végrehajtási intézkedéseket az adatvédelmi hatóságok között ([57]) a nemzetközi horderejű főbb adatvédelmi kérdésekben. A közösségi hálózatokkal és a keresőmotorokkal ([58]), valamint a távközlési és egészségbiztosítási kérdések különböző tagállamokban végzett összehangolt ellenőrzésével kapcsolatban is ez volt a helyzet.

149. A jelenlegi keret szerint azonban a munkacsoport által vállalható végrehajtási intézkedéseknek korlátai vannak. A munkacsoport hozhat közös álláspontokat, de nincs olyan eszköz, amely biztosítaná, hogy ezeket az állásfoglalásokat a gyakorlatban hatékonyan végrehajtják.

150. Az európai adatvédelmi biztos javasolja olyan kiegészítő rendelkezések belefoglalását a jogi eszközbe, amelyek támogathatják az összehangolt érvényesítést, konkrétan:

— Kötelezettség annak biztosítására, hogy az adatvédelmi hatóságok és az Európai Bizottság kellően figyelembe veszik a 29. cikk alapján létrehozott munkacsoport által elfogadott véleményeket és közös álláspontokat ([59]).

— Kötelezettség az adatvédelmi hatóságok számára, hogy megbízhatóan működjenek együtt egymással és az Európai Bizottsággal, valamint a 29. cikk alapján létrehozott munkacsoporttal. ([60]) A megbízható együttműködés gyakorlati szemléltetése céljából létre lehetne hozni egy eljárást, amelynek keretében az adatvédelmi hatóságok tájékoztatnák az Európai Bizottságot vagy a munkacsoportot a határokon átnyúló elemet tartalmazó nemzeti végrehajtási intézkedésekről – a jelenlegi keretben a nemzeti megfelelőségi határozatokra alkalmazandó eljárás mintájára.

— A szavazásra vonatkozó szabályok megállapítása annak érdekében, hogy növeljék az adatvédelmi hatóságok elkötelezettségét a munkacsoport határozatainak végrehajtása iránt. Úgy lehetne rendelkezni, hogy a munkacsoport irányozzon elő konszenzusos döntést, és amennyiben konszenzus nem érhető el, a

([56]) Az Európai Elektronikus Hírközlési Szabályozók Testületének (BEREC) és Hivatalának létrehozásáról szóló, 2009. november 25-i 1211/2009/EK európai parlamenti és tanácsi rendelet, (HL L 337., 2009.12.18., 1. o.).

([57]) A 29. cikk alapján létrehozott munkacsoporton kívül az adatvédelmi biztosok európai konferenciája mintegy tíz évvel ezelőtt állandó munkaértekezletet hozott létre, amelynek célja a határokon átnyúló panaszok összehangolt kezelése. Bár ez a munkaértekezlet tagadhatatlanul hozzáadott értéket jelent az adatvédelmi hatóságok személyzete közötti adatcsere tekintetében, és a kapcsolattartó pontok megbízható hálózatát nyújtja, nem tekinthető koordinációs mechanizmusnak a döntéshozatal tekintetében.

([58]) Lásd a 29. cikk alapján létrehozott munkacsoport 2010. május 12-én és 2010. május 26-án kelt leveleit, amelyeket a 29. cikk alapján létrehozott munkacsoport honlapján tettek közzé (http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010-others_en.htm).

([59]) A fent említettek szerint az 1211/2009/EK rendelet is hasonló kötelezettséget tartalmaz, amely meghatározza az Európai Elektronikus Hírközlési Szabályozók Testülete (BEREC) szerepét.

([60]) Ezzel kapcsolatban lásd az 1211/2009/EK rendelet fent idézett 3. cikkét.

munkacsoport kizárólag minősített többséggel érvényesítse az intézkedéseket. Ezenkívül az egyik preambulumbekezdés előirányozhatná, hogy azoknak az adatvédelmi hatóságoknak, amelyek igennel szavaznak egy dokumentumra, kötelezettsége vagy politikai elkötelezettsége keletkezik az adott dokumentum nemzeti szintű végrehajtására.

151. Az európai adatvédelmi biztos óvást emelne erősebb intézkedések bevezetése ellen; ilyen például a 29. cikk alapján létrehozott munkacsoport álláspontjainak kötelező erejűvé tétele. Ez aláásná az egyes adatvédelmi hatóságok függetlenségét, amit a tagállamoknak garantálniuk kell nemzeti jogszabályaikban. Ha a munkacsoport döntéseinek közvetlen hatása van harmadik felekre, például adatkezelőkre, új eljárásokat kell előirányozni, beleértve az olyan garanciákat, mint az átláthatóság és a jogorvoslat, köztük az Európai Bíróságra történő esetleges fellebbezés.

10.5. *Az európai adatvédelmi biztos és a munkacsoport közötti együttműködés*

152. Az európai adatvédelmi biztos és a munkacsoport együttműködésének módját is finomítani lehetne. Az európai adatvédelmi biztos a munkacsoport tagja, és a csoporton belül hozzájárul a legfőbb stratégiai uniós fejlesztésekkel kapcsolatos álláspontokhoz, ugyanakkor biztosítja az összhangot a saját álláspontjaival. Az európai adatvédelmi biztos megjegyzi, hogy az adatvédelmi kérdések száma a magán- és az állami szektorban egyaránt egyre nő, aminek számos tagállamban nemzeti szinten is kihatása van, és ebben a tekintetben a munkacsoport speciális szerepet játszik.

153. Az európai adatvédelmi biztosnak van egy kiegészítő szerepe, nevezetesen a tanácsadás az Európai Unióval összefüggő fejlesztésekkel kapcsolatban, amit fenn kell tartani. Európai szervként az adatvédelmi biztos ugyanúgy gyakorolja tanácsadó hatáskörét az uniós intézmények felé, mint ahogyan a nemzeti adatvédelmi hatóságok nyújtanak tanácsadást kormányuknak.

154. Az európai adatvédelmi biztos és a munkacsoport különböző, de egymást kiegészítő perspektívából jár el. Ezért szükséges a munkacsoport és az európai adatvédelmi biztos közötti koordináció fenntartása és esetleges javítása annak érdekében, hogy együtt dolgozzanak a fő adatvédelmi kérdéseken, például a menetrendek rendszeres összehangolásával ([61]), valamint átláthatóság biztosításával olyan kérdésekben, amelyeknek inkább nemzeti vagy speciális európai uniós vonatkozása van.

155. Ez az irányelv nem említi a koordinációt azon egyszerű oknál fogva, hogy az európai adatvédelmi biztos tisztsége az irányelv elfogadásakor még nem létezett, de hatévi működés után az európai adatvédelmi biztos és a munkacsoport egymást kiegészítő vonatkozásai nyilvánvalóak és hivatalosan is elismerhetők lehetnének. Az európai adatvédelmi biztos emlékeztet arra, hogy a 45/2001/EK rendelet értelmében együtt kell működnie a nemzeti adatvédelmi hatóságokkal, és részt kell vennie a munkacsoport tevékenységeiben. Az európai adatvédelmi biztos ajánlja az együttműködés kifejezett említését az új jogi eszközben, továbbá annak strukturálását szükség esetén, például együttműködési eljárás megállapításával.

10.6. *Az európai adatvédelmi biztos és az adatvédelmi hatóságok közötti együttműködés az uniós rendszerek felügyeletével kapcsolatban*

156. Ezek a megfontolások azokra a területekre is érvényesek, ahol a felügyeletet össze kell hangolni az európai és a nemzeti szint között. Ez a helyzet azon uniós szervek esetében, amelyek nemzeti hatóságoktól származó jelentős mennyiségű adatot dolgoznak fel, illetve az európai és nemzeti elemet egyaránt tartalmazó nagyléptékű információs rendszerek esetében.

157. A néhány uniós szerv és nagyléptékű információs rendszerek tekintetében fennálló jelenlegi rendszer – például az Europol, az Eurojust és az első generációs Schengeni Információs Rendszer (SIS) közös ellenőrző hatóságokkal rendelkezik, amelyeket a nemzeti adatvédelmi hatóságok képviselői alkotnak – a Lisszaboni Szerződés előtti korszakban létezett kormányközi együttműködés maradványa, és nem tartja tiszteletben az EU intézményi struktúráját, amelynek az Europol és az Eurojust most már szerves részét képezi, és amelybe a schengeni vívmányok most már szintén beletartoznak ([62]).

158. A közlemény bejelenti, hogy az Európai Bizottság 2011-ben konzultációt kezd az összes érintett érdekelttel az említett felügyeleti rendszerek felülvizsgálatáról. Az európai adatvédelmi biztos sürgeti az Európai Bizottságot, hogy a lehető legrövidebb időn belül (rövid és meghatározott időn belül, lásd fent) foglaljon állást a felügyeletről jelenleg folyó vitában. Az európai adatvédelmi biztos a következő álláspontot fogja képviselni ebben a vitában:

159. Kiindulópontként garantálni kell, hogy minden felügyeleti szerv megfelel a függetlenség, az erőforrások és a végrehajtó hatáskör nélkülözhetetlen feltételeinek. Ezenfelül biztosítani kell az uniós szinten meglévő perspektívák és szaktudás figyelembevételét. Ez azt jelent, hogy az együttműködésnek nemcsak a nemzeti hatóságok között kell fennállnia, hanem az európai adatvédelmi hatósággal is (azaz jelenleg az európai adatvédelmi biztossal). Az európai adatvédelmi biztos szükségesnek látja egy olyan modell követését, amely megfelel ezeknek a követelményeknek ([63]).

160. Az elmúlt években kidolgozták az „összehangolt felügyelet" modelljét. Ezt a felügyeleti modellt, amely jelenleg az Eurodac-nál működik és része a váminformációs rendszernek, hamarosan a Vízuminformációs Rendszerre és a második generációs Schengeni Információs Rendszerre (SIS II) is kiterjesztik. Ennek a modellnek három rétege van: (1) nemzeti szinten a felügyeletet az adatvédelmi hatóságok biztosítják; (2) uniós szinten a felügyeletet az európai adatvédelmi biztos biztosítja; (3) a koordinációt az európai adatvédelmi

([61]) Pl. az évente közzétett és rendszeresen frissített jogalkotási tevékenységek leltára alapján, amely elérhető az európai adatvédelmi biztos honlapján.

([62]) A 45/2001/EK rendelet értelmében az európai adatvédelmi biztos köteles együttműködni ezekkel a szervekkel.

([63]) Az Eurojust esetében a modellnek figyelembe kell vennie azt is, hogy az adatvédelmi felügyelet tiszteletben tartja a bírói kar függetlenségét, amennyiben az Eurojust büntetőeljárással kapcsolatos adatokat dolgoz fel.

biztos által összehívott rendszeres megbeszélések biztosítják, aki mint a fenti koordinációs mechanizmus titkára jár el. Ez a modell sikeresnek és hatékonynak bizonyult, és a jövőben más információs rendszerek esetében is elő kell irányozni.

C. **HOGYAN KELL JAVÍTANI A JELENLEGI KERET ALKALMAZÁSÁT?**

11. **Rövid távon**

161. Amíg folyik a felülvizsgálati eljárás, az erőfeszítéseket a jelenlegi szabályok teljes körű és hatékony végrehajtására kell fordítani. Ezek a szabályok a jövőbeli keret elfogadásáig és a tagállamok nemzeti jogszabályaiba való beemeléséig alkalmazandók. Ezzel kapcsolatban számos cselekvési irány azonosítható.

162. Először, az Európai Bizottságnak folytatnia kell a 95/46/EK irányelv tagállamok általi betartásának nyomon követését, és szükség esetén használnia kell az EUMSZ 258. cikke alapján fennálló hatáskörét. A közelmúltban jogsértési eljárásokat indítottak az irányelv 28. cikkének nem megfelelő végrehajtása miatt, figyelemmel az adatvédelmi hatóságok függetlenségének követelményére ([64]). Az irányelv teljes körű betartását más területeken is nyomon kell követni és ki kell kényszeríteni ([65]). Az európai adatvédelmi biztos ezért üdvözli és teljes mértékben támogatja az Európai Bizottság közleményben foglalt elkötelezettségét a tevékeny jogsértési politika folytatása iránt. Az Európai Bizottságnak folytatnia kell a strukturális párbeszédet is a tagállamokkal a végrehajtásról ([66]).

163. Másodszor, ösztönözni kell a nemzeti szintű érvényesítést az adatvédelmi szabályok gyakorlati alkalmazásának biztosítása érdekében, az új technológiai jelenségek és a globális szereplők tekintetében is. Az adatvédelmi hatóságoknak teljes körűen használniuk kell vizsgálati és szankcionálási hatáskörüket. Az is fontos, hogy az érintettek meglévő jogai – különösen a hozzáférési jog – teljes mértékben érvényesüljenek a gyakorlatban.

164. Harmadszor, rövid távon szükségesnek látszik a koordináció a szabályok érvényesítése terén. A 29. cikk alapján létrehozott munkacsoport és értelmező dokumentumainak szerepe ebben a tekintetben döntő fontosságú, de az adatvédelmi hatóságoknak is mindent meg kell tenniük e dokumentumok gyakorlati érvényesítése érdekében. Az uniós szintű vagy globális ügyek eltérő kimenetelét el kell kerülni; közös megközelítéseket lehet és kell elérni a munkacsoporton belül. A munkacsoport égisze alatt végzett összehangolt uniós szintű vizsgálatok szintén jelentős hozzáadott értéket eredményezhetnek.

165. Negyedszer, az adatvédelmi elveket proaktívan „be kell építeni" azokba az új előírásokba, amelyeknek közvetlen vagy közvetett hatása lehet az adatvédelemre. Az európai adatvédelmi biztos uniós szinten jelentős erőfeszítéseket tesz arra, hogy hozzájáruljon a jobb európai jogszabályokhoz, és erre nemzeti szinten is törekedni kell. Az adatvédelmi hatóságoknak tehát teljes mértékben használniuk kell tanácsadó hatáskörüket a fenti proaktív megközelítés biztosítása érdekében. Az adatvédelmi hatóságok – az európai adatvédelmi biztost is beleértve – szintén proaktív szerepet játszhatnak a technológiai fejlemények nyomon követésében. A nyomon követés fontos annak érdekében, hogy már korai stádiumban azonosítsák a kialakuló trendeket, kiemeljék a lehetséges adatvédelmi kihatásokat, támogassák az adatvédelem-barát megoldásokat, és fokozzák az érdekelt felek tudatosságát.

166. Végül, aktívan törekedni kell a további együttműködésre a különböző szereplők között nemzetközi szinten. Ezért fontos az együttműködés nemzetközi eszközeinek erősítése. Az olyan kezdeményezések, mint például a madridi szabványok, valamint az Európa Tanácson és az OECD-n belül folyó munka, teljes körű támogatást érdemelnek. Ezzel kapcsolatban nagyon pozitív, hogy az adatvédelmi biztosok nemzetközi konferenciájának keretében az Amerikai Egyesült Államok Szövetségi Kereskedelmi Bizottsága is csatlakozott az adatvédelmi biztosok családjához.

D. **KÖVETKEZTETÉSEK**

ÁLTALÁNOS ÉSZREVÉTELEK

167. Az európai adatvédelmi biztos összességében üdvözli az Európai Bizottság közleményét, mivel meg van győződve arról, hogy szükséges a jelenlegi adatvédelmi jogi keret felülvizsgálata annak érdekében, hogy hatékony védelmet biztosítsanak egy fokozatosan fejlődő és globalizált információs társadalomban.

168. A közlemény megállapítja a fő kérdéseket és kihívásokat. Az európai adatvédelmi biztos osztja az Európai Bizottság nézetét, miszerint a jövőben is szükség lesz erős adatvédelmi rendszerre azon az alapon, hogy az adatvédelem jelenlegi általános elvei továbbra is indokoltak egy olyan társadalomban, amely alapvető változásokon megy át. Az európai adatvédelmi biztos egyetért a közlemény azon állításával, miszerint a kihívások óriásiak, és kiemeli azt a következményt, hogy tervezett megoldásoknak ennek megfelelően ambiciózusnak kell lenniük, és fokozniuk kell a védelem hatékonyságát. Ezért több ponton ambiciózusabb megközelítést kér.

169. Az európai adatvédelmi biztos támogatja az adatvédelem átfogó megközelítését. Sajnálatát fejezi ki azonban amiatt, hogy a közlemény bizonyos területeket – például az uniós intézmények és szervek általi adatfeldolgozást – kizár az általános jogi eszköz hatálya alól. Ha az Európai Bizottság úgy döntene, hogy kihagyja ezeket a területeket, az

([64]) Lásd a fent idézett C-518/07. sz. ügyet és az Európai Bizottság 2010. október 28-i sajtóközleményét (IP/10/1430).

([65]) Az Európai Bizottság különféle adatvédelmi rendelkezések – a viselkedésalapú hirdetésre vonatkozóan az elektronikus kommunikáció bizalmas jellegének követelményét is beleértve – állítólagos megszegése miatt jogsértési eljárást indított az Egyesült Királyság ellen. Lásd az Európai Bizottság 2009. április 9-i sajtóközleményét (IP/09/570).

([66]) Lásd az Európai Bizottság fent idézett első jelentését az adatvédelmi irányelv végrehajtásáról, 22. o. és az azt követő oldalak.

európai adatvédelmi biztos sürgeti, hogy az Európai Bizottság a lehető legrövidebb időn belül, de lehetőség szerint 2011 végéig fogadjon el európai uniós szintű javaslatot.

FŐ PERSPEKTÍVÁK

170. A felülvizsgálati eljárás kiindulópontjai az európai adatvédelmi biztos számára a következők:

— Az adatvédelmi intézkedéseknek a lehető legnagyobb mértékben aktívan támogatniuk kell – nem pedig akadályozniuk – más jogos érdekeket (mint pl. az európai gazdaság, az egyének biztonsága és a kormányok elszámoltathatósága).

— Az adatvédelem általános elveit nem szabad és nem lehet megváltoztatni.

— A további harmonizációnak a felülvizsgálat egyik legfontosabb célkitűzésének kell lennie.

— Az alapvető jogok perspektívájának a felülvizsgálati eljárás középpontjában kell lennie. Egy alapvető jog célja a polgárok védelme minden körülmények között.

— Az új jogi eszközbe bele kell foglalni a rendőrségi és igazságügyi ágazatot.

— Az új jogi eszközt technológiailag a lehető legsemlegesebb módon kell megszövegezni, és az új jogi eszköz céljának a jogbiztonság hosszú távra való megteremtésének kell lennie.

AZ ÚJ KERET ELEMEI

Harmonizáció és egyszerűsítés

171. Az európai adatvédelmi biztos üdvözli az Európai Bizottság elkötelezettségét aziránt, hogy megvizsgálja az adatvédelem további, uniós szintű harmonizációjának módját. Az európai adatvédelmi biztos meghatározza azokat a területeket, ahol a további és jobb harmonizációra sürgős szükség van: fogalom-meghatározások, az adatfeldolgozás indokai, az érintettek jogai, nemzetközi adattovábbítások és adatvédelmi hatóságok.

172. Az európai adatvédelmi biztos javasolja a következő alternatívák mérlegelését az értesítési követelmények egyszerűsítése és/vagy alkalmazási körének korlátozása érdekében:

— Az értesítési kötelezettség korlátozása bizonyos fajta, speciális kockázattal járó adatfeldolgozási műveletekre.

— Egyszerű regisztrációs kötelezettség, amelynek keretében az adatkezelő köteles az adatfeldolgozást nyilvántartásba venni (ellentétben az összes adatfeldolgozási művelet széles körű nyilvántartásba vételével).

— Szabványosított páneurópai bejelentési nyomtatvány bevezetése.

173. Az európai adatvédelmi biztos szerint a rendelet, azaz a tagállamokban közvetlenül alkalmazandó egységes okmány az adatvédelemhez való alapvető jog megvédésének és a további belső piaci konvergencia elérésének leghatékonyabb módja.

Az egyének jogainak erősítése

174. Az európai adatvédelmi biztos támogatja a közleményt, ahol a közlemény az egyének jogainak erősítését javasolja. A következő javaslatokat teszi:

— Az átláthatóság elvét bele lehetne foglalni a jogszabályba. Még fontosabb azonban ennél az átláthatósággal kapcsolatos meglévő rendelkezések – például a 95/46/EK irányelv 10. és 11. cikke – megerősítése.

— Az általános eszközben be kell vezetni egy olyan rendelkezést a személyes adatok megsértése esetén fennálló tájékoztatási kötelezettséggel kapcsolatban, amely a felülvizsgált elektronikus hírközlési adatvédelmi irányelvben egyes szolgáltatókra vonatkozó kötelezettséget az összes adatkezelőre kiterjeszti.

— Pontosítani kell a hozzájárulás korlátait. Mérlegelni kell azon esetek körének szélesítését, ahol kifejezett hozzájárulás szükséges, valamint kiegészítő szabályok elfogadását az online környezetre vonatkozóan.

— Kiegészítő jogokat kell bevezetni, mint például az adathordozhatóság és a személyes adatok tárolásának megszüntetéséhez való jog, különösen az interneten elérhető, az információs társadalommal összefüggő szolgáltatások tekintetében.

— Jobban kell védeni a gyermekek érdekeit. Ehhez számos kiegészítő rendelkezésre van szükség külön a gyermekek adatainak gyűjtésére és további feldolgozására vonatkozóan.

— Az adatvédelmi szabályok megsértése esetére kollektív jogorvoslati mechanizmusokat kell bevezetni az uniós jogszabályokban annak érdekében, hogy felhatalmazzanak minősített szervezeteket egyének csoportjainak nevében történő keresetindításra.

A szervezetek/adatkezelők kötelezettségeinek erősítése

175. A keretnek tartalmaznia kell ösztönzőket az adatkezelők számára, hogy proaktív módon illesszenek be adatvédelmi intézkedéseket eljárásaikba. Az európai adatvédelmi biztos javasolja általános rendelkezések bevezetését az elszámoltathatósággal és a beépített adatvédelemmel kapcsolatban. Az adatvédelmi tanúsítási rendszerekkel kapcsolatban is intézkedés szükséges.

Globalizáció és alkalmazandó jog

176. Az európai adatvédelmi biztos támogatja az adatvédelmi biztosok nemzetközi konferenciájának keretében végzett ambiciózus munkát, amely az ún. madridi szabványok kidolgozására irányult, és célja e szabványoknak egy kötelező erejű jogi aktusba történő integrálása, és lehetőség szerint egy kormányközi konferencia kezdeményezése. Az európai adatvédelmi biztos felhívja a Bizottságot, hogy tegyen konkrét lépéseket ebbe az irányba, együttműködve az OECD-vel és az Európa Tanáccsal.

177. Az új jogi eszköznek pontosítania kell az alkalmazandó jog meghatározására irányadó kritériumokat. Biztosítani kell, hogy az Európai Unió határain kívül feldolgozott adatok ne bújjanak ki az uniós joghatóság alól, ha indokolt az európai uniós jogszabályok alkalmazása. Ha a jogi keret rendelet formáját öltené, azonos szabályok lennének irányadók az összes tagállamban, és kevésbé lenne lényeges az alkalmazandó jog meghatározása (az EU-n belül).

178. Az európai adatvédelmi biztos teljes mértékben támogatja azt a célkitűzést, hogy biztosítsanak egységesebb és koherensebb megközelítést harmadik országokkal és nemzetközi szervezetekkel szemben. A kötelező erejű vállalati szabályokat bele kell foglalni a jogi eszközbe.

A rendőrség és igazságügy területe

179. A rendőrséget és az igazságügyet is magában foglaló átfogó eszköz lehetővé teszi olyan speciális szabályok alkotását, amelyek kellően figyelembe veszik az ágazat jellemzőit, összhangban a Lisszaboni Szerződéshez csatolt 21. nyilatkozattal. Konkrét garanciákat kell életbe léptetni annak érdekében, hogy kiegészítő védelem nyújtásával kárpótolják az érintetteket egy olyan területen, ahol a személyes adatok feldolgozása – természeténél fogva – tolakodóbb jellegű lehet.

180. Az új jogi keretnek a lehető legnagyobb mértékig egyértelműnek, egyszerűnek és következetesnek kell lennie. El kell kerülni annak elterjedését, hogy különböző rendszerek vonatkozzanak például az Europolra, az Eurojustra, a SIS-re és a Prümre. Az európai adatvédelmi biztos megérti, hogy a különböző rendszerekből származó szabályok összehangolását gondosan és fokozatosan kell elvégezni.

Az adatvédelmi hatóságok és együttműködés az adatvédelmi hatóságok között

181. Az európai adatvédelmi biztos teljes mértékben támogatja a Bizottság azon célkitűzését, hogy az adatvédelmi hatóságok jogállásának kérdésével foglalkozni kell, és erősíteni kell azok függetlenségét, erőforrásait és végrehajtási hatáskörét. Ajánlja, hogy:

— alapvető fogalomként kodifikálják az új jogi eszközben az adatvédelmi hatóságok függetlenségét, ahogyan azt az EB meghatározta;

— mondják ki a jogszabályban, hogy elegendő forrást kell biztosítani az adatvédelmi hatóságok számára;

— adjanak harmonizált vizsgálati és szankcionálási hatáskört a hatóságoknak.

182. Az európai adatvédelmi biztos további előrelépéseket javasol a 29. cikk alapján létrehozott munkacsoport működése tekintetében, beleértve a csoport infrastruktúráját és függetlenségét. Elegendő forrást és megerősített titkárságot is biztosítani kell a munkacsoport számára.

183. Az európai adatvédelmi biztos javasolja a munkacsoport tanácsadó szerepének megerősítését olyan módon, hogy állapítsanak meg kötelezettséget az adatvédelmi hatóságok és az Európai Bizottság számára, hogy vegyék kellően figyelembe a munkacsoport által elfogadott véleményeket és közös álláspontokat. Az európai adatvédelmi biztos nem pártolja, hogy kötelező erővel ruházzák fel a munkacsoport álláspontjait – elsősorban az egyes adatvédelmi hatóságok független jogállása miatt. Az európai adatvédelmi biztos ajánlja, hogy az Európai Bizottság vezessen be konkrét intézkedéseket az új jogi eszközben az európai adatvédelmi biztossal való együttműködés fokozására.

184. Az európai adatvédelmi biztos sürgeti, hogy az Európai Bizottság a lehető legrövidebb időn belül foglaljon állást az uniós szervek és nagyléptékű információs rendszerek felügyeletének kérdésében, figyelembe véve, hogy minden felügyelő szervnek meg kell felelnie a függetlenség, elegendő erőforrások és végrehajtási hatáskör elengedhetetlen kritériumainak, továbbá biztosítani kell az uniós perspektíva megfelelő jelenlétét. Az európai adatvédelmi biztos támogatja az „összehangolt felügyelet" modelljét.

Előrelépések a jelenlegi rendszer keretében:

185. Az európai adatvédelmi biztos arra biztatja az Európai Bizottságot, hogy:

— folytassa a 95/46/EK irányelv tagállamok általi betartásának nyomon követését, és szükség esetén használja az EUMSZ 258. cikke alapján fennálló végrehajtási hatáskörét;

— segítse elő a szabályok érvényesítését nemzeti szinten, valamint az érvényesítés összehangolását;

— proaktívan építse be az adatvédelmi elveket azokba az új előírásokba, amelyeknek közvetlen vagy közvetett hatása lehet az adatvédelemre;

— aktívan mozdítsa elő a további együttműködést a különféle szereplők között nemzetközi szinten.

Kelt Brüsszelben, 2011. január 14-én.

Peter HUSTINX

európai adatvédelmi biztos