Az európai adatvédelmi biztos véleménye a szabadságon, a biztonságon és a jog érvényesülésén alapuló, a polgárok szolgálatában álló térségről szóló, a Tanácshoz és az Európai Parlamenthez intézett bizottsági közleményről

(2009/C 276/02)

AZ EURÓPAI ADATVÉDELMI BIZTOS,

tekintettel az Európai Közösséget létrehozó szerződésre, és különösen annak 286. cikkére,

tekintettel az Európai Unió Alapjogi Chartájára, és különösen annak 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,

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, és különösen annak 41. cikkére,

ELFOGADTA A KÖVETKEZŐ VÉLEMÉNYT:

I. BEVEZETÉS

1. A Bizottság 2009. június 10-én elfogadta a szabadságon, a biztonságon és a jog érvényesülésén alapuló, a polgárok szolgálatában álló térségről szóló, a Tanácshoz és az Európai Parlamenthez intézett közleményét ([1]). Az európai adatvédelmi biztos a 45/2001/EK rendelet 41. cikkével összhangban véleményt nyilvánít.

2. A Bizottság a közlemény elfogadását megelőzően, 2009. május 19-i levelében informálisan konzultált arról az európai adatvédelmi biztossal. Az európai adatvédelmi biztos 2009. május 20-án válaszolt erre a levélre, és közölte a közlemény szövegének javítását szolgáló informális észrevételeit. Az európai adatvédelmi biztos emellett aktívan közreműködött a rendőrségi és igazságügyi munkacsoport 2009. január 14-i, a szabadságon, a biztonságon és a jog érvényesülésén alapuló térség többéves programjáról szóló levelében ([2]).

3. A közlemény (1. pontja) hangsúlyozza, hogy az Uniónak „olyan új többéves programra van szüksége, amely – az eddigi előrehaladás alapján és a meglévő hiányosságok tanulságainak levonásával – markáns jövőképet vázol fel. Ennek az új programnak meg kell határoznia a következő öt év prioritásait." Ez a többéves program (más néven a stockholmi program) a tamperei és a hágai program nyomába lép, amelyek erős politikai lendületet adtak a szabadságon, a biztonságon és a jog érvényesülésén alapuló térség számára.

4. A közlemény szándék szerint ezen új többéves programot alapozza meg. Az európai adatvédelmi biztos ezzel kapcsolatban megjegyzi, hogy bár a többéves programok önmagukban nem kötelező erejű eszközök, jelentős hatást gyakorolnak az érintett területen folytatott intézményi politikákra, ugyanis számos konkrét jogalkotási és nem jogalkotási intézkedés a programokból ered.

5. A közleményt ebből a szempontból kell vizsgálni. A közlemény a következő lépése annak a vitának, amely a Tanács elnöksége által ötletek felvetése céljából létrehozott ún. jövő munkacsoport 2008. júniusi alábbi két jelentésével kezdődött: „Szabadság, biztonság, a magánélet védelme – európai belügyek egy nyitott világban" ([3]), valamint „A jövőbeli uniós igazságügyi program tekintetében javasolt megoldások" ([4]).

II. A VÉLEMÉNY FŐBB RÉSZEI

6. Ez a vélemény nemcsak a közleménnyel foglalkozik, hanem az európai adatvédelmi biztos hozzájárulását is tartalmazza a szabadságon, a biztonságon és a jog érvényesülésén alapuló térség jövőjéről folyó szélesebb körű vitához, amelynek az EU svéd elnöksége által bejelentett új stratégiai munkaprogramhoz (a stockholmi program) ([5]) kell vezetnie. Ezenkívül a Lisszaboni Szerződés esetleges hatálybalépésének néhány következményét is tárgyalja.

7. A vélemény III. része a fő szempontokat ismerteti, a IV. rész pedig általánosságban vizsgálja a közleményt.

8. Az V. rész azzal a problémával foglalkozik, hogy a személyes adatok egyre növekvő méretű cseréje mellett hogyan lehet a magánélet és a személyes adatok védelmét folyamatosan biztosítani. Az elemzés középpontjában a közleménynek a személyes adatok és a magánélet védelmével foglalkozó 2.3. pontja áll, továbbá általánosabban az adatvédelem keretét javító további jogalkotási és nem jogalkotási intézkedések szükségessége.

([1]) COM(2009) 262 végleges (a továbbiakban: a közlemény).

([2]) Nem tették közzé. A rendőrségi és igazságügyi munkacsoportot az adatvédelmi biztosok európai konferenciája hozta létre annak érdekében, hogy előkészítse a bűnüldözés területén elfoglalt álláspontjukat és sürgős esetekben eljárjon a nevükben.

([3]) A Tanács 11657/08 sz. dokumentuma (a továbbiakban: a belügyi jelentés).

([4]) A Tanács 11549/08 sz. dokumentuma (a továbbiakban: az igazságügyi jelentés).

([5]) A kormány uniós munkaprogramja, http://www.regeringen.se

9. A VI. rész az információ tárolásának és cseréjének, valamint az információhoz való hozzáférésnek – mint a bűnüldözés, vagy a közlemény szavaival élve „a védelmet nyújtó Európa" eszközei – a szükségességét és lehetőségeit tárgyalja. A közlemény 4. pontja az információáramlással és a technológiai eszközökkel kapcsolatos több célkitűzést tartalmaz, különösen a 4.1.2. pont (Az információk ellenőrzése), a 4.1.3. pont (A szükséges technológiai eszközök mozgósítása) és a 4.2.3.2. pont (Információs rendszerek). A legnagyobb kihívást rejtő javaslatnak ezek között az európai információs modell kidolgozása tekinthető (4.1.2. pont). Az európai adatvédelmi biztos véleményében részletesen elemzi ezt a javaslatot.

10. A VII. rész a szabadságon, a biztonságon és a jog érvényesülésén alapuló térség kérdéskörén belül egy konkrét, adatvédelmi vonatkozású témát érint röviden, nevezetesen az igazságszolgáltatás és az e-igazságszolgáltatás igénybevételének lehetőségét.

III. A VÉLEMÉNY SZEMPONTJAI

11. Ez a vélemény elsődlegesen az alapvető jogok védelmének szükségessége szempontjából elemzi a közleményt, általánosabban pedig a szabadságon, a biztonságon és a jog érvényesülésén alapuló térségnek az új többéves program szerint alakított jövője szempontjából. Emellett az európai adatvédelmi biztos által – főként tanácsadó szerepében – az e területen folytatott uniós politikához nyújtott hozzájárulásokra is épít. Az európai adatvédelmi biztos eddig több mint harminc olyan véleményt és észrevételt fogadott el, amely a hágai programból eredő kezdeményezésekre vonatkozik, és ezek mindegyike megtalálható a weboldalán.

12. A közlemény vizsgálatakor az európai adatvédelmi biztos különösen az alábbi négy, a szabadságon, a biztonságon és a jog érvényesülésén alapuló térséggel kapcsolatos szempontot veszi figyelembe. Mindegyik szempont kulcsfontosságú szerepet kap a közleményben is.

13. Az első szempont az, hogy az információs és kommunikációs technológiák térnyerése következtében rohamosan növekvő mennyiségű digitális információ keletkezik a polgárokról ([6]). A társadalom egy gyakran „megfigyelt társadalomnak" nevezett állapot felé tart, amelyben a polgárok minden ügylete és majdnem minden lépése valószínűleg digitális nyomot hagy maga után. Az RFID-címkék (rádiófrekvenciás azonosítás) használata révén máris gyorsan fejlődik az ún. „tárgyak internete" és a „környezeti intelligencia". Egyre nagyobb mértékben alkalmazzák az emberi test digitalizált jellemzőit (biometria). Mindez oda vezet, hogy a világ egyre jobban összekapcsolódik, és a közbiztonsági szervezetek óriási mennyiségű potenciálisan hasznos információhoz juthatnak hozzá, ami közvetlenül érintheti az érintett személyek életét.

14. A második szempont a nemzetközivé válás. Egyrészt a digitális korban az adatcserét nem korlátozzák az Európai Unió külső határai, másrészt pedig a szabadságon, a biztonságon és a jog érvényesülésén alapuló térségben végzett uniós tevékenységek egész sorában egyre nagyobb az igény a nemzetközi együttműködés iránt: a terrorizmus elleni küzdelem, a rendőrségi és igazságügyi együttműködés, a polgári igazságszolgáltatás és a határellenőrzés csak néhány példa erre.

15. A harmadik szempont az adatok bűnüldözési célú felhasználása: a társadalmat érintő közelmúltbeli fenyegetések – függetlenül attól, hogy a terrorizmushoz kapcsolódtak-e vagy sem – ahhoz (az igényhez) vezettek, hogy a bűnüldöző hatóságok több lehetőséggel rendelkez(ze)nek a személyes adatok gyűjtésére, tárolására és cseréjére. Számos esetben a magánszférához tartozó feleket is aktívan bevonják, ezt mutatják többek között az adatmegőrzési irányelv ([7]) és a PNR-adatokkal kapcsolatos különböző jogi eszközök ([8]).

16. A negyedik szempont a szabad mozgás. A szabadságon, a biztonságon és a jog érvényesülésén alapuló térség fokozatos továbbfejlesztése megköveteli, hogy a belső határokat és a területen belüli szabad mozgás előtt álló esetleges akadályokat szélesebb körben felszámolják. Az e területen elfogadott új eszközöknek semmiképpen sem szabad visszaállítaniuk az akadályokat. A jelen összefüggésben a szabad mozgás jelenti egyrészt a személyek szabad mozgását, másrészt viszont a (személyes) adatok szabad áramlását is.

17. A felsorolt négy szempont azt mutatja, hogy az információ felhasználási környezete gyorsan változik. Ilyen körülmények között nem lehet vitás, hogy szükség van egy olyan erőteljes mechanizmusra, amely védi a polgárok alapvető jogait, különösen pedig a magánéletet és az adatokat. Az európai adatvédelmi biztos – amint azt a 11. pontban is említette – ezért választotta az elemzés fő szempontjának a védelem szükségességét.

([6]) A belügyi jelentés egyenesen „digitális cunamiról" beszél.

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

([8]) Lásd pl. az Európai Unió és az Amerikai Egyesült Államok közötti megállapodást az utas-nyilvántartási adatállomány (PNR) adatainak a légi fuvarozók általi feldolgozásáról és az Egyesült Államok Belbiztonsági Minisztériuma részére történő továbbításáról (2007. évi PNR-megállapodás) (HL L 204., 2007.8.4., 18. o.) és az utas-nyilvántartási adatok (PNR) bűnüldözési célú felhasználásáról szóló tanácsi kerethatározatra irányuló javaslatot, COM(2007) 654 végleges.

IV. ÁLTALÁNOS ELEMZÉS

18. A közlemény és a stockholmi program célja, hogy megállapítsa az elkövetkező öt évre szóló uniós terveket, amelyek hatása esetleg még hosszabb távon is érvényesülhet. Az európai adatvédelmi biztos megállapítja, hogy a közlemény ún. „lisszaboni szempontból semleges" módon készült. Az európai adatvédelmi biztos teljes mértékben megérti, hogy a Bizottság miért választotta ezt a megközelítést, de sajnálja, hogy a közlemény így nem tudta teljesen kihasználni a Lisszaboni Szerződés kínálta további lehetőségeket. Ebben a véleményben nagyobb hangsúlyt kapnak a Lisszaboni Szerződés perspektívái.

19. A közlemény a szabadságon, a biztonságon és a jog érvényesülésén alapuló térségben az elmúlt években végzett uniós tevékenység eredményeire épül. Az eredmények eseményekhez kötődnek, és külön hangsúlyt kapnak a bűnüldöző hatóságok hatáskörét kiterjesztő és a polgárok magánéletébe beavatkozó intézkedések. Magától értetődően ez a helyzet azokon a területeken, ahol széles körben kerül sor a személyes adatok felhasználására és cseréjére, és ezért alapvető szükség van az adatvédelemre. Az eredmények eseményekhez kapcsolódnak, hiszen a külső események, például a szeptember 11-i merénylet, valamint a madridi és londoni robbantások, erőteljes lökést adtak a jogalkotási tevékenységnek. Példaként említhető, hogy az Egyesült Államokba küldött utas-nyilvántartási adatok a szeptember 11-i merénylet következményének tekinthetők ([9]), a londoni robbantások pedig a 2006/24/EK adatmegőrzési irányelvhez ([10]) vezettek. A hangsúly a beavatkozóbb jellegű intézkedéseken volt, mivel az uniós jogalkotó az adatok felhasználását és cseréjét megkönnyítő intézkedésekre összpontosított, míg a személyes adatok védelmét biztosítani hivatott intézkedésekről nem tárgyaltak ilyen sürgősséggel. A legfontosabb védelmi eszköz a büntetőügyekben folytatott rendőrségi és igazságügyi együttműködés keretében feldolgozott személyes adatok védelméről szóló 2008/977/IB tanácsi kerethatározat ([11]) volt, amelyet a Tanács előzőleg három éven keresztül tárgyalt. Az eredmény egy nem teljesen kielégítő tanácsi kerethatározat lett (lásd a 29–30. pontot).

20. Az elmúlt évek tapasztalata azt mutatja, hogy az új eszközök elfogadását megelőzően meg kell vizsgálni, hogy azok milyen következményekkel járhatnak a bűnüldöző hatóságok és az európai polgárok számára. A vizsgálat során kellően figyelembe kell venni, hogy milyen költségek merülnek fel a magánélet védelme szempontjából és milyen hatékonyságot biztosít a bűnüldöző szervek számára, mégpedig először az új eszköz javaslatakor és megvitatásakor, azt követően pedig az eszközök végrehajtása után, rendszeres felülvizsgálat keretében. Ezt a vizsgálatot azt megelőzően is célszerű elvégezni, hogy egy új többéves program alapvető kezdeményezéseket határozna meg a közeljövőre nézve.

21. Az európai adatvédelmi biztos örömmel állapítja meg, hogy a közlemény a szabadságon, a biztonságon és a jog érvényesülésén alapuló térség jövőjének egyik kulcskérdéseként ismeri el az alapvető jogok védelmét, és különösen a személyes adatok védelmét. A közlemény 2. pontja az alapvető jogok védelme szempontjából közös értékeken alapuló, egyedülálló területnek tekinti az Európai Uniót. Szintén fontos, hogy a közlemény kiemelten említi az emberi jogok európai egyezményéhez történő csatlakozást, sőt ez az elsőként tárgyalt prioritás. A csatlakozás lényeges előrelépést jelent az alapvető jogok védelmét biztosító harmonikus és koherens rendszer irányába. Végül, de nem utolsósorban az adatvédelem megkülönböztetett helyet kapott a közleményben.

22. A közlemény középpontjában álló kérdések arra a határozott szándékra utalnak, hogy biztosítsák a polgárok jogainak védelmét, és ezáltal kiegyensúlyozottabb szemléletet kövessenek. A kormányoknak megfelelő eszközökre van szükségük a polgárok biztonságának garantálásához, de az európai társadalmunkban teljes mértékben tiszteletben kell tartaniuk a polgárok alapvető jogait. A polgárok szolgálata ([12]) olyan Európai Uniót követel, amely megőrzi ezt az egyensúlyt.

23. Az európai adatvédelmi biztos véleménye szerint a közlemény kitűnően számításba veszi ezt az egyensúlyi követelményt, beleértve a személyes adatok védelmének szükségességét. Elismeri, hogy máshova kell helyezni a hangsúlyt. Ez lényeges kérdés, ugyanis a szabadságon, a biztonságon és a jog érvényesülésén alapuló térség politikáinak nem szabad a megfigyelt társadalom irányába történő fokozatos elmozdulást támogatniuk. Az európai adatvédelmi biztos elvárja, hogy a Tanács a stockholmi programban ugyanezt a szemléletet kövesse, többek között az alábbi 25. pontban szereplő iránymutatások tudomásulvételével.

24. Ez annál is fontosabb, mivel a szabadságon, a biztonságon és a jog érvényesülésén alapuló térség olyan terület, amely „formálja a polgárok életkörülményeit, különösen a magánéletüket, valamint a politikai és szociális biztonsági körülményeiket, amelyeket az alapvető jogok védenek", amint azt a közelmúltban a német szövetségi bíróság által 2009. június 30-án hozott, a Lisszaboni Szerződéssel kapcsolatos ítélet is hangsúlyozta ([13]).

([9]) Az előző lábjegyzetben említett, 2007. évi PNR-megállapodás és előzményei.

([10]) Az Európai Parlament és Tanács 2006. március 15-i 2006/24/EK irányelve a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtása, illetve a nyilvános hírközlő hálózatok keretében előállított vagy feldolgozott adatok megőrzéséről és a 2002/58/EK irányelv módosításáról (HL L 105., 2006.4.13., 54. o.). Bár a jogalap az EK-Szerződés 95. cikke, az irányelv a londoni robbantásokra való azonnali reakcióként született.

([11]) 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.).

([12]) Lásd a közlemény címét.

([13]) A Németország Szövetségi Alkotmánybírósága által 2009. június 30-án kiadott 72/2009. sz. sajtóközlemény 2c). pontja.

25. Az európai adatvédelmi biztos kiemeli, hogy egy ilyen térségben:

— A tagállamok hatóságai – így adott esetben az európai szervek és adatbázisok – közötti információcserét a polgárok alapvető jogait teljes mértékben tiszteletben tartó és a kölcsönös bizalmat biztosító, megfelelő és hatékony mechanizmusokon keresztül kell lebonyolítani.

— Ez nemcsak az információ rendelkezésre állását követeli meg a tagállamok (és az EU) jogrendszereinek kölcsönös elismerésével párosulva, hanem az információ védelmét szolgáló előírások összehangolását is, például, de nem kizárólag egy közös adatvédelmi keret révén.

— Ezeket a közös előírásokat nem csak a határokon átnyúló helyzetekre kell vonatkoztatni. A kölcsönös bizalom csak akkor létezhet, ha az előírások stabilak és mindig betartják azokat, és nem áll fenn a figyelmen kívül hagyásuk veszélye olyan esetben sem, amikor a határon átnyúló dimenzió nem vagy már nem nyilvánvaló. Emellett, különösen amikor az információ felhasználására kerül sor, a „belföldi" és a „határokon átnyúló" adatok megkülönböztetése a gyakorlatban nem működhet ([14]).

V. AZ ADATVÉDELEM ESZKÖZEI

V.1. Egy átfogó adatvédelmi rendszer felé

26. Az európai adatvédelmi biztos helyesli azt a stratégiai megközelítést, amely szerint az adatvédelem megkülönböztetett helyet kapott a közleményben. A szabadságon, a biztonságon és a jog érvényesülésén alapuló térségben indított számos kezdeményezés a személyes adatok felhasználásán alapul, ezért a megfelelő adatvédelem elengedhetetlen a sikerükhöz. A magánélet tiszteletben tartása és az adatvédelem nemcsak uniós szinten egyre inkább elismert jogi kötelezettség, hanem – az Eurobarométer felmérései szerint ([15]) – az európai polgárok szemében is alapvető kérdés. Emellett a bűnüldöző szervek bizalmának elnyeréséhez is szükség van a személyes adatokhoz való hozzáférés korlátozására.

27. A közlemény 2.3. pontja kijelenti, hogy az uniós hatáskörbe tartozó valamennyi területet lefedő, átfogó adatvédelmi rendszerre van szükség ([16]). Az európai adatvédelmi biztos a Lisszaboni Szerződés hatálybalépésétől függetlenül teljes mértékben támogatja ezt a célkitűzést. Megjegyzi továbbá, hogy egy ilyen rendszer nem feltétlenül jelent egyetlen, mindenféle adatfeldolgozásra alkalmazandó jogi keretet. A jelenleg hatályos szerződések alapján a minden adatfeldolgozásra alkalmazandó, átfogó jogi keret elfogadásának lehetőségei korlátozottak, egyrészt a pilléres szerkezet miatt, másrészt mert – legalábbis az első pillérben – az európai intézmények által feldolgozott adatok védelmére külön-külön jogalap szerint kerül sor (az EKSz. 286. cikke). Az európai adatvédelmi biztos azonban felhívja a figyelmet arra, hogy a hatályos szerződések kínálta lehetőségek teljes mértékű kihasználásával is elérhető bizonyos javulás, amint azt már a Bizottság „A hágai program végrehajtása: további teendők" c. közleményében ([17]) is hangsúlyozta. A Lisszaboni Szerződés hatálybalépését követően az Európai Unió működéséről szóló szerződés (EUMSz.) 16. cikke biztosítja majd a szükséges jogalapot a minden adatfeldolgozásra alkalmazandó, átfogó jogi kerethez.

28. Az európai adatvédelmi biztos megjegyzi, hogy mindenképpen biztosítani kell az adatvédelmi jogi kereten belüli összhangot, szükség esetén a szabadságon, a biztonságon és a jog érvényesülésén alapuló térségben alkalmazandó különböző jogi eszközök harmonizációja és konszolidációja révén.

A hatályos szerződések alapján

29. Az első lépés megtételére a 2008/977/IB tanácsi kerethatározat ([18]) közelmúltbeli elfogadásával került sor. Ez a jogi eszköz azonban nem tekinthető átfogó keretnek, alapvetően azért, mert a rendelkezései nem általános alkalmazásúak. Nem vonatkoznak az olyan belföldi helyzetekre, amikor a személyes adatok ugyanabból a tagállamból származnak, mint amelyik felhasználja azokat. Ez a megszorítás szükségszerűen csökkenti a tanácsi kerethatározat hozzáadott értékét, hacsak valamennyi tagállam úgy nem dönt, hogy a nemzeti végrehajtó jogszabályokba belefoglalja a belföldi helyzeteket is, ez azonban nem valószínű.

30. A második ok, amely miatt az európai adatvédelmi biztos úgy véli, hogy a 2008/977/IB tanácsi kerethatározat hosszú távon nem biztosít kielégítő adatvédelmi keretet a szabadságon, a biztonságon és a jog érvényesülésén alapuló térségben, az, hogy számos lényeges rendelkezése nincs összhangban a 95/46/EK irányelvvel. A hatályos szerződések alapján a második lépés a tanácsi kerethatározat hatályának kiterjesztése és a 95/46/EK irányelvhez való igazítása lehetne.

31. A világos és hosszú távú terv kialakítása további ösztönzést adhatna az átfogó adatvédelmi rendszer létrehozásának. Ennek a tervnek része lehetne az adatgyűjtést és adatcserét, a meglévő adatbázisok működtetését, valamint az európai adatvédelmi biztosítékokat meghatározó, átfogó és koherens megközelítés. A tervnek meg kell akadályoznia a szükségtelen átfedéseket és a párhuzamos eszközök meglétét (ezzel együtt a személyes adatok párhuzamos feldolgozását). Elő kell segítenie az e területen folytatott uniós politikák egységességét, valamint növelnie kell a polgárok

([14]) Az adatvédelmi biztos ez utóbbi ponttal kapcsolatban a büntetőügyekben folytatott rendőrségi és igazságügyi együttműködés keretében feldolgozott személyes adatok védelméről szóló tanácsi kerethatározati javaslatról (COM (2005)475 végleges) szóló, 2005. december 19-i véleményében (HL C 47., 2006.2.25., 27.o., 30–32. pont) fejtette ki az álláspontját.

([15]) Data Protection in the European Union – Citizens' perceptions – Analytical report (Adatvédelem az Európai Unióban – A polgárok véleménye – Elemzés) , Flash Eurobarometer Series 225, Jan. 2008, http://www.ec.europa.eu/public_opinion/flash/fl_225_en.pdf

([16]) Lásd még a közlemény prioritásait.

([17]) COM(2006) 331 végleges, 2006. június 28-án.

([18]) Lásd a 11. lábjegyzetet.

adatainak a hatóságok általi kezelésébe vetett bizalmat. Az európai adatvédelmi biztos azt ajánlja a Tanácsnak, hogy a stockholmi programban jelentse be a világos és hosszú távú terv szükségességét.

32. Az európai adatvédelmi biztos azt ajánlja továbbá, hogy értékeljék és összefüggéseiben elemezzék az e területen már elfogadott intézkedéseket, konkrét végrehajtásukat és hatékonyságukat. Az értékelés során kellően vegyék figyelembe a magánélet védelmének költségeit és a bűnüldözés hatékonyságát. Amennyiben az értékelések azt mutatják, hogy egyes intézkedések nem hozzák a várt eredményt, vagy nem arányosak a kitűzött célokkal, a következő lépéseket kell mérlegelni:

— Első lépésként az intézkedések módosítása vagy hatályon kívül helyezése, amennyiben a létjogosultságukat nem igazolja kellően a bűnüldöző hatóságok vagy az európai polgárok számára általuk teremtett konkrét hozzáadott érték.

— Második lépésként annak megvizsgálása, hogy volna-e lehetőség a meglévő intézkedések alkalmazásának javítására.

— Csak harmadik lépésként új jogalkotási eszközök javaslata, amennyiben valószínűsíthető, hogy az új intézkedések szükségesek a tervezett célok eléréséhez. Új eszközöket csak akkor szabad elfogadni, ha egyértelmű és konkrét hozzáadott értéket képviselnek a bűnüldöző hatóságok vagy az európai polgárok számára.

Az európai adatvédelmi biztos javasolja, hogy a stockholmi programban utaljanak a meglévő intézkedések értékelési rendszerére.

33. Végül de nem utolsósorban kiemelt figyelmet kell fordítani a meglévő biztosítékok jobb alkalmazására, az adatvédelmi irányelv jobb végrehajtását célzó munkaprogram nyomon követéséről szóló bizottsági közleménnyel ([19]) és az európai adatvédelmi biztosnak a közleményről szóló véleményében ([20]) adott javaslataival összhangban. Sajnálatos módon a harmadik pillérben a Bizottságnak nincs lehetősége jogsértési eljárást kezdeményezni.

A Lisszaboni Szerződés alapján

34. A Lisszaboni Szerződés megnyitja egy valódi átfogó adatvédelmi keret lehetőségét. Az Európai Unió működéséről szóló szerződés 16.2. cikke előírja, hogy a Tanács és az Európai Parlament állapítsa meg azokat a szabályokat, amelyek az uniós intézmények, szervek, hivatalok és ügynökségek, a tagállamok – amikor az uniós jog hatálya alá eső tevékenységet végeznek – és a magánszférához tartozó felek által biztosítandó adatvédelemre vonatkoznak.

35. Az európai adatvédelmi biztos megérti, hogy a közlemény középpontjában egy átfogó adatvédelmi rendszer áll, ami a Bizottság azon szándékát mutatja, hogy egy minden adatfeldolgozási tevékenységre alkalmazandó jogi keretet javasoljon. Az európai adatvédelmi biztos helyesli ezt a szándékot, amely javítja a rendszer egységességét, jogbiztonságot nyújt, és ezáltal fokozza a védelmet. A segítségével a jövőben elkerülhetők lennének az olyan nehézségek, mint a pillérek közötti választóvonal meghúzása olyan esetekben, amikor a magánszektorban kereskedelmi célokból összegyűjtött adatokat később a bűnüldözés céljára használják fel. A pillérek közötti választóvonal nem tükrözi teljes mértékben a valóságot, amint azt a Bíróságnak a PNR-rel ([21]) és az adatmegőrzéssel ([22]) kapcsolatban hozott fontos ítéletei bizonyítják.

36. Az európai adatvédelmi biztos javasolja, hogy a stockholmi programban hangsúlyozzák az átfogó adatvédelmi rendszer kialakításának fenti indokait. Látszik belőlük, hogy egy ilyen rendszer nem egyszerűen előnyben részesített megoldás, hanem az adatfelhasználás változó gyakorlata következtében szükségesség. Az európai adatvédelmi biztos azt ajánlja, hogy a stockholmi programban prioritásként szerepeljen egy új jogalkotási keret – többek között a 2008/977/IB tanácsi kerethatározat helyébe lépve – igénye.

37. Az európai adatvédelmi biztos hangsúlyozza, hogy az általános jogi kereten alapuló átfogó adatvédelmi rendszer koncepciója nem zárja ki annak lehetőségét, hogy a rendőrségi és igazságügyi ágazat tekintetében kiegészítő adatvédelmi szabályokat fogadjanak el. Ezek a kiegészítő szabályok figyelembe vehetnék a bűnüldözés sajátos igényeit, amint azt a Lisszaboni Szerződéshez csatolt 21. nyilatkozat ([23]) is kijelenti.

V.2. **Az adatvédelmi elvek újraírása**

38. A közlemény megállapítja, hogy a magánszemélyek, valamint az állami és magánszervezetek közötti kommunikációt átalakító technológiai változások mentek végbe. A Bizottság szerint ez több adatvédelmi alapelv újraírását teszi szükségessé.

([19]) COM(2007) 87 végleges, 2007. március 7.

([20]) A 2007. július 25-i vélemény (HL C 255., 2007.10.27., 1. o.), különösen annak 30. pontja.

([21]) A Bíróságnak a C-317/04. sz. az Európai Parlament kontra az Európai Unió Tanácsa és a C-318/04. sz. Európai Parlament kontra az Európai Közösségek Bizottsága ügyben 2006. május 30-án hozott ítélete, C-317/04.. és C-318/04. sz. egyesített ügyek, EBHT 2006., I-4721. o.

([22]) A Bíróságnak a C-301/06. sz. Írország kontra Európai Parlament és az Európai Unió Tanácsa ügyben 2009. február 10-én hozott ítélete, még nem tették közzé.

([23]) Lásd a Lisszaboni Szerződést elfogadó kormányközi konferencia zárónyilatkozatához csatolt 21. nyilatkozatot a személyes adatok védelméről a büntetőügyekben folytatott igazságügyi, valamint a rendőrségi együttműködés területén (HL C 115., 2008.5.9., 345. o.).

39. Az európai adatvédelmi biztos üdvözli a közlemény ezen szándékait. Rendkívül hasznos ezen elvek hatékonyságának a technológiai változások szempontjából történő értékelése. Elsőként is meg kell jegyezni, hogy az adatvédelmi elvek újraírásának és ismételt megerősítésének nem kell minden esetben közvetlenül a technológiai fejlődéshez kapcsolódnia. Más okok is szükségessé tehetik ezt, például a fenti III. részben említett okok, a nemzetközivé válás, az adatoknak a bűnüldözés céljára való növekvő mértékű felhasználása és a szabad mozgás.

40. Ezenkívül az európai adatvédelmi biztos véleménye szerint ezt az értékelést be lehet vonni a 2009. május 19–20-án „Személyes adatok – fokozott felhasználás, nagyobb védelem" címmel megtartott konferencián a Bizottság által bejelentett nyilvános konzultációba. Ez a nyilvános konzultáció értékes adalékokat nyújthat ([24]). Az európai adatvédelmi biztos azt javasolja, hogy a Tanács a stockholmi program szövegében, a Bizottság pedig a konzultációra vonatkozó nyilvános nyilatkozataiban hangsúlyozza a közlemény 2.3. pontjában megfogalmazott szándékok, valamint az adatvédelem jövőjéről folytatott nyilvános konzultáció közötti kapcsolatot.

41. Az értékelés tartalmának illusztrálásaként a következő pontok említhetők:

— A szabadságon, a biztonságon és a jog érvényesülésén alapuló térségben a személyes adatok valószínűleg rendkívül érzékenynek számítanak (például a büntetőítéletekkel kapcsolatos, rendőrségi és biometrikus adatok, ez utóbbiak például ujjlenyomatok és DNS-profilok).

— Feldolgozásuk negatív következményekkel járhat az adatalanyok számára, különösen ha figyelembe vesszük a bűnüldöző hatóságok kényszerítő jogkörét. Emellett az adatok ellenőrzése és elemzése egyre inkább automatizált, gyakran történik emberi beavatkozás nélkül. A technológia lehetővé teszi, hogy a személyes adatokat tartalmazó adatbázisokat általános keresésre használják (adatbányászat, profilalkotás stb.) Egyértelműen meg kell határozni azokat a jogi kötelezettségeket, amelyeken az adatfeldolgozás alapul.

— Az adatvédelmi jogszabályok sarokköve, hogy a személyes adatokat meghatározott célból kell összegyűjteni, és azokat nem szabad e céllal összeegyeztethetetlen módon felhasználni. Az összeegyeztethetetlen célból történő felhasználás csak akkor engedhető meg, ha azt jogszabály írja elő, és valamely közérdek – például az Emberi Jogok Európai Egyezményének 8.2. cikkében említettek – szükségessé teszi.

— Azon igény, hogy tiszteletben tartsák a célok korlátozásának elvét, következményekkel járhat az adatfelhasználás jelenlegi tendenciáira nézve. A bűnüldöző szervek felhasználják azokat az adatokat, amelyeket magánvállalatok a távközlési, közlekedési és pénzügyi ágazatban kereskedelmi célból gyűjtöttek össze. Emellett nagy méretű információs rendszerek jönnek létre, például a bevándorlás és a határellenőrzés területén. Lehetőség van az adatbázisok közötti kölcsönös kapcsolatokra és a hozzáférésre, ezáltal a személyes adatok összegyűjtésének eredeti céljához képest bővül a kör. E jelenlegi tendenciák átgondolására van szükség, beleértve szükség esetén az esetleges kiigazításokat és/vagy a további biztosítékokat.

— A közleményben említett adatvédelmi elveken túlmenően az értékelés során figyelmet kell fordítani a feldolgozás átláthatóságának igényére, lehetővé téve az adatalany számára jogai gyakorlását. A bűnüldözés területén különösen problémás kérdés az átláthatóság, elsősorban azért, mert az átláthatóságot a nyomozás veszélyeztetésével kell szembeállítani.

— Megoldásokat kell találni a harmadik országokkal folytatott adatcserére.

42. Az értékelésnek továbbá azokra a lehetőségekre kell összpontosítania, amelyekkel az adatvédelmi elvek alkalmazása javítható. Ezzel kapcsolatban hasznos lehet azokra az eszközökre koncentrálni, amelyek az adatkezelők felelősségét erősíthetik Ezeknek az eszközöknek lehetővé kell tenniük az adatkezelőknek az adatkezelésért való teljes körű elszámoltathatóságát. Az „adatkormányzás" hasznos kifejezés ebben az összefüggésben. Beletartozik minden olyan jogi, technikai és szervezeti eszköz, amellyel a szervezetek az adatkezelés módjáért való teljes körű felelősségvállalást biztosítják, például a tervezés és ellenőrzés, a helyes technológia alkalmazása, a személyzet megfelelő képzése, megfelelőségi ellenőrzések stb.

V.3. **A magánéletet tiszteletben tartó technológiák**

43. Az európai adatvédelmi biztos örömmel állapítja meg, hogy a közlemény 2.3. pontja megemlíti a magánéleti tanúsítványt. Emellett hivatkozni lehetne a „beépített adatvédelemre", valamint az EU adatvédelmi keretébe illeszkedő „rendelkezésre álló legjobb technikák" megállapításának igényére.

44. Az európai adatvédelmi biztos véleménye szerint a „beépített adatvédelem" és a magánéletet tiszteletben tartó technológiák hasznos eszköznek bizonyulhatnak a jobb adatvédelem és az információ hatékonyabb felhasználása számára. Az európai adatvédelmi biztos két, egymást nem kizáró továbblépési lehetőséget javasol:

— Magánélet- és adatvédelmi tanúsítási rendszer ([25]) mint választási lehetőség az információs rendszerek kiépítői és felhasználói számára, uniós finanszírozással és jogszabályi támogatással vagy anélkül.

([24]) A 29. cikk alapján létrehozott adatvédelmi munkacsoport, amelynek az európai adatvédelmi biztos is tagja, úgy döntött, hogy jelentős erőfeszítéseket tesz a nyilvános konzultációhoz történő hozzájárulása érdekében.

([25]) Ilyen rendszerre példa az európai adatvédelmi bizalompecsét (EuroPriSe).

— Az információs rendszerek kiépítői és felhasználói számára előírt azon jogi kötelezettség, hogy a beépített adatvédelem elvével összhangban álló rendszereket alkalmazzanak. Ez szükségessé teheti az adatvédelmi jogszabályok jelenlegi hatályának kiterjesztését olyan módon, hogy a rendszerek kiépítőit felelőssé teszik az általuk kifejlesztett információs rendszerekért ([26]).

Az európai adatvédelmi biztos javasolja, hogy a stockholmi program említse meg ezeket a továbblépési lehetőségeket.

V.4. **Külső szempontok**

45. Egy másik, szintén a közleményben tárgyalt kérdés a nemzetközi adatvédelmi előírások kidolgozása és előmozdítása. Jelenleg számos tevékenység folyik a globális alkalmazású, megvalósítható előírások megállapítása érdekében, például az adatvédelmi és a magánélet védelmével foglalkozó biztosok nemzetközi konferenciája keretében. A közeljövőben e tevékenységek nyomán nemzetközi megállapodás is születhet. Az európai adatvédelmi biztos javasolja, hogy a stockholmi program támogassa ezeket a tevékenységeket.

46. A közlemény megemlíti az Egyesült Államokkal közösen elért eredményeken alapuló, kétoldalú megállapodások megkötését is. Az európai adatvédelmi biztos egyetért azzal, hogy világos jogi keretre van szükség a harmadik országokba irányuló adattovábbításhoz, és ezért üdvözölte az uniós és az amerikai hatóságoknak a magas szintű kapcsolattartó csoport keretében végzett, egy esetleges transzatlanti adatvédelmi eszközzel kapcsolatos közös munkáját, egyidejűleg azonban további pontosításra és a konkrét kérdésekkel kapcsolatban nagyobb odafigyelésre szólít fel ([27]). Ezzel összefüggésben érdemes megemlíteni a szabadság, a biztonság és a jogérvényesülés területén létrehozandó euroatlanti együttműködési térségről szóló belügyi jelentés felvetéseit; a jelentés szerint az Uniónak 2014-ig kellene döntenie ebben az ügyben. Ez a térség nem jöhet létre megfelelő adatvédelmi biztosítékok nélkül.

47. Az európai adatvédelmi biztos véleménye szerint az európai adatvédelmi előírásoknak – amelyek az Európa Tanácsnak az egyének személyes adataik gépi feldolgozása során való védelméről szóló 108. sz. egyezményén ([28]), valamint az Európai Bíróság és az Emberi Jogok Európai Bírósága ítélkezési gyakorlatán alapulnak – az Egyesült Államokkal kötendő általános adatvédelmi és adatcsere-megállapodásban meg kellene határozniuk a védelem szintjét. Egy ilyen általános megállapodás lehetne a személyes adatok cseréjére vonatkozó konkrét megállapodások alapja. A kérdés még fontosabb a közlemény 4.2.1. pontjában megfogalmazott szándék fényében, amely szerint az Európai Uniónak szükség esetén rendőrségi együttműködési megállapodásokat kell kötnie.

48. Az európai adatvédelmi biztos teljes mértékben megérti, hogy fokozni kell a nemzetközi együttműködést, esetenként az alapvető jogokat nem védő országokkal is. Nem szabad azonban megfeledkezni arról ([29]), hogy az ilyen nemzetközi együttműködés várhatóan az adatgyűjtés és a nemzetközi adattovábbítás nagymértékű növekedéséhez vezet. Alapvető fontosságú ezért, hogy a tisztességes és jogszerű adatfeldolgozás elvei – csakúgy, mint általában a jogszerű eljárás elvei – a személyes adatoknak az Unió határain átnyúló gyűjtésére és továbbítására is vonatkozzanak, és hogy a személyes adatokat harmadik országok vagy nemzetközi szervezetek számára csak abban az esetben továbbítsák, ha az érintett harmadik felek biztosítják az adatvédelem megfelelő szintjét, vagy megfelelő biztosítékokat nyújtanak.

49. Összefoglalva, az európai adatvédelmi biztos javasolja, hogy a stockholmi program térjen ki az Egyesült Államokkal és más harmadik országokkal kötendő, az EU területén garantált védelmi szinten alapuló általános adatvédelmi és adatcsere-megállapodások jelentőségére. Szélesebb körben szemlélve, harmadik országok és nemzetközi szervezetek összefüggésében az európai adatvédelmi biztos felhívja a figyelmet arra, hogy aktívan elő kell mozdítani az alapvető jogok tiszteletben tartását, különösen pedig az adatvédelmet ([30]). A stockholmi program ezenkívül megemlíthetné azt az általános koncepciót, hogy a személyes adatok harmadik országokkal folytatott cseréje megköveteli, hogy az érintett harmadik felek biztosítsák az adatvédelem megfelelő szintjét, vagy megfelelő biztosítékokat nyújtsanak.

VI. **AZ INFORMÁCIÓ FELHASZNÁLÁSA**

VI.1. **Az európai információs modell felé**

50. A jobb információcsere alapvető politikai cél az Európai Unió számára a szabadságon, a biztonságon és a jog érvényesülésén alapuló térségben. A közlemény 4.1.2. pontja hangsúlyozza, hogy az Európai Unió biztonsága a tagállami hatóságok és az európai szereplők közötti információcserét szolgáló hatékony mechanizmusoktól függ. Európai rendőrség, európai büntető igazságszolgáltatási rendszer és

([26]) Az adatvédelmi jogszabályok hatálya kiterjed az információ felhasználóira, valamint az adatkezelőkre és -feldolgozókra is.

([27]) Lásd az európai adatvédelmi biztos 2008. november 11-i véleményét az információcserével, valamint a magánélet és a személyes adatok védelmével foglalkozó EU–USA magas szintű kapcsolattartó csoport végső jelentéséről (HL C 128., 2009.6.6., 1. o.).

([28]) ETS 108. szám, 1981.1.28.

([29]) Lásd az európai adatvédelmi biztos 2005. november 28-i levelét a szabadságon, a biztonságon és a jog érvényesülésén alapuló térség külső dimenziójáról szóló bizottsági közleményről, amely az európai adatvédelmi biztos honlapján olvasható.

([30]) A terroristák névsorával kapcsolatos közelmúltbeli ítélkezési gyakorlat azt bizonyítja, hogy garanciákra van szükség – az ENSZ-szel fennálló kapcsolatokban is – annak biztosítására, hogy a terrorizmusellenes intézkedések megfeleljenek az alapvető jogokkal kapcsolatos uniós előírásoknak (a C-402/05 P. és a C-415/05 P sz. Kadi and Al Barakaat Foundation kontra Tanács egyesített ügyekben 2008. szeptember 3-án hozott ítélet, még nem tették közzé).

európai határellenőrzés hiányában logikus, hogy az információcsere ilyen hangsúlyos helyet foglal el. Ezért az információval kapcsolatos intézkedések az Európai Unió alapvető hozzájárulásait jelentik, amelyek lehetővé teszik a tagállami hatóságok számára, hogy hatékonyan lépjenek fel a határokon átnyúló bűnözés ellen, és hatékonyan védjék a külső határokat. Az intézkedések azonban nemcsak a polgárok biztonságát érintik, hanem a szabadságukat – a személyek szabad mozgását már korábban, e vélemény szempontjai között említettük –, valamint az igazságszolgáltatást is.

51. Pontosan ez az oka annak, hogy a hozzáférhetőség elve bekerült a hágai programba. Az elv kimondja, hogy a bűnözés elleni küzdelemhez szükséges információknak akadálymentesen kell átlépniük az EU belső határait. Az utóbbi idők tapasztalatai azt mutatják, hogy nehéz volt ezt az elvet átültetni a jogalkotási intézkedésekbe. A hozzáférhetőség elve alapján történő információcseréről szóló tanácsi kerethatározatra vonatkozó, 2005. október 12-i bizottsági javaslatot ([31]) a Tanács nem fogadta el. A tagállamok nem voltak hajlandók teljes mértékben elfogadni a hozzáférhetőség elvének következményeit. Ehelyett korlátozottabb hatályú eszközöket ([32]) fogadtak el, mint például a különösen a terrorizmus és a határokon átnyúló bűnözés elleni küzdelemre irányuló, határokon átnyúló együttműködés megerősítéséről szóló, 2008. június 23-i 2008/615/IB tanácsi határozatot ([33]) (prümi határozat).

52. Míg a hágai program középpontjában a hozzáférhetőség elve állt, úgy látszik, hogy a Bizottság most szerényebb megközelítést keres. Azt tervezi, hogy egy európai információs modell bevezetésével fogja tovább ösztönözni a tagállami hatóságok közötti információcserét. Az EU svéd elnöksége hasonlóképpen gondolkodik ([34]). Az elnökség az információcsere stratégiájára vonatkozó javaslatot fog előterjeszteni. A Tanács már megkezdte az Európai Unió információkezelési stratégiájára vonatkozó nagyszabású projekttel kapcsolatos munkát, amely szorosan kapcsolódik az európai információs modellhez. Az európai adatvédelmi biztos nagy érdeklődéssel követi ezeket a fejleményeket, és hangsúlyozza, hogy a projektekben figyelmet kell fordítani az adatvédelmi vonatkozásokra.

Európai információs modell és adatvédelem

53. Kiindulásként hangsúlyozni kell, hogy a szabadságon, a biztonságon és a jog érvényesülésén alapuló térség jövője nem lehet a technológia által vezérelt, abban az értelemben, hogy az új technológiák kínálta szinte korlátlan lehetőségeket mindig az adatvédelmi elvekkel kell szembeállítani, és csak akkor felhasználni, ha megfelelnek ezeknek az elveknek.

54. Az európai adatvédelmi biztos megállapítja, hogy a közleményben bemutatott információs modell nemcsak technikai modell, hanem a stratégiai elemzési kapacitás fokozását és az operatív információk jobb összegyűjtését és kezelését is szolgálja. Elismeri továbbá, hogy az adatvédelmi elvek betartásával egyidejűleg a politikai szempontokat – például az információ összegyűjtésének, megosztásának és feldolgozásának kritériumait – is figyelembe kell venni.

55. Az információs technológiai és a jogi feltételek egyaránt alapvetően fontosak és fontosak is maradnak. Az európai adatvédelmi biztos üdvözli, hogy a közlemény abból a feltételezésből indul ki, hogy az európai információs modell nem épülhet technikai megfontolásokra. Lényeges, hogy az információ összegyűjtésére, megosztására és feldolgozására kizárólag konkrét biztonsági igények szerint és az adatvédelmi elvek betartásával kerüljön sor. Az európai adatvédelmi biztos teljes mértékben egyetért azzal is, hogy nyomon követési mechanizmust kell kidolgozni az információcsere működésének értékelésére. Azt javasolja, hogy a Tanács a stockholmi programban alaposabban dolgozza ki ezeket az elemeket.

56. Ehhez kapcsolódóan az európai adatvédelmi biztos hangsúlyozza, hogy a polgárok védelmét szolgáló adatvédelmet nem szabad a hatékony adatkezelés akadályának tekinteni. Az adatvédelem hasznos eszközökkel szolgál az információ tárolásának, cseréjének, valamint az információhoz való hozzáférésnek a javítása számára. Az adatalanyok azon joga, hogy tájékoztatást kapjanak a rájuk vonatkozó információ feldolgozásáról és helyesbítsék a hibás információt, szintén javíthatja az adatkezelő rendszerekben található adatok pontosságát.

57. Az adatvédelmi jogszabályok lényegében az alábbi következményekkel járnak: ha az adatokra konkrét és törvényes célból van szükség, akkor felhasználhatók; ha nem jól meghatározott célból van rájuk szükség, akkor a személyes adatokat nem szabad felhasználni. Az első esetben a megfelelő biztosítékok további intézkedéseket tehetnek szükségessé.

58. Az európai adatvédelmi biztos azonban bírálja, hogy a közleményben a „jövőbeli igények meghatározása" mekkora szerepet kap az információs modell részeként. Hangsúlyozza, hogy az információs rendszerek kiépítésekor a jövőben is a célok korlátozásának elve kell, hogy érvényesüljön ([35]). Ez az adatvédelmi rendszer által a polgároknak nyújtott egyik alapvető garanciát jelenti: a polgárnak előre tudnia kell, hogy a rá vonatkozó adatokat milyen célból gyűjtik össze, és hogy azokat csak arra a célra fogják felhasználni, különösen a jövőben. Ezt a garanciát az Európai Unió Alapjogi Chartájának 8. cikke is tartalmazza. A célok korlátozásának elve lehetővé teszi a kivételeket – különösen a szabadságon, a biztonságon és a jog érvényesülésén alapuló térséggel kapcsolatban –, de a kivételek nem határozhatják meg a rendszer felépítését.

([31]) COM(2005) 490 végleges.

([32]) A hozzáférhetőség tekintetében a prümi határozat széles körű rendelkezéseket tartalmaz a biometrikus adatokkal (DNS és ujjlenyomat) kapcsolatban.

([33]) HL L 210., 2008.8.6., 1. o.

([34]) Lásd az 5. lábjegyzetben említett kormányzati uniós munkaprogramot, 23. o.

([35]) Lásd a fenti 41. pontot is.

A helyes szerkezet megválasztása

59. Az információcsere helyes szerkezetének megválasztása mindennek az alapja. Az információ helyes szerkezetének jelentőségét a közlemény is elismeri (4.1.3. pont), de sajnos csak az átjárhatósággal kapcsolatban.

60. Az európai adatvédelmi biztos egy másik szempontot is hangsúlyoz: az európai információs modellben az adatvédelmi követelményeknek minden rendszerfejlesztés szerves részét kell képezniük, és nem szabad azokat csak a rendszer törvényességéhez szükséges feltételnek tekinteni ([36]). Figyelembe kell venni a „beépített adatvédelem" koncepcióját és a „rendelkezésre álló legjobb technikák ([37])" meghatározásának szükségességét, a fenti 43. pontnak megfelelően. Az európai információs modellnek e koncepciókra kell épülnie. Ez pontosabban fogalmazva azt jelenti, hogy a közbiztonsági célokra kidolgozott információs rendszereknek mindig a „beépített adatvédelem" elvével összhangban kell elkészülniük. Az európai adatvédelmi biztos azt javasolja, hogy a Tanács ezeket az elemeket foglalja bele a stockholmi programba.

A rendszerek átjárhatósága

61. Az európai adatvédelmi biztos hangsúlyozza, hogy az átjárhatóság nem pusztán technikai kérdés, hanem következményei vannak a polgárok védelmére, különösen az adatvédelemre nézve. Az adatvédelem szempontjából nézve a rendszerek átjárhatósága – amennyiben helyesen alakítják ki – egyértelmű előnyökkel jár a kettős tárolás elkerülése céljából. Nyilvánvaló azonban, hogy ha az adatokhoz való hozzáférést vagy az adatcserét technikailag lehetővé teszik, ez sok esetben erőteljes ösztönzést jelent a tényleges hozzáférésre vagy adatcserére. Más szóval az átjárhatósággal együtt jár a különböző rendeltetésű adatbázisok összekapcsolásának a különös kockázata ([38]). Ez érintheti az adatbázisok céljára vonatkozó szigorú korlátozásokat.

62. Röviden, pusztán az a tény, hogy az átjárható adatbázisok között technikailag kivitelezhető a digitális információ cseréje, illetve ezek az adatbázisok egyesíthetők, nem jelenti a célok korlátozásának elve alóli kivétel igazolását. Az átjárhatóságnak konkrét esetekben világos és megfontolt politikai döntésen kell alapulnia. Az európai adatvédelmi biztos azt javasolja, hogy a stockholmi program tartalmazza ezt a gondolatmenetet.

([36]) Lásd a PRISE projekt keretében kidolgozott, a magánélet védelmét erősítő biztonsági technológiák kidolgozására, alkalmazására és felhasználására vonatkozó iránymutatásokat és kritériumokat (http://www.prise.oeaw.ac.at).

([37]) A rendelkezésre álló legjobb technikák a tevékenységek és a működési módszerek kidolgozásának leghatékonyabb és legfejlettebb szakaszát jelentik, amelyek azt mutatják, hogy adott technikák a gyakorlatban alkalmasak arra, hogy elvi alapot biztosítsanak ahhoz, hogy az ITS-alkalmazások és -rendszerek megfeleljenek az EU szabályozási keretében előírt magánéleti, adatvédelmi és biztonsági követelményeknek.

([38]) Lásd az európai adatvédelmi biztosnak az európai adatbázisok közötti kölcsönös átjárhatóságról szóló bizottsági közleményhez fűzött, 2006. március 10-i észrevételeit az alábbi címen: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2006/06-03-10_Interoperability_EN.pdf

VI.2. **Az egyéb célra összegyűjtött információ felhasználása**

63. A közlemény nem foglalkozik kifejezetten az elmúlt évek egyik legfontosabb tendenciájával, nevezetesen a magánszektorban kereskedelmi célokból összegyűjtött adatok bűnüldözési célú felhasználásával. A tendencia nemcsak a elektronikus kommunikáció forgalmi adatai és az (egyes) harmadik országokba repülő személyekre vonatkozó utasforgalmi adatok esetén ([39]), hanem a pénzügyi ágazatban is érvényesül. Példa erre az Európai Parlament és a Tanács 2005. október 26-i 2005/60/EK irányelve ([40]) a pénzügyi rendszereknek a pénzmosás, valamint terrorizmus finanszírozása céljára való felhasználásának megelőzéséről. Egy másik jól ismert és sokat vitatott példa a személyes adatoknak a Society for Worldwide Interbank Financial Telecommunication (SWIFT) általi feldolgozása ([41]), mégpedig olyan adatoké, amelyek az USA Pénzügyminisztériuma számára a terrorizmus finanszírozásának felderítését célzó programhoz szükségesek.

64. Az európai adatvédelmi biztos úgy véli, hogy ezekre a tendenciákra a stockholmi programban különös figyelmet kell fordítani. Ezek a célok korlátozásának elvétől való eltérésnek tekinthetők, és gyakran rendkívüli módon sértik a magánéletet, mert az adatok felhasználása sokat elárulhat valakinek a viselkedéséről. Minden olyan esetben, amikor ilyen, a magánéletet sértő intézkedés javaslatára kerül sor, nagyon nyomós érvekkel kell alátámasztani az intézkedés szükségességét. Ha a szükségesség igazolható, biztosítani kell az egyének jogainak teljes mértékű védelmét.

65. Az európai adatvédelmi biztos véleménye szerint a kereskedelmi célokból összegyűjtött személyes adatok bűnüldözési célú felhasználása kizárólag szigorú feltételekkel engedhető meg, például:

— Az adatokat kizárólag eseti alapon, konkrétan meghatározott célokra – pl. a terrorizmus vagy a súlyos bűncselekmények elleni küzdelem céljára – használják.

— Az adatokat „push" (küldő) és nem „pull" (lehívó) rendszerben továbbítják ([42]).

([39]) Lásd pl. a fenti 15. pontot.

([40]) HL L 309, 2005.11.25., 15. o.

([41]) Lásd a 29. cikk alapján létrehozott munkacsoport véleményét a személyes adatoknak a Society for Worldwide Interbank Financial Telecommunication (SWIFT) általi feldolgozásáról.

([42]) A „push" rendszer esetében az adatkezelő küldi meg kérésre az adatokat a bűnüldöző hatóságnak. A „pull" rendszerben a bűnüldöző hatóságnak hozzáférése van az adatkezelő adatbázisához, és lehívja az információt az adatbázisból. A „pull" rendszerben az adatkezelő felelősségvállalása nehezebb.

— Az adatok iránti kérelmeknek arányosnak és célirányosnak kell lenniük, és elvileg adott személyekkel kapcsolatos gyanún kell alapulniuk.

— A rutinkeresés, az adatbányászat és a profilalkotás kerülendő.

— A bűnüldözési célú adatfelhasználásról naplót kell vezetni annak érdekében, hogy a jogait gyakorló adatalany, az adatvédelmi hatóságok és az igazságügyi hatóságok ténylegesen ellenőrizhessék a felhasználást.

VI.3. **Információs rendszerek és uniós szervek**

Információs rendszerek centralizált adattárolással vagy anélkül ([43])

66. Az elmúlt években jelentősen megnőtt az uniós jogon alapuló információs rendszerek száma a szabadságon, a biztonságon és a jog érvényesülésén alapuló térségben. Időnként olyan rendszer létrehozásáról születik határozat, amely európai szintű, centralizált adattárolással jár, más esetekben a jogszabály csak a nemzeti adatbázisok közötti információcserét írja elő. A centralizált adattárolásra valószínűleg a Schengeni Információs Rendszer a legjobb példa. A centralizált tárolás nélküli rendszerre adatvédelmi szempontból a legfontosabb példa a 2008/615/IB tanácsi határozat ([44]) (prümi határozat), amely hatalmas mennyiségű biometrikus adatnak a tagállami hatóságok közötti cseréjét irányozza elő.

67. A közlemény szerint folytatódni fog az új rendszerek létrehozásának tendenciája. A 4.2.2. pontból vett első példa az az információs rendszer, amely az Európai Bűnügyi Nyilvántartási Információs Rendszert (ECRIS) bővíti ki annak érdekében, hogy az Unión kívüli országok állampolgáraira is kiterjedjen. A Bizottság már megrendelte a harmadik országok elítélt állampolgárainak európai indexére (EICTCN) vonatkozó tanulmányt, amelynek eredményeképpen várhatóan centralizált adatbázis fog készülni. Egy másik példa erre a más tagállamok fizetésképtelenségi nyilvántartásaiban szereplő személyekre vonatkozó információnak az e-igazságszolgáltatás keretében (a közlemény 3.4.1. pontja) végzett cseréje, centralizált tárolás nélkül.

68. A decentralizált rendszer adatvédelmi szempontból bizonyos előnyökkel járna. Az adatokat nem két helyen tárolják – a tagállam hatóságánál és a centralizált rendszerben –, egyértelmű, hogy ki felel az adatokért, hiszen a tagállam hatósága az adatkezelő, továbbá az igazságügyi és adatvédelmi hatóságok tagállami szinten végezhetik az ellenőrzést. A rendszernek azonban megvannak a maga gyenge pontjai is a más joghatóságokkal végzett adatcsere során, például annak biztosításakor, hogy az információ mind a származási, mind a célországban naprakész maradjon, valamint a mindkét oldali hatékony ellenőrzés biztosításakor. Még bonyolultabb az adatcserét végző műszaki rendszerért való felelősségvállalás biztosítása. Ezeket a problémákat olyan centralizált rendszer létrehozásával lehet orvosolni, amelyben legalább a rendszer egyes részeiért (pl. a műszaki infrastruktúráért) európai szervek felelnek.

69. A fentiek alapján hasznos lenne olyan érdemi kritériumokat kidolgozni, amelyek szerint választani lehetne a centralizált és a decentralizált rendszer között, és amelyek az egyes konkrét esetekben biztosítanák az egyértelmű és megfontolt választást. Ezek a kritériumok hozzájárulhatnak maguknak a rendszereknek a működéséhez, valamint a polgárok adatainak a védelméhez is. Az európai adatvédelmi biztos javasolja, hogy a stockholmi program tartalmazza az ilyen kritériumok kidolgozásának szándékát.

Nagy méretű információs rendszerek

70. A közlemény 4.2.3.2. pontja röviden tárgyalja a nagy méretű információs rendszerek jövőjét, különös tekintettel a Schengeni Információs Rendszerre (SIS) és a Vízuminformációs Rendszerre (VIS).

71. A 4.2.3.2. pont megemlíti a tagállamok területére történő belépést, illetve az onnan történő kilépést nyilvántartó elektronikus rendszert, valamint az utas-nyilvántartási programokat is. Ezt a rendszert a Bizottság Franco Frattini alelnök kezdeményezésére a „határcsomag" részeként már korábban is bejelentette ([45]). Az európai adatvédelmi biztos előzetes észrevételeiben ([46]) meglehetősen kritikusan szemlélte ezt a javaslatot, mivel nem sikerült kellő mértékben igazolni, hogy a meglévő nagy méretű rendszerek mellett szükség lenne egy ilyen, a magánéletbe betolakodó rendszerre. Az európai adatvédelmi biztos nem látja, hogy további bizonyítékokat sorakoztattak volna fel a rendszer szükségessége mellett, ezért azt javasolja, hogy a Tanács ne említse meg ezt a gondolatot a stockholmi programban.

72. Ehhez kapcsolódóan az európai adatvédelmi biztos utalni kíván az uniós információcsere területén indított különböző kezdeményezésekről nyilvánított véleményeire ([47]), amelyek számos javaslatot és észrevételt tartalmaznak a nagy adatbázisok uniós szintű felhasználásának adatvédelmi vonatkozásairól. Egyebek között kiemelt figyelmet szentelt annak a kérdésnek, hogy erőteljes és egyénre szabott biztosítékokra

([43]) Ebben az összefüggésben a centralizált adattárolás a központi európai szintet jelenti, a decentralizált tárolás pedig a tagállami szintű tárolást.

([44]) Lásd a 33. lábjegyzetet.

([45]) A Bizottság közleménye „Az Európai Unió határigazgatása terén teendő újabb lépések előkészítéséről" címmel, 2008.2.13. COM(2008) 69.

([46]) Az adatvédelmi biztos előzetes észrevételei a határigazgatással kapcsolatos három bizottsági közleményről (COM(2008) 69, COM(2008) 68 és COM (2008) 67, 2008. március 3.: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2008/08-03-03_Comments_border_package_EN.pdf

([47]) Különösképpen: Az európai adatvédelmi biztos 2005. március 23-i véleménye a vízuminformációs rendszerről (VIS) és a rövid távú tartózkodásra jogosító vízumokra vonatkozó adatok tagállamok közötti cseréjéről szóló európai parlamenti és tanácsi rendeletre vonatkozó javaslatról (HL C 181., 2005.7.23., 13. o.), valamint az európai adatvédelmi biztos 2005. október 19-i véleménye a Schengeni Információs Rendszer (SIS II) második generációjáról szóló három javaslatról (HL C 91., 2006.4.19., 38. o.).

van szükség, valamint hogy arányos mértékű hatásvizsgálatot kell végezni, mielőtt bármiféle intézkedést javasolnának vagy hajtanának végre ezen a területen. Az európai adatvédelmi biztos mindig is hangoztatta, hogy helyes és az adatvédelemnek megfelelő egyensúlyt kell tartani a biztonsági követelmények, valamint a rendszer hatálya alá tartozó személyek magánéletének védelme között. Ugyanezt az álláspontot képviselte akkor is, amikor a rendszerek központi részét felügyelte.

73. Az európai adatvédelmi biztos továbbá megragadja ezt a lehetőséget annak hangsúlyozására, hogy a teljes uniós információcsere tekintetében egységes szemléletre van szükség, beleértve a már meglévő és a kifejlesztés alatt álló rendszerek közötti jogi, műszaki és felügyeleti összhangot. Valóban, minden eddiginél nagyobb, merész és átfogó elgondolásra van szükség azzal kapcsolatban, hogy az uniós információcserének és a jövőbeli nagymértékű információs rendszereknek milyen formát kell ölteniük. Csakis ilyen elgondolás alapján lehet ismételten mérlegelni a tagállamok területére történő belépést, illetve az onnan történő kilépést nyilvántartó elektronikus rendszert.

74. Az európai adatvédelmi biztos azt javasolja, hogy a stockholmi programban utaljanak ezen elgondolás kidolgozásának szándékára, amelyben ki kell térni a Lisszaboni Szerződés esetleges hatálybalépésére, valamint annak az első és a harmadik pillérhez tartozó jogalapokon nyugvó rendszerekre gyakorolt hatásaira.

75. Végezetül a közlemény megemlíti egy új ügynökség felállítását, amelynek – a közlemény szerint – a belépést és kilépést nyilvántartó elektronikus rendszer is a hatáskörébe tartozna. A Bizottság időközben elfogadta az új ügynökség felállításáról szóló javaslatát ([48]). Az európai adatvédelmi biztos elvben támogatja ezt a javaslatot, mert a rendszerek működését, beleértve az adatvédelmet is, hatékonyabbá teheti. Kellő időben véleményt fog nyilvánítani a javaslatról.

Az Europol és az Eurojust

76. A közlemény több helyen is megemlíti az Europol szerepét, és prioritásnak tekinti, hogy az Europol központi szerepet kapjon a koordináció, az információcsere és a szakemberképzés területén. A közlemény 4.2.2. pontja utal arra, hogy az Europol és az Eurojust közötti együttműködés jogi kerete a közelmúltban megváltozott, és bejelenti, hogy folytatódni fog az Eurojust megerősítése érdekében végzett munka, különösen a határokon átnyúló szervezett bűnözés elleni nyomozás tekintetében. Az európai adatvédelmi biztos teljes mértékben támogatja ezeket a célkitűzéseket, amennyiben megfelelő módon biztosítják az adatvédelmet.

77. Ezzel összefüggésben az európai adatvédelmi biztos üdvözli az Europol és az Eurojust közötti új megállapodásnak a közelmúltban kidolgozott tervezetét ([49]), amelynek célja a két szerv közötti kölcsönös együttműködés javítása és fokozása, valamint a közöttük folytatott hatékony információcsere biztosítása. Ebben a munkában az eredményes és hatékony adatvédelem alapvető szerepet tölt be.

VI.4. **A biometrikus adatok felhasználása**

78. Az európai adatvédelmi biztos megállapítja, hogy a közlemény nem foglalkozik azzal a kérdéssel, hogy az információcseréről szóló különböző európai uniós jogi eszközökben egyre gyakoribb a biometrikus adatok alkalmazása, beleértve a nagy méretű információs rendszerek létrehozásáról szóló eszközöket. Ez igen sajnálatos, mert adatvédelmi és magánéleti szempontból rendkívül fontos és érzékeny kérdésről van szó.

79. Bár az európai adatvédelmi biztos elismeri a biometria alkalmazásának általános előnyeit, folyamatosan hangsúlyozza, hogy az ilyen adatok felhasználása milyen jelentős hatást gyakorol az egyének jogaira, és azt javasolja, hogy minden egyes rendszerbe szigorú biztosítékokat építsenek be a biometria alkalmazására vonatkozóan. Az Emberi Jogok Európai Bíróságának az *S. and Marper kontra Egyesült Királyság* ügyben ([50]) hozott közelmúltbeli ítélete hasznos adalékokkal szolgál ezzel kapcsolatban, különös tekintettel a biometrikus adatok felhasználásának igazolására és határaira. Különösen a DNS-adatok felhasználása tárhat fel érzékeny információkat az egyénekről, figyelembe véve azt a tényt is, hogy technikailag egyre inkább lehetővé válik információ kinyerése a DNS-ből. Amennyiben az információs rendszerekben nagy mennyiségű biometrikus adatot használnak, problémát jelentenek az ezek összegyűjtésében és összehasonlításában rejlő pontatlanságok. Ezért az uniós jogalkotónak önmérsékletet kell gyakorolnia az ilyen adatok felhasználása terén.

80. Az elmúlt évek visszatérő témája a gyermekek és idősek ujjlenyomatának felhasználása az e korcsoportok esetében a biometrikus rendszerekben rejlő tökéletlenségek miatt. Az európai adatvédelmi biztos mélyreható tanulmányt kért annak érdekében, hogy helyesen határozzák meg e rendszerek pontosságát ([51]). Amennyiben a tanulmány más eredményt nem hoz, azt javasolja, hogy a gyermekek esetében a korhatárt 14 évben határozzák meg. Az európai adatvédelmi biztos azt javasolja, hogy a stockholmi program térjen ki erre a kérdésre.

([48]) A Bizottság 2009. június 24-i javaslata a Schengeni Információs Rendszer (SIS II), a Vízuminformációs Rendszer (VIS), az EURODAC, valamint a szabadságon, a biztonságon és a jog érvényesülésén alapuló térség egyéb nagyméretű IT-rendszereinek operatív irányítását végző ügynökség létrehozásáról szóló európai parlamenti és tanácsi rendeletre (COM(2009) 293/2).

([49]) A Tanács által jóváhagyott és a két fél aláírására váró megállapodástervezet. Lásd a Tanács nyilvántartását:
http://register.consilium.europa.eu/pdf/en/09/st10/st10019.en09.pdf
http://register.consilium.europa.eu/pdf/hu/09/st10/st10107.hu09.pdf

([50]) A 30562/04. és 30566/04. sz. S. and Marper kontra Egyesült Királyság egyesített ügyekben 2008. december 4-én hozott ítélet, EBHT: még nem tették közzé.

([51]) Az európai adatvédelmi biztos 2008. március 26-i véleménye a tagállamok által kiállított útlevelek és úti okmányok biztonsági jellemzőire és biometrikus elemeire vonatkozó előírásokról szóló 2252/2004/EK tanácsi rendelet módosításáról szóló rendeletjavaslatról (HL C 200., 2008.8.6., 1. o.).

81. A fentiek alapján az európai adatvédelmi biztosnak az a véleménye, hogy hasznos lenne érdemi kritériumokat kidolgozni a biometrikus adatok használatára vonatkozóan E kritériumoknak biztosítaniuk kell, hogy az adatokat kizárólag szükség esetén, helyesen és arányos mértékben használják fel, és kizárólag akkor, ha a jogalkotó bizonyította, hogy kifejezett, meghatározott és törvényes célról van szó. Egyértelműen fogalmazva, nem szabad biometrikus adatokat, különösen nem DNS-adatokat használni olyankor, ha ugyanaz az eredmény más, kevésbé érzékeny információ segítségével is megkapható.

VII. **AZ IGAZSÁGSZOLGÁLTATÁS ÉS AZ E-IGAZSÁGSZOLGÁLTATÁS IGÉNYBEVÉTELE**

82. A technológia a jobb igazságügyi együttműködést is szolgálni fogja. A közlemény 3.4.1. pontja szerint az e-igazságszolgáltatás megkönnyíti a polgárok számára az igazságszolgáltatás igénybevételét. Az e-igazságszolgáltatás egy információkat és a jogi eljárás részét képező videokonferenciákat tartalmazó portálból áll. Emellett lehetővé teszi az online jogi eljárásokat, és szerepel benne a nemzeti nyilvántartások, pl. a fizetésképtelenségi nyilvántartások összekapcsolásának terve. Az európai adatvédelmi biztos megállapítja, hogy a közlemény nem említ új kezdeményezéseket az e-igazságszolgáltatás terén, hanem a már folyamatban levő intézkedéseket erősíti meg. Az európai adatvédelmi biztos az „Úton az európai e-igazságügyi stratégia felé” című bizottsági közleményről nyilvánított, 2008. december 19-i véleményét ([52]) követően részt vesz ezen intézkedések egy részében.

83. Az e-igazságszolgáltatás teljes körű támogatást érdemlő, ambiciózus projekt. Hatékonyan javíthatja az európai igazságügyi rendszert és a polgároknak az igazságszolgáltatás általi védelmét. Emellett jelentős előrelépés az európai igazságügyi térség irányába. Szem előtt tartva ezt a kedvező értékelést, a következő néhány észrevételt lehet tenni:

— Az e-igazságszolgáltatás technológiai rendszereinek a beépített adatvédelem elvével összhangban kell kiépülniük. A korábban az európai információs modellhez kapcsolódóan elmondottaknak megfelelően, a helyes szerkezet megválasztása mindennek az alapja.

— A rendszerek összekapcsolásakor és átjárhatóságuk lehetővé tételekor be kell tartani a célok korlátozásának elvét.

— A különböző szereplők felelősségét pontosan meg kell határozni.

— Előzetesen elemezni kell, hogy az érzékeny személyes adatokat tartalmazó nemzeti nyilvántartások – pl. a fizetésképtelenségi nyilvántartások – összekapcsolása milyen következményekkel jár az egyének számára.

VIII. **ÖSSZEGZÉS**

84. Az európai adatvédelmi biztos egyetért azzal, hogy a közlemény a szabadságon, a biztonságon és a jog érvényesülésén alapuló térség jövőjének egyik kulcskérdéseként kiemelten tárgyalja az alapvető jogok védelmét, és különösen a személyes adatok védelmét. Az európai adatvédelmi biztos véleménye szerint a közlemény helyesen kíván egyensúlyt teremteni a polgárok biztonságát garantáló megfelelő eszközök iránti igény, valamint az alapvető jogaik védelme között. Elismeri, hogy a személyes adatok védelmének nagyobb hangsúlyt kellene kapnia.

85. Az európai adatvédelmi biztos teljes mértékben támogatja a közlemény 2.3. pontját, amely a Lisszaboni Szerződés hatálybalépésétől függetlenül egy átfogó adatvédelmi rendszer létrehozására szólít fel, amely az uniós hatáskörbe tartozó valamennyi területet felöleli. Ezzel összefüggésben a következőket javasolja:

— a stockholmi programban az említett átfogó rendszerre vonatkozó, világos és hosszú távú szemlélet szükségességének bejelentése;

— az e területen elfogadott intézkedések, valamint konkrét végrehajtásuk és hatékonyságuk értékelése, figyelembe véve, hogy milyen költségekkel fognak járni a magánélet védelme szempontjából és milyen hatékonysággal a bűnüldöző szervek számára;

— a stockholmi programban prioritásként egy új jogalkotási keret igényének szerepeltetése, többek között a 2008/977/IB tanácsi kerethatározat helyébe lépve.

86. Az európai adatvédelmi biztos üdvözli a Bizottság azon szándékát, hogy újólag megerősítse az adatvédelmi elveket, amelyeket össze kell kapcsolni a 2009. május 19–20-án „Személyes adatok – fokozott felhasználás, nagyobb védelem” címmel megtartott konferencián a Bizottság által bejelentett nyilvános konzultációval. Az európai adatvédelmi biztos hangsúlyozza, hogy a célok korlátozásának elve az adatvédelmi jogszabályok sarokköve, továbbá hogy azokra a lehetőségekre kell összpontosítani amelyek révén – az adatkezelők felelősségét erősítő eszközökkel – az adatvédelmi elvek alkalmazásának hatékonysága javítható.

87. A „beépített adatvédelem” és a magánéletet tiszteletben tartó technológiák az alábbiak révén mozdíthatók elő:

— Magánélet- és adatvédelmi tanúsítási rendszer mint választási lehetőség az információs rendszerek kiépítői és felhasználói számára.

— Az információs rendszerek kiépítői és felhasználói számára előírt azon jogi kötelezettség, hogy a beépített adatvédelem elvével összhangban álló rendszereket alkalmazzanak.

88. Az adatvédelem külső vetületeivel kapcsolatban az európai adatvédelmi biztos a következőket ajánlja:

— a stockholmi programban az Egyesült Államokkal és más harmadik országokkal kötendő általános adatvédelmi és adatcsere-megállapodások jelentőségének hangsúlyozása,

([52]) Az európai adatvédelmi biztos 2008. december 19-i véleménye az „Úton az európai e-igazságügyi stratégia felé” című bizottsági közleményről (HL C 128., 2009.6.6., 13. o.).

— harmadik országok és nemzetközi szervezetek összefüggésében az alapvető jogok tiszteletben tartásának, különösen pedig az adatvédelemnek az aktív előmozdítása,

— a stockholmi programban azon általános koncepció megemlítése, hogy a személyes adatok harmadik országokkal folytatott cseréje megköveteli, hogy az érintett harmadik felek biztosítsák az adatvédelem megfelelő szintjét, vagy megfelelő biztosítékokat nyújtsanak.

89. Az európai adatvédelmi biztos nagy érdeklődéssel figyeli az Európai Unió információkezelési stratégiája és az európai információs modell irányába történő előrelépéseket, és hangsúlyozza, hogy a projektekben figyelmet kell fordítani az adatvédelmi vonatkozásokra, amelyeket a stockholmi programban kell jobban kidolgozni. Az információcsere szerkezetének a „beépített adatvédelmen" és a „rendelkezésre álló legjobb technikákon" kell alapulnia.

90. Pusztán az a tény, hogy az átjárható adatbázisok között technikailag kivitelezhető a digitális információ cseréje, illetve ezek az adatbázisok egyesíthetők, nem jelenti a célok korlátozásának elve alóli kivétel igazolását. Az átjárhatóságnak konkrét esetekben világos és megfontolt politikai döntésen kell alapulnia. Az európai adatvédelmi biztos azt javasolja, hogy a stockholmi program tartalmazza ezt a gondolatmenetet.

91. A kereskedelmi célokból összegyűjtött személyes adatok bűnüldözési célú felhasználása – az európai adatvédelmi biztos véleménye szerint – kizárólag szigorú, e vélemény 65. pontjában felsorolt feltételekkel engedhető meg.

92. A személyekre vonatkozó információ felhasználásával kapcsolatos egyéb javaslatok:

— Olyan érdemi kritériumok kidolgozása, amelyek szerint választani lehetne a centralizált és a decentralizált rendszer között; a stockholmi programnak tartalmaznia kellene az ilyen kritériumok kidolgozásának szándékát.

— A tagállamok területére történő belépést, illetve az onnan történő kilépést nyilvántartó elektronikus rendszer, valamint az utas-nyilvántartási programok kidolgozását nem szabad megemlíteni a stockholmi programban.

— Az Europol és az Eurojust megerősítéséhez, valamint a közelmúltban kidolgozott, általuk kötendő új megállapodáshoz nyújtott támogatás.

— A biometrikus adatok használatára vonatkozó érdemi kritériumok kidolgozása, amelyek biztosítják, hogy az adatokat kizárólag szükség esetén, helyesen és arányos mértékben használják fel, és kizárólag akkor, ha a jogalkotó bizonyította, hogy kifejezett, meghatározott és törvényes célról van szó. A DNS-adatokat nem szabad felhasználni olyankor, ha ugyanaz az eredmény más, kevésbé érzékeny információ segítségével is elérhető.

93. Az európai adatvédelmi biztos támogatja az e-igazságszolgáltatást, és néhány észrevételt tett a projekt javításával kapcsolatban (lásd a 83. pontot).

Kelt Brüsszelben, 2009. július 10-én.

Peter HUSTINX

európai adatvédelmi biztos