

HU

HU

HU



EURÓPAI BIZOTTSÁG

Brüsszel, 2010.11.4.
COM(2010) 609 végleges

**A BIZOTTSÁG KÖZLEMÉNYE AZ EURÓPAI PARLAMENTNEK, A
TANÁCSNAK, A GAZDASÁGI ÉS SZOCIÁLIS BIZOTTSÁGNAK ÉS A RÉGIÓK
BIZOTTSÁGÁNAK**

A személyes adatok Európai Unión belüli védelmének átfogó megközelítése

A BIZOTTSÁG KÖZLEMÉNYE AZ EURÓPAI PARLAMENTNEK, A TANÁCSNAK, A GAZDASÁGI ÉS SZOCIÁLIS BIZOTTSÁGNAK ÉS A RÉGIÓK BIZOTTSÁGÁNAK

A személyes adatok Európai Unión belüli védelmének átfogó megközelítése

1. A SZEMÉLYES ADATOK VÉDELME NEK ÚJ KIHÍVÁSAI

Az 1995. évi adatvédelmi irányelv¹ mérföldkövet jelentett a személyes adatok Európai Unión belüli védelmének történetében. Az irányelv felöleli az európai integrációs folyamat két legrégebbi és egyaránt fontos törekvését: egyrészt a személyek alapvető jogainak és szabadságainak – kiváltképpen az adatvédelemhez való alapvető jognak – a védelmét, másrészt pedig a belső piac megvalósítását – jelen esetben a személyes adatok szabad áramlását.

Ötven évvel később továbbra is érvényes ez a kétirányú célkitűzés, és az irányelvbe foglalt elvek szilárd alapokon nyugszanak. **Azonban a gyors technológiai fejlődés és a globalizáció alapvetően megváltoztatta a környező világot, és új kihívásokat támasztott a személyes adatok védelme tekintetében.**

Korunk technológiája lehetővé teszi az egyének számára, hogy könnyűszerrel megosszák a magatartásukkal és preferenciáikkal kapcsolatos információkat, és minden eddiginél nagyobb mértékben, nyilvánosan és globálisan hozzáférhetővé tegyék azokat. Világszerte terjednek a több száz millió tagot számláló közösségi hálózati weboldalak, amelyek talán a legnyilvánvalóbb, bár korántsem az egyetlen példái ennek a jelenségnek. A „számítási felhő” – vagyis az olyan internet-alapú számítás, amikor a szoftver, a megosztott erőforrások és az információk egymástól távoli szervereken („a felhőben”) helyezkednek el – szintén adatvédelmi kihívásokat támaszthat, mivel ennek alkalmazásával esetleg megszűnik az egyének ellenőrzése potenciálisan érzékeny adataik felett, amikor egy másik személy számítógépén futó programok segítségével tárolják azokat. Egy nemrégiben napvilágot látott tanulmány megerősítette, hogy a jelek szerint az adatvédelmi hatóságok, az üzleti szövetségek és a fogyasztóvédelmi szervezetek álláspontja megegyezik abban, hogy az online tevékenységgel összefüggésben növekednek a magánéletet és a személyes adatok védelmét érintő kockázatok².

Ugyanakkor **a személyes adatok gyűjtését egyre kifinomultabb és egyre nehezebben felderíthető módszerekkel végzik.** A kifinomult eszközök használata lehetővé teszi például, hogy a gazdasági szereplők az egyének magatartásának nyomon követése segítségével célzottabban szólítsák meg őket. Emellett az egyre növekvő mértékben alkalmazott automatikus adatgyűjtéssel járó eljárások – így az elektronikus menetjegyváltás, útdíjbeszedés – vagy a földrajzi helymeghatározó eszközök megkönnyítik az egyes személyek földrajzi

¹ Az Európai Parlament és a Tanács 95/46/EK irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról (HL L 281., 1995.11.23., 31. o.).

² Lásd: *Study on the economic benefits of privacy enhancing technologies* (A magánélet védelmét erősítő technológiák gazdasági előnyeiről szóló tanulmány), London Economics, 2010. július, (http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf), 14. o.

helyzetének behatárolását pusztán azáltal, hogy mobil eszközt használnak. A hatóságok szintén egyre több személyes adatot használnak különféle célokból. (ilyenek például a járványos betegségek kitörése esetén az egyes személyek nyomon követése, a terrorizmus és a bűnözés elleni hatékonyabb küzdelem és megelőzés, a társadalombiztosítási rendszerek működtetése, adózási célok vagy az e-kormányzati alkalmazások részei, stb.)

Mindez elkerülhetetlenné teszi annak a kérdésnek a felvetését, hogy a meglévő uniós adatvédelmi jogszabályok továbbra is képesek-e teljes mértékben és hatékonyan kezelni az említett kihívásokat.

A fenti kérdés megválaszolása céljából a Bizottság elindította a jelenlegi jogi keret felülvizsgálatát, amely egy 2009. májusi magas szintű konferenciával kezdődött, amit 2009 végéig tartó nyilvános konzultáció követett³. Több tanulmányt is kezdeményeztünk⁴.

A megállapítások megerősítették, hogy az irányelv alapvető elvei továbbra is érvényesek, és hogy meg kell őrizni annak technológia-semleges jellegét. Mindazonáltal több problémás és sajátos kihívásokat támasztó kérdésre mutattak rá. Az alábbiak tartoznak ezek közé:

- *Az új technológiák hatásának kezelése*

A magánszemélyektől és szervezetektől a konzultációkhoz érkezett hozzászólások megerősítették, hogy tisztázni és pontosítani kell az adatvédelmi elvek alkalmazását az új technológiákra, hogy biztosítsuk az egyének személyes adatainak valóban hatékony védelmét – bármelyik technológiát alkalmazzák is azok feldolgozására –, továbbá hogy az adatkezelők teljes mértékben tisztában legyenek az új technológiák adatvédelmi vonatkozásaival. Az általános adatvédelmi irányelvet az elektronikus hírközlési ágazatban⁵ tekintetében részletező és kiegészítő 2002/58/EK irányelv (az úgynevezett e-magánélet irányelv)⁶ részben orvosolta ezt a problémát.

³ A Bizottság nyilvános konzultációjára érkezett válaszok az alábbi internetcímen érhetők el: http://ec.europa.eu/justice/news/consulting_public/news_consulting_0003_en.htm. 2010 folyamán célzottabb konzultációt folytattak az érdekeltekkel. Emellett 2010. október 5-én Brüsszelben az érdekeltek bevonásával sor került egy magas szintű ülésre, amelyen Viviane Reding alelnök elnökölt. A Bizottság konzultációt folytatott a 29. cikk alapján létrehozott munkacsoporttal is, amely átfogó hozzájárulást nyújtott a 2009-es konzultációhoz (WP 168). és 2010. júliusában az elszámoltathatóság fogalmáról szóló külön véleményt (WP 173) fogadott el.

⁴ *A magánélet védelmét erősítő technológiák gazdasági előnyeiről szóló tanulmány* (id.: 2. lábjegyzet) mellett lásd még az alábbi tanulmányt: *Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments (A magánéletet – különösen a technológiai fejlődés következtében – fenyegető új kihívások eltérő megközelítéseiről szóló összehasonlító tanulmány)* 2010. január (http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf). A személyes adatok védelmére vonatkozó jövőbeni uniós jogi keret hatásvizsgálatáról szóló tanulmány elkészítése folyamatban van.

⁵ A 95/46/EK adatvédelmi irányelv valamennyi uniós jogszabályra – így (a 2009/136/EK irányelvvel [HL L 337., 2009.12.28., 1. o.] módosított) 2002/58/EK e-magánélet irányelvre – nézve meghatározza az adatvédelmi normákat. A e-magánélet irányelv a nyilvános hírközlő hálózatokon nyilvánosan hozzáférhető elektronikus hírközlési szolgáltatások nyújtásával összefüggő személyesadat-feldolgozásra vonatkozik. E jogszabály az elektronikus hírközlési ágazatra vonatkozó különös szabályokat határozza meg az adatvédelmi irányelvben megfogalmazott elvek alapján. A 95/46/EK irányelv többek között a nem nyilvános hírközlési szolgáltatásokra is alkalmazandó.

⁶ Az Európai Parlament és a Tanács 2002/58/EK irányelve (2002. július 12.) az elektronikus hírközlési ágazatban a személyes adatok feldolgozásáról és a magánélet védelméről (Elektronikus hírközlési adatvédelmi irányelv) (HL L 201., 2002.7.31., 37. o.).

- *Az adatvédelem belső piaci dimenziójának erősítése*

Az érdekeltek – kiváltképpen a multinacionális vállalatok – egyik legfontosabb, állandó aggálya, hogy a közös uniós jogi keret ellenére a tagállamok adatvédelmi jogszabályai nincsenek megfelelően összehangolva. Hangsúlyozták a jogbiztonság erősítésének, az adminisztratív teher csökkentésének, valamint a gazdasági szereplők és egyéb adatkezelők közötti egyenlő feltételek biztosításának szükségességét.

- *A globalizáció problémájának kezelése és a nemzetközi adattovábbítás javítása*

Több érdekelt rámutatott, hogy az adatfeldolgozás növekvő mértékű – és igen gyakran az Unión kívülre történő – kiszervezése több problémát is felvet az adatfeldolgozásra alkalmazandó joggal és az ahhoz társuló felelősség megosztásával kapcsolatban. Ami a nemzetközi adattovábbítást illeti, sok szervezet szerint a jelenlegi szabályozások nem teljes mértékben megfelelőek, ezért az adattovábbítás egyszerűsítése és nehézségének csökkentése céljából felül kell vizsgálni és korszerűsíteni kell azokat.

- *Erősebb intézményi struktúra biztosítása az adatvédelmi szabályok hatékony érvényesítése céljából*

Az érdekeltek egyetértenek abban, hogy az adatvédelmi szabályok jobb érvényesítése céljából meg kell erősíteni az adatvédelmi hatóságok szerepét. Néhány szervezet emellett sürgette, hogy fokozzák a 29. cikk alapján létrehozott munkacsoport munkájának áttekinthetőségét (lásd a lenti 2.5. pontot), és tisztázzák annak feladatait és hatáskörét.

- *Az adatvédelmi jogi keret következetességének javítása*

A nyilvános konzultáció során az összes érdekelt kiemelte, hogy az integrált megközelítés, valamint a folyamatos, következetes és hatékony adatvédelem érdekében olyan átfogó jogi aktusra van szükség, amely az összes ágazatban és uniós szakpolitikai területen végzett adatfeldolgozási műveletre alkalmazandó⁷.

A fenti kihívások **megkövetelik, hogy az Unió átfogó és következetes megközelítést dolgozzon ki, amely az Unió határain belül is azon túl is garantálja az egyének adatvédelméhez fűződő alapvető jogának teljes körű tiszteletben tartását.** A Lisszaboni Szerződés további eszközöket biztosított az Unió számára ennek megvalósításához: az EU Alapjogi Chartája – amelynek 8. cikke önálló jogként ismeri el a személyes adatok védelmét – jogilag kötelezővé vált, továbbá olyan új jogalapot foglaltak bele a Szerződésbe⁸, amely lehetővé teszi a személyes adatok feldolgozása és az ilyen adatok szabad áramlása tekintetében az egyének védelmére vonatkozó átfogó és következetes uniós jogszabályok elfogadását. Az új jogalap először is lehetőséget ad arra, hogy az EU a büntetőügyekben folytatott rendőrségi és igazságügyi együttműködésre is kiterjedő, egységes jogi aktust fogadjon el az adatvédelem szabályozására. Az EUMSz. 16. cikke a közös kül- és

⁷ A nyilvános konzultáció befejezését követően tett külön hozzászólásaikban az Europol és az Eurojust mindazonáltal azt kérte, hogy vegyék figyelembe a bűnüldözési és bűnmegelőzési koordináció terén végzett munkájuk sajátosságait.

⁸ Lásd az Európai Unió működéséről szóló szerződés (EUMSz.) 16. cikkét.

biztonságpolitikára csak részben terjed ki, mivel a tagállamok általi adatfeldolgozásra vonatkozó különös szabályokat eltérő jogalapra épülő tanácsi határozattal kell megállapítani⁹.

Az említett új jogi lehetőségek alapján a Bizottság kiemelt prioritásként fogja kezelni, hogy az egész Unióban, az összes szakpolitikája terén betartassa az adatvédelemhez való alapvető jogot, miközben megerősíti a belső piaci dimenziót és elősegíti a személyes adatok szabad áramlását. A fentiek keretében a Chartába foglalt más kapcsolódó alapjogokat és a Szerződések egyéb célkitűzéseit teljes mértékben figyelembe kell venni a személyes adatok védelméhez való alapvető jog biztosítása során.

E 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 korszerűsítésére irányuló bizottsági megközelítést, amely arra irányul, hogy továbbra is garantálja az egyének magas szintű védelmét személyes adataik feldolgozása tekintetében az Unió valamennyi cselekvési területén. Mindez lehetővé teszi, hogy az EU a jövőben is világszerte vezető szerepet játsszon a magas szintű adatvédelmi normák előmozdításában.

2. AZ ÁTFOGÓ ADATVÉDELMI MEGKÖZELÍTÉS LEGFONTOSABB CÉLKITŰZÉSEI

2.1. A személyek jogainak erősítése

2.1.1. Az egyének megfelelő védelmének biztosítása minden körülmények között

A jelenlegi uniós adatvédelmi jogszabályokba foglalt szabályok célja **a természetes személyek alapvető jogainak – így különösen a személyes adatok védelméhez való jogának – védelme**, összhangban az EU Alapjogi Chartával¹⁰.

A „személyes adat” a jelenlegi uniós adatvédelmi jogszabályok egyik legfontosabb egyének védelmére irányuló fogalma, amely maga után vonja az adatkezelőket és az adatfeldolgozókat terhelő kötelezettségek alkalmazását¹¹. A „személyes adat” fogalommeghatározásának az a célja, hogy lefedjen minden olyan információt, amely – akár közvetlenül, akár közvetve – valamely azonosított vagy azonosítható személlyel kapcsolatos. Annak meghatározására, hogy egy személy azonosítható-e vagy sem, számba kell venni „minden lehetséges eszközt, amely valószínűsíthetően az adatkezelő vagy bármely más személy által az említett személy azonosítására indokoltan felhasználható”¹². A jogalkotó által választott ilyen körülmények megközelítés a rugalmasság előnyével jár, lehetővé téve, hogy a fogalmat az alapvető jogokat érintő különféle helyzetek és fejlemények esetén alkalmazzák, ideértve azokat is, amelyek az irányelv elfogadásakor nem voltak előre láthatók. Azonban az ennyire tág és rugalmas megközelítés következtében számos olyan eset is előáll, amikor nem mindig egyértelmű, hogy

⁹ Lásd az EUMSZ. 16. cikke (2) bekezdésének utolsó albekezdését, valamint az Európai Unióról szóló szerződés 39. cikkét.

¹⁰ Lásd az Európai Bíróság esetében a C-101/01. sz. Bodil Lindqvist ügyben [EBHT 2003., I-1297. o.] hozott ítélet 96. és 97. pontját, valamint a C-275/06. sz. Productores de Música de España (Promusicae) kontra Telefónica de España SAU [EBHT 2008., I-271. o.] ügyet. Lásd továbbá az Emberi Jogok Európai Bíróságának ítélkezési gyakorlatát pl. az alábbi ügyekben: S. és Marper kontra Egyesült Királyság, 2008.12.4. (30562/04. és 30566/04. sz. keresetek) ügy, valamint a Rotaru kontra Románia ügyben hozott 2000. május 4-i 28341/95. sz. ítélet 55. pontja, Ítéletek és határozatok tára 2000-V.

¹¹ Az „adatkezelő” és az „adatfeldolgozó” fogalma megtalálható a 95/46/EK irányelv 2. cikkének d) és e) pontjában.

¹² Lásd a 95/46/EK irányelv (26) preambulumbekzdését

az irányelv végrehajtása során melyik megközelítést kell választani, és az egyének rendelkeznek-e adatvédelmi jogosultságokkal, továbbá hogy az adatkezelőknek meg kell-e felelniük az irányelvben megszabott kötelezettségeknek¹³.

Előfordulnak olyan helyzetek, amikor sajátos információk feldolgozása az uniós jog szerinti, további intézkedéseket tennie szükségessé. Néhány esetben már most is léteznek ilyen intézkedések. Például (pl.: a mobiltelefonok) végberendezéseiben csak az érintett személyek hozzájárulásával tárolhatók adatok. Az alábbi információk tekintetében is uniós szintű szabályozás válhat szükségessé: a kódolt adatok, a földrajzi helymeghatározási adatok, a különböző forrásokból származó adatok kombinálását lehetővé tévő „adatbányászati” technológiák, illetve olyan helyzetek, amikor biztosítani kell az informatikai rendszerek titkosságát és integritását¹⁴.

Ezért az összes említett kérdés körültekintő vizsgálatot igényel.

A Bizottság mérlegelni fogja, hogy az új technológiáknak az egyének jogaira és szabadságaira gyakorolt hatását, és a személyes adatok belső piacon való szabad áramlásának biztosítására vonatkozó célkitűzést szem előtt tartva hogyan biztosítható az adatvédelmi szabályok következetes alkalmazása.

2.1.2. Az átláthatóság növelése az érintettek számára

Az átláthatóság az alapfeltétele annak, hogy az egyének ellenőrzést gyakorolhassanak saját adataik felett és biztosíthassák a személyes adatok hatékony védelmét. Ezért lényeges, hogy az adatkezelők **áttekinthető módon, megfelelő és világos tájékoztatást nyújtsanak** az érintett személyeknek arról, hogy adataik összegyűjtését és feldolgozását ki, hogyan, mely okból és milyen hosszú ideig végzi, továbbá hogy milyen jogokkal rendelkeznek, amennyiben hozzá kívánnak férni az adataikhoz, vagy kijavítani, illetve törölni szeretnék azokat. Az érintetteknek nyújtandó tájékoztatásra vonatkozó rendelkezések¹⁵ nem elégségesek.

Az átláthatóság alapvető részét jelenti az a követelmény, hogy **a tájékoztatásnak egyszerűen hozzáférhetőnek és könnyen érthetőnek kell lennie, valamint világos és közérthető nyelven** kell azt megfogalmazni. Mindez különösen fontos az online környezetben, ahol az adatvédelmi nyilatkozatok gyakran homályosak, nehezen hozzáférhetőek, áttekinthetetlenek¹⁶ és nem minden esetben felelnek meg teljes mértékben a meglévő szabályoknak. Igaz lehet ez a viselkedésalapú online reklám esetében, ahol a viselkedésalapú reklámtevékenységben részt vevő szereplők nagy száma és e gyakorlat technológiai bonyolultsága egyaránt megnehezíti az egyén számára annak megismerését és megértését, hogy amennyiben gyűjtik a személyes adatait, ki és milyen céllal teszi ezt.

¹³ Lásd például az IP-címek ügyét, amelyet a 29. cikk alapján létrehozott munkacsoport a személyes adat fogalmáról szóló 4/2007 véleményében (WP 136) vizsgált meg.

¹⁴ Lásd például a Német Szövetségi Alkotmánybíróság (Bundesverfassungsgericht) 2008. február 27-i ítéletét, 1 BvR 370/07.

¹⁵ Lásd a 95/46/EK irányelv 10. és 11. cikkét

¹⁶ Egy 2009-ben végzett Eurobarométer felmérés azt mutatta, hogy a válaszadók fele szerint a weboldalakon található adatvédelmi nyilatkozatok „nagyon” vagy „meglehetősen homályosak” (lásd a 282. sz. Eurobarométer gyorsfelmérést: http://ec.europa.eu/public_opinion/flash/fl_282_en.pdf).

E tekintetben különös védelmet kell biztosítani a **gyermeknek**, mivel ők kevésbé lehetnek tisztában a személyes adatok feldolgozásának kockázataival, következményeivel és az arra vonatkozó biztosítékokkal és jogosultságokkal¹⁷.

A Bizottság mérlegelni fogja az alábbiakat:

- a **személyes adatok átlátható feldolgozásának általános elvét** beilleszti a jogi keretbe;
- **konkrét kötelezettségeket** ró az adatkezelőkre a nyújtandó tájékoztatás típusa és a – többek között a **gyermekkel** kapcsolatos – tájékoztatásadás **módja** vonatkozásában;
- egy vagy több, adatkezelők által alkalmazandó **uniós formanyomtatványt („adtvédelmi nyilatkozatokat”)** készít.

Fontos továbbá, hogy tájékoztassák az érintett személyeket, ha adataikat véletlenül vagy jogellenesen megsemmisítik, ellopják, megváltoztatják, illetve ha jogosulatlan személyek hozzáférnek azokhoz vagy pedig felfedik azokat ilyen személyek számára. Az e-magánélet irányelv közelmúltbeli felülvizsgálata bevezette a **személyes adatok megsértésének kötelező bejelentését**, amely azonban csak a hírközlési ágazatra terjed ki. Mivel más ágazatokban (pl.: a pénzügyi szektorban) is fennáll az adatsértés veszélye, a Bizottság megvizsgálja, hogy milyen módon terjeszthető ki egyéb ágazatokra a személyes adatok megsértésére vonatkozó bejelentési kötelezettség, összhangban az elektronikus hírközlés szabályozási keretének reformjával összefüggésben az adatsértések bejelentésére vonatkozóan az Európai Parlament előtt tett 2009. évi bizottsági nyilatkozattal¹⁸. Ez a vizsgálat nem érinti az e-magánélet irányelv rendelkezéseit, amelyeket 2011. május 25-ig át kell ültetni a nemzeti jogba¹⁹. E tárgyban biztosítani kell a következetes és egységes megközelítést.

A Bizottság:

- megvizsgálja, hogy a **személyes adatok megsértésének általános bejelentése** milyen módon illeszthető be a jogi keretbe, ideértve az ilyen bejelentések címzettjeit és a bejelentési kötelezettséget keletkeztető kritériumokat.

¹⁷ Lásd a 9-10 és 12-14 éves gyermekekre vonatkozó Biztonságosabb internetet a gyermekeknek elnevezésű kvalitatív tanulmányt, amely azt mutatta, hogy a gyermekek hajlamosak alábecsülni az internet használatával kapcsolatos kockázatokat és lekicsinyelni a kockázatos viselkedés következményeit (a tanulmány az alábbi internetcímen érhető el:

http://ec.europa.eu/information_society/activities/sip/surveys/qualitative/index_en.htm).

¹⁸ „A Bizottság tudomásul veszi az Európai Parlament azon törekvését, hogy a személyes adatok megsértése esetén fennálló tájékoztatási kötelezettség ne csak az elektronikus hírközlési ágazatra korlátozódjon, hanem olyan szereplőkre is vonatkozzon, mint például az információs társadalommal összefüggő szolgáltatásokat nyújtó jogi személyek [...]. A Bizottság ezért késedelem nélkül kezdeményezni fogja a megfelelő előkészítő munkát, beleértve az érintettekkel való konzultációt is, annak érdekében, hogy e területen - szükség szerint - javaslatokat terjesszen elő 2011 végéig [...]”, hozzáférhető az alábbi internetcímen: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2009-0360+0+DOC+XML+V0//HU> Lásd továbbá a 2002/58/EK e-magánélet irányelvet módosító 2009/136/EK irányelv (59) preambulumbekzdését: „A felhasználóknak ez a tájékoztatásra vonatkozó általános érdeke egyáltalán nem korlátozódik az elektronikus hírközlési ágazatra, éppen ezért közösségi szinten kiemelkedő fontosságúnak kell tekinteni a kifejezett, kötelező és minden ágazatra és az információs társadalommal összefüggő szolgáltatások szolgáltatóira kiterjedő tájékoztatási kötelezettség szükségességét is ideértve.”

¹⁹ A 2009/136/EK irányelv 4. cikke.

2.1.3. A saját adatok ellenőrzésének erősítése

Az egyének az alábbi két fontos előfeltétel megvalósulása esetén élvezhetnek magas szintű adatvédelmet: **az adatkezelő feldolgozási tevékenységének korlátozása annak célja szerint (az adatminimalizálás elve)**, továbbá az érintettek részéről **a saját adataik feletti hatékony ellenőrzés** megőrzése. A Charta 8. cikkének (2) bekezdése kimondja, hogy „Mindenkinek joga van ahhoz, hogy a róla gyűjtött adatokat megismerje, és joga van azokat kijavíttatni.” Az érintett személyeknek minden esetben képesnek kell lenniük az adataikhoz hozzáférni, azokat kijavítani, törölni vagy letiltani, kivéve amennyiben jogszabályban előírt jogos okokból nem teszik azt lehetővé. Az említett jogok már a jelenlegi jogi keretben is léteznek. Azonban e jogok gyakorlásának módját nem egységesítették, ezért egyes tagállamokban a többenél könnyebben gyakorolhatók. Emellett különösen nagy kihívást jelent mindez az online környezetben, ahol gyakran anélkül őrzik meg az adatokat, hogy az érintett személyt tájékoztatnák erről és/vagy megkapták volna a hozzájárulását.

Az online közösségi hálózatok kiváltképpen szemléletes példát nyújtanak erre, hiszen ezek esetében különösen nagy kihívást jelent az egyének számára, hogy hatékony ellenőrzést gyakoroljanak személyes adataik felett. A Bizottság különféle kérdéseket kapott olyan személyektől, akik nem minden esetben tudtak hozzáférést szerezni a személyes adataikhoz (pl.: a fényképeikhez) az online szolgáltatóknál, tehát akadályozták őket a hozzáféréshez, kijavításhoz és törléshez való jogosultságuk gyakorlásában.

Ezért nyilvánvalóbbá, egyértelműbbé, és lehetőség szerint erősebbé kell tenni ezeket a jogosultságokat.

Ennélfogva a Bizottság megvizsgálja, hogy milyen módon valósíthatók meg az alábbiak:

- az **adatminimalizálás elvének** megerősítése;
- **az adatokhoz való hozzáférési, kijavítási, törlési és letiltási jogok** tényleges **gyakorlására vonatkozó szabályok javítása** (pl.: az egyéni megkeresések esetén válaszadási határidő bevezetésével, az elektronikus eszközök révén történő joggyakorlás engedélyezésével, vagy annak előírásával, hogy a hozzáférési jogot fő szabályként térítésmentesen kell biztosítani);
- a személyes adatok tárolásának megszüntetéséhez való jog („**right to be forgotten**”), vagyis a személyek azon jogának tisztázása, hogy töröljék az adatait vagy megszüntessék azok feldolgozását, amennyiben már nem szükségesek a jogszerű célokhoz. Ez a helyzet áll elő például akkor, ha a feldolgozás az érintett személy hozzájárulásán alapul és az illető visszavonja a hozzájárulását, vagy ha letelt az engedélyezett adattárolási idő;
- az érintettek jogainak kiegészítése az „**adathordozhatóság**” biztosításával, vagyis megadva az egyéneknek azt a kifejezett jogosultságot, hogy – amennyiben műszakilag megvalósítható – az adatkezelők általi akadályoztatás nélkül visszavonhassák adataikat (pl.: fényképeiket, barátaik listáit) egy alkalmazásból vagy szolgáltatástól abból a célból, hogy a visszavont adatokat átviessék egy másik alkalmazásba vagy szolgáltatásba.

2.1.4. A tudatosság fokozása

Jóllehet az átláthatóság rendkívül lényeges, arra is szükség van, hogy a közvélemény – és különösen a fiatalok – jobban ismerjék a személyes adatok feldolgozásával kapcsolatos kockázatokat és a jogaikat. Egy 2008. évi Eurobarométer felmérés kimutatta, hogy az uniós tagállamok lakosságának nagy többsége úgy véli, hogy a saját országában keveset tudnak a

személyes adatok védelméről²⁰. Tehát a szereplők szélesebb körének (pl.: a tagállami hatóságoknak, különösen az adatvédelmi hatóságoknak és az oktatási szervezeteknek, valamint az adatkezelőknek és a civil társadalmi egyesületeknek) kell ösztönöznie és elősegítenie a tudatosság fokozására irányuló tevékenységeket. Ezeknek nem jogalkotási intézkedéseket is fel kell ölelniük (pl.: felvilágosító kampányok a nyomtatott és az elektronikus médiában, valamint egyértelmű információk közzététele a weboldalakon, az érintettek jogainak és az adatkezelők kötelezettségeinek világos kifejtésével).

A Bizottság megvizsgálja:

- annak lehetőségét, hogy **az adatvédelemről szóló ismeretterjesztő kampányokat** az uniós költségvetésből **társfinanszírozzák**;

- annak szükségességét és lehetőségét, hogy az e területre vonatkozó **tudatosságerősítő tevékenység végzésére vonatkozó kötelezettséget** foglaljanak bele a jogi keretbe.

2.1.5. *A tájékozottságon alapuló és önkéntes beleegyezés biztosítása*

A jelenlegi szabályok szerint, amennyiben tájékozottságon alapuló beleegyezést írnak elő, az érintett személy kívánságának „önkéntes, kifejezett és tájékozott kinyilvánítása” szükséges, amellyel beleegyezését adja személyes adatainak feldolgozásához²¹. A tagállamok azonban jelenleg különféleképpen értelmezik az említett feltételeket. Az értelmezések az általánosan megkövetelt írásbeli hozzájárulástól a hallgatóságos beleegyezés elfogadásáig terjednek.

Ezen felül az online környezetben az adatvédelmi politikák homályossága miatt gyakran még nagyobb nehézséget okoz az érintetteknek, hogy megismerjék a jogukat és tájékozott beleegyezést adjanak. Még bonyolultabbá teszi a helyzetet, hogy némely esetben az sem világos, hogy mi számít az adatfeldolgozásba való önkéntes, kifejezett és tájékozott beleegyezésnek. Ilyen például a viselkedésalapú reklámozás, amelynek esetében vannak olyanok, akik a felhasználói beleegyezés kinyilvánításának tekintik az internetes böngésző beállításait, mások pedig nem.

Tehát tisztázni kell az érintett beleegyezésének feltételeit annak érdekében, hogy mindig garantálhassuk a tájékozott beleegyezést és azt, hogy az érintett – az EU Alapjogi Chartája 8. cikkének megfelelően – teljes mértékben tisztában legyen azzal, hogy beleegyezést ad, és tudja, hogy mely adatok feldolgozásához járul hozzá. Az alapvető fogalmak tisztázása elősegíti továbbá az uniós joggal összhangban álló gyakorlati megoldások kidolgozására irányuló önszabályozási kezdeményezések kialakítását.

A Bizottság megvizsgálja, hogy milyen módon **tisztázhatók és erősíthetik a beleegyezésre vonatkozó szabályok**.

2.1.6. *Az érzékeny adatok védelme*

Az érzékeny adatok, vagyis a faji vagy etnikai hovatartozásra, a politikai véleményre, a vallási vagy világnézeti meggyőződésre, a szakszervezeti tagságra utaló adatok, valamint az egészségi állapotra vagy a szexuális életre vonatkozó adatok feldolgozása – néhány, megfelelő feltételekhez és biztosítékokhoz kötött, korlátozott kivételtől eltekintve –

²⁰ Lásd: 225. sz. Eurobarométer gyorsfelmérés – Adatvédelem az Európai Unióban: http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf.

²¹ Vö.: a 95/46/EGK irányelv 2. cikkének h) pontjával.

főszabályként már jelenleg is tilos²². Mindazonáltal a technológiai és az egyéb társadalmi fejlődés fényében újra kell gondolni az érzékeny adatokra vonatkozó meglévő rendelkezéseket, és meg kell vizsgálni, hogy szükséges-e kiterjeszteni azokat további adatkategoriákra, valamint tovább kell pontosítani azok feldolgozásának feltételeit. Ez például a genetikai adatokra vonatkozik, amelyeket jelenleg nem említene kifejezetten az érzékeny adatok kategóriájában.

A Bizottság mérlegelni fogja az alábbiakat:

- fel kell-e venni az „**érzékeny adatok**” közé egyéb adatkategoriákat, így például a **genetikai adatokat**;
- az érzékeny adatok feldolgozása engedélyezési **feltételeinek** további pontosítása és **harmonizálása**.

2.1.7. A jogorvoslatok és szankciók hatékonyságának növelése

Az adatvédelmi szabályok érvényesítéséhez elengedhetetlenül szükségesek a **jogorvoslatokra és a szankciókra vonatkozó hatékony rendelkezések**. Az adatvédelmi szabályok megsértése sok esetben nem csupán egy konkrét személyt érint, hanem számos olyan egyéb személyt is, akik hasonló helyzetben vannak.

A Bizottság ezért:

- mérlegeli annak lehetőségét, hogy **a tagállami bíróság előtti keresetindítási jogot kiterjessze** az adatvédelmi hatóságokra és a civil társadalmi egyesületekre, valamint **az érintettek érdekeit képviselő egyéb egyesületekre**;
- vizsgálja, hogy szükség van-e **a szankciókra vonatkozó meglévő rendelkezések erősítésére**, például oly módon, hogy a hatékonyság növelése érdekében súlyos adatvédelmi jogsértések esetén kifejezetten büntetőjogi szankciókat vezetnek be.

2.2. A belső piaci dimenzió erősítése

2.2.1. A jogbiztonság erősítése és az egyenlő feltételek biztosítása az adatkezelők számára

Az Unión belüli adatvédelem **erős belső piaci dimenzióval rendelkezik**, vagyis a belső piacon biztosítani kell a személyes adatok tagállamok közötti szabad áramlását. Ennek megfelelően a tagállami adatvédelmi jogszabályokat összehangoló irányelv nem korlátozódik minimális mértékű harmonizációra, hanem annak lényegében teljes harmonizációt kell eredményeznie²³.

Ugyanakkor az irányelv bizonyos területeken hagy mérlegelési mozgásteret a tagállamok számára, és felhatalmazza azokat a különleges helyzetekre vonatkozó egyedi szabályozás fenntartására és bevezetésére²⁴. Mindennek következtében – és az irányelv tagállamok általi, esetenként helytelen átültetése miatt – **eltérések keletkeztek az irányelvet átültető nemzeti jogszabályok között, ami ellentétes a jogi aktus egyik legfontosabb célkitűzésével, vagyis a személyes adatok belső piacon való szabad áramlásának biztosításával**. Így van ez

²² Vö. a 95/46/EGK irányelv 8. cikkével.

²³ Az Európai Bíróság C-101/01. sz. Bodil Lindqvist ügyben [EBHT 2003., I-1297. o.] hozott ítéletének 96. és 97. pontja.

²⁴ u.a. 97. pont. Lásd továbbá a 95/46/EK irányelv (9) preambulumbekzdését.

számos ágazatban és összefüggésben, pl. a foglalkoztatással összefüggő vagy közegészségügyi célú személyesadat-feldolgozás során. A harmonizáció hiánya a magánérdekeltek – kiváltképpen a gazdasági szereplők – által ismételt megemlítet egyik legfontosabb probléma, amely többletköltségeket és adminisztratív terhet okoz a számukra. Mindez különösen igaz a több tagállamban letelepedett adatkezelőkre, amelyek az érintett országok mindegyikében kötelesek megfelelni a követelményeknek és a gyakorlatoknak. Ezen felül az irányelv eltérő tagállami végrehajtása nem csupán az adatkezelőknek okoz jogi bizonytalanságot, hanem az érintettek számára is, és ezáltal torzíthatja az irányelv révén megvalósítandó és biztosítandó azonos szintű védelmet.

A Bizottság megvizsgálja az uniós szintű adatvédelmi szabályok további harmonizálásának megvalósítására szolgáló eszközöket.

2.2.2. Az adminisztratív teher csökkentése

Az egyenlő feltételek biztosítása révén csökkenni fog az eltérő nemzeti követelményeknek való megfelelés iránti igény, és ily módon jelentősen mérséklődik az adatkezelőkre nehezedő adminisztratív teher. **A mostani bejelentési rendszer felülvizsgálata és egyszerűsítése**²⁵ lehetne a következő konkrét lépés az adatkezelők adminisztratív terheinek és költségeinek mérséklése terén. Az adatkezelők között általános az egyetértés, hogy meglehetősen terhes, és önmagában véve nem biztosít valódi hozzáadott értéket az érintettek személyes adatainak védelme terén az a jelenlegi általános kötelezettség, miszerint valamennyi adatfeldolgozást be kell jelenteni az adatvédelmi hatóságok számára. Emellett ez az egyik olyan terület, ahol az irányelv bizonyos mérlegelési mozgásteret hagy a tagállamok számára, amelyek szabadon dönthetnek az esetleges kivételekről és egyszerűsítésekről, valamint a követendő eljárásról.

A harmonizált és egyszerűsített rendszer mérsékelné a költségeket, valamint az adminisztratív terheket, kiváltképpen a több tagállamban letelepedett multinacionális vállalatok számára.

A Bizottság megvizsgálja a jelenlegi bejelentési rendszer egyszerűsítésének és harmonizálásának különféle lehetőségeit, az egész EU-ra kiterjedő, egységes regisztrációs űrlap elkészítését is beleértve.

2.2.3. Az alkalmazandó jogra és a tagállamok felelősségére vonatkozó szabályok tisztázása

Az adatvédelmi irányelv végrehajtásáról szóló, első bizottsági jelentés²⁶ már 2003-ban rámutatott, hogy az alkalmazandó jogra vonatkozó rendelkezések²⁷ „több esetben hiányosak, aminek következtében olyan fajta kollízió alakulhat ki, amelynek elkerülésére e cikk törekszik”. Azóta nem javult a helyzet, és ennek következtében nem mindig egyértelmű az adatkezelők és az adatvédelmi felügyelő hatóságok számára, hogy amennyiben több tagállam is érintett, melyik a felelős tagállam, és melyik jogot kell alkalmazni. Mindez különösen igaz akkor, ha különböző tagállamok eltérő követelményei vonatkoznak az adatkezelőre, amennyiben egy multinacionális vállalat egynél több tagállamban telepedett le, illetve ha az adatkezelő nem telepedett le az EU területén, viszont uniós lakosok számára nyújtja a szolgáltatásait.

²⁵ Lásd a 95/46/EK irányelv 18. cikkét

²⁶ A Bizottság jelentése – Első jelentés az adatvédelmi irányelv (95/46/EK) végrehajtásáról (COM (2003) 265.

²⁷ Lásd a 95/46/EK irányelv 4. cikkét.

A globalizáció és a technológiai fejlődés szintén hozzájárul a helyzet egyre bonyolultabbá válásához: az adatkezelők növekvő mértékben terjesztik ki tevékenységüket több tagállamra és országra, és a nap 24 órájában nyújtanak szolgáltatásokat és támogatást. Az internet nagyon megkönnyíti az Európai Gazdasági Térségen (a továbbiakban: EGT)²⁸ kívül letelepedett adatkezelőknek, hogy távolról nyújtsanak szolgáltatásokat és az online környezetben személyes adatokat dolgozzanak fel; továbbá gyakorta nehezen állapítható meg, hogy a személyes adatok hol helyezkednek el, és az adott időpontban melyik eszközt alkalmazzák (pl.: a „számítási felhő” alkalmazásai és szolgáltatásai).

A Bizottság mindazonáltal úgy véli, hogy az érintettek nem foszthatók meg az EU Alapjogi Chartája és az uniós adatvédelmi jogszabályok alapján őket megillető védelemtől amiatt, hogy a személyes adatok feldolgozását harmadik országban letelepedett adatkezelő végzi.

A Bizottság megvizsgálja, miként kell **felülvizsgálni és tisztázni az alkalmazandó jogra vonatkozó meglévő rendelkezéseket**, köztük a felelős tagállam meghatározására vonatkozó kritériumokat annak érdekében, hogy javítsa a jogbiztonságot, tisztázza az adatvédelmi szabályok alkalmazásáért viselt tagállami felelősséget, és végső soron azonos szintű védelmet biztosítson az uniós érintettek számára, függetlenül az adatkezelő földrajzi helyétől.

2.2.4. Az adatkezelők felelősségének erősítése

Az adminisztratív egyszerűsítés következtében **nem mérséklődhet az adatkezelő átfogó felelőssége a hatékony adatvédelem biztosításáért.** Éppen ellenkezőleg, a Bizottság véleménye szerint a jogi keretnek még egyértelműbben meg kell határoznia a kötelezettségeket, amelyek többek között a belső kontroll mechanizmusra és az adatvédelmi felügyelő hatóságokkal való együttműködésre is kiterjednek. Emellett biztosítani kell, hogy ez a felelősség vonatkozzon a szakmai titoktartási kötelezettség alá tartozó adatkezelőkre (pl.: ügyvédek), valamint arra az egyre általánosabbá váló esetre is, amikor az adatkezelők az adatfeldolgozást más szervezetekre (pl.: adatfeldolgozók) ruházzák át.

A Bizottság ezért megvizsgálja, miként **biztosítható, hogy az adatkezelők hatékony politikákat és mechanizmusokat hozzanak létre az adatvédelmi szabályok betartása érdekében.** Ennek során figyelembe vesszük az elszámoltathatóság („accountability”) elvének esetleges bevezetéséről most zajló vitát²⁹. Ez nem az adatkezelők adminisztratív terheinek növelésére irányulna, mivel ezen intézkedések inkább olyan biztosítékok és mechanizmusok kialakítását helyezik előtérbe, amelyek révén hatékonyabban teljesülnek az adatvédelmi előírások, miközben egyes adminisztratív formalitások – pl.: a bejelentések (*lásd a fenti 2.2.2. pontot*) – csökkennek és egyszerűbbé válnak.

Ebben a tekintetben – pl. az adatbiztonság biztosítása terén – jelentős szerepet játszhatnak az adatvédelmet erősítő technológiák (amint arra az e témáról szóló 2007. évi bizottsági közlemény is rámutatott), valamint a „beépített adatvédelem” („privacy by design”) elve³⁰.

²⁸ Az Európai Gazdasági Térség Norvégiára, Liechtensteinre és Izlandra is kiterjed.

²⁹ Lásd elsősorban a 29. cikk alapján létrehozott munkacsoport július 13-án elfogadott 3/2010. sz. véleményét.

³⁰ Az adatvédelmet erősítő technológiákról lásd az alábbi dokumentumot: „A Bizottság Közleménye az Európai Parlamentnek és a Tanácsnak az adatvédelemnek a magánélet védelmét erősítő technológiák által történő ösztönzéséről” – COM(2007) 228. A „beépített adatvédelem” elve azt jelenti, hogy a magánélet és az adatok védelme a technológiák teljes életciklusába bele van ágyazva, a tervezési szakasztól a bevezetésen és alkalmazáson át az üzemből való végső kivonásig. Ez az elv kiemelt helyen

A Bizottság az adatkezelők felelősségének erősítése céljából az alábbi intézkedéseket fogja megvizsgálni:

- a független **adatvédelmi tisztviselő** kinevezésének kötelezővé tétele, és a tisztviselő feladat- és hatásköreire vonatkozó szabályok összehangolása³¹, mérlegelve ugyanakkor a megfelelő küszöbértéket, hogy elkerüljék a – különösen a kis- és mikrovállalkozásokat érintő – indokolatlan adminisztratív terheket;
- az adatkezelők azon kötelezettségének belefoglalása a jogi keretbe, hogy **adatvédelmi hatásvizsgálatokat** kell készíteniük egyes különleges esetekben, például érzékeny adatok feldolgozásakor, vagy amikor a feldolgozás típusa egyéb sajátos kockázatokat hordoz magában, különösen amikor sajátos technológiákat, mechanizmusokat vagy eljárásokat – többek között profilalkotást és videokamerás megfigyelést – alkalmaznak;
- az adatvédelmet erősítő technológiák alkalmazásának és „**beépített adatvédelem**” („**privacy by design**”) elve konkrét alkalmazási lehetőségeinek fokozott támogatása.

2.2.5. *Az önszabályozási kezdeményezések ösztönzése és az európai uniós tanúsítási rendszerek lehetőségeinek vizsgálata*

A Bizottság továbbra is úgy gondolja, hogy az adatkezelők **önszabályozási kezdeményezései hozzájárulhatnak az adatvédelmi szabályok érvényesítésének javításához**. A magánérdekeltek eddig ritkán alkalmazták az adatvédelmi irányelv önszabályozásra vonatkozó rendelkezéseit, vagyis a magatartási kódex készítésére vonatkozó szabályokat³², amelyeket nem tartottak megfelelőnek.

Emellett a Bizottság megvizsgálja annak lehetőségét, hogy a magánélet védelmét tiszteletben tartó eljárásokra, technológiákra, termékekre és szolgáltatásokra vonatkozó európai uniós **tanúsítási rendszereket (pl.: „adatvédelmi címkéket”)** hívjon életre³³. Ezek nem pusztán az ilyen technológiák, termékek és szolgáltatások felhasználóinak nyújtanának iránymutatást, hanem az adatkezelő felelőssége tekintetében is irányadók volnának: a tanúsított technológiák, termékek és szolgáltatások igénybe vétele mellett döntés elősegíthetné annak igazolását, hogy az adatkezelő eleget tett kötelezettségeinek (lásd a fenti 2.2.4. pontot). Természetesen létfontosságú lenne az **ilyen adatvédelmi címkék megbízhatóságának** biztosítása, és annak vizsgálata, hogy ezek hogyan illeszkednek a jogi kötelezettségek és a nemzetközi technikai szabványok keretébe.

szerepel többek között az „Az európai digitális menetrend” című bizottsági közleményben – COM (2010) 245.

³¹ Már több tagállam átültette (lásd pl. a „*Beaufragter für den Datenschutz*” Németországban, és a „*correspondant informatique et libertés (CIL)*” Franciaországban) azt a meglévő lehetőséget, hogy az adatkezelő adatvédelmi tisztviselőt nevezhet ki annak érdekében, hogy az függetlenül eljárva gondoskodjon az uniós és nemzeti adatvédelmi szabályok betartásáról és segítséget nyújtson az érintetteknek.

³² Lásd a 95/46/EK irányelv 27. cikkét.

³³ Ebben a tekintetben, lásd továbbá az adatvédelmet erősítő technológiákról szóló közleményt, id.: 30. lábjegyzet.

A Bizottság:

- megvizsgálja az **önszabályozási kezdeményezések jövőbeni ösztönzésének** eszközeit, beleértve a magatartási kódexek tevékeny előmozdítását;
- megvizsgálja **európai uniós tanúsítási rendszerek** létrehozásának megvalósíthatóságát a magánélet és az adatok védelme terén.

2.3. A büntetőügyekben folytatott rendőrségi és igazságügyi együttműködés terén meglévő adatvédelmi szabályok felülvizsgálata

Az adatvédelmi irányelv a tagállamok állami és magánszektoraiban végzett valamennyi személyesadat-feldolgozási tevékenységre alkalmazandó. Mindazonáltal nem vonatkozik személyes adatok olyan tevékenység során való feldolgozására, amely kívül esik a közösségi jog hatályán. Ilyenek például a büntetőügyekben folytatott rendőrségi és igazságügyi együttműködés terén folytatott tevékenységek³⁴. A Lisszaboni Szerződés azonban eltörölte az EU korábbi pillérszerkezetét, és új, átfogó jogalapot teremtett a személyes adatoknak az összes uniós szakpolitikára kiterjedő védelme érdekében³⁵. Ezért a fentiek alapján, és az Európai Unió Alapjogi Chartájára figyelemmel, a Stockholmi Programról és a stockholmi cselekvési tervről szóló bizottsági közlemény hangsúlyozta, hogy „*átfogó adatvédelmi szabályozásra van szükség*” és „*meg kell szilárdítan[ni] az Unió helyzetét az egyének személyes adatainak védelme tekintetében, az összes uniós szakpolitika – így a bűnüldözés és a bűnmegelőzés [...] – terén*”³⁶.

A büntetőügyekben folytatott rendőrségi és igazságügyi együttműködés terén az adatvédelmet szabályozó uniós jogi aktus a **2008/977/IB kerethatározat**³⁷, amely fontos előrelépést jelent az említett területen, ahol nagy szükség volt közös adatvédelmi normákra. Azonban további erőfeszítéseket kell tenni.

A kerethatározat csak a személyes adatok Unión belüli határokon átnyúló cseréjére alkalmazandó, és nem érinti a tagállamokon belüli, belföldi adatfeldolgozási műveleteket. A gyakorlatban nehezen alkalmazható ez a megkülönböztetés, amely megnehezítheti a kerethatározat tényleges végrehajtását és alkalmazását³⁸.

Emellett a kerethatározat **túl sok kivételt engedélyez a célhoz kötöttség elve alól**. További hiányosság, hogy a jogszabály nem tartalmaz olyan rendelkezéseket, miszerint az eltérő adatkategóriákat meg kell különböztetni pontosságuk és megbízhatóságuk foka szerint, illetve a tényeken alapuló adatokat meg kell különböztetni a véleményeken vagy személyes

³⁴ Lásd a 95/46/EK irányelv 3. cikke (2) bekezdésének első francia bekezdését.

³⁵ Lásd az EUMSZ. 16. cikkét.

³⁶ Lásd: COM(2009) 262., 2009.6.10., valamint COM(2010) 171., 2010.4.20.

³⁷ A Tanács 2008/977/IB kerethatározata (2008.11.27.) a büntetőügyekben folytatott rendőrségi és igazságügyi együttműködés keretében feldolgozott személyes adatok védelméről (HL L 350., 2008.12.30., 60. o.) A kerethatározat csak az adatvédelmi normák minimális harmonizációját kívánja elérni.

³⁸ Ez a megkülönböztetés nem jelenik meg az alábbi vonatkozó Európa tanácsi jogi aktusokban: Az egyéneknek a személyes adatok gépi feldolgozása során való védelméről szóló egyezmény (CETS sz.: 108.), az egyezménynek a felügyeleti hatóságokra és a határokon átnyúló adatáramlásra vonatkozó kiegészítő jegyzőkönyve (CETS sz. 181.) valamint az Európa Tanács Miniszteri Bizottságának 1987. szeptember 17-én elfogadott R (87) 15. sz. ajánlása a személyes adatok rendőri ágazatban való felhasználásának szabályozásáról.

megítélésen alapulóktól³⁹, továbbá hogy különbséget kell tenni az érintettek különféle kategóriái között (bűnözők, gyanúsítottak, áldozatok, tanúk, stb.), és különleges biztosítékokat kell megállapítani a nem gyanúsított személyekre vonatkozó adatok tekintetében⁴⁰.

Ezen felül a kerethatározat nem helyettesítheti a büntetőügyekben folytatott rendőrségi és igazságügyi együttműködésre vonatkozó, uniós szinten elfogadott különféle ágazatspecifikus jogi aktusokat⁴¹, kiváltképpen azokat, amelyek az Europol, az Eurojust, a Schengeni Információs Rendszer (SIS), és a váminformációs rendszer (VIR)⁴² működését szabályozzák. Az említett jogszabályok saját adatvédelmi szabályozást tartalmaznak és/vagy rendszeresen hivatkoznak az Európa Tanács adatvédelmi jogi aktusaira. A büntetőügyekben folytatott rendőrségi és igazságügyi együttműködés terén végzett tevékenységek vonatkozásában valamennyi tagállam aláírta a rendőri ágazat esetében a 108. egyezmény elveit rögzítő R (87) 15. sz. Európa tanácsi ajánlást, amely azonban jogilag nem kötelező.

Ez a helyzet közvetlenül befolyásolhatja az érintettek lehetőségeit adatvédelmi jogosultságaik e területen való gyakorlására (pl.: annak megismerésére, kik, milyen célból, mely személyes adataikat dolgozzák fel és cserélik ki, és miként élhetnek a jogaikkal, így az adataikhoz való hozzáférés jogával).

Az átfogó és egységes – egyben harmadik országokkal szemben is alkalmazható – európai uniós szabályrendszer létrehozásának célkitűzése **szükségessé teszi, hogy fontolóra vegyük a büntetőügyekben folytatott rendőrségi és igazságügyi együttműködés jelenlegi adatvédelmi szabályainak felülvizsgálatát**. A Bizottság hangsúlyozza, hogy az átfogó adatvédelmi szabályozás fogalma nem zárja ki különös szabályok alkalmazását a rendőrségi és igazságügyi ágazatban, figyelembe véve e területek sajátos jellegét, amelyet a Lisszaboni Szerződéshez csatolt 21. nyilatkozat rögzített. Ez például azt jelenti, hogy egyes adatvédelmi jogok esetében mérlegelni kell, hogy az érintettek általi igénybevétel milyen mértéke akadályozhatná a bűncselekmények megelőzését, kivizsgálását, felderítését, a büntetőeljárás lefolytatását vagy büntetőjogi szankciók végrehajtását.

A Bizottság elsősorban:

- mérlegeli az **általános adatvédelmi szabályok alkalmazásának kiterjesztését a büntetőügyekben folytatott rendőrségi és igazságügyi együttműködésre**, beleértve a belföldi szintű adatfeldolgozást is, miközben szükség esetén harmonizált **korlátozásokat** állapít meg az érintettek egyes adatvédelmi jogosultságai – pl.: a hozzáféréshez való jog vagy az átláthatóság elve – tekintetében;
- megvizsgálja, hogy az új általános adatvédelmi keretben szükség van-e **különös és harmonizált rendelkezésekre** például a **genetikai adatok** büntetőjogi célú feldolgozására vonatkozó adatvédelem, vagy a büntetőügyekben folytatott rendőrségi és igazságügyi együttműködés terén az érintettek különféle kategóriáinak (tanúk, gyanúsítottak, stb.) megkülönböztetése érdekében;

³⁹ Amint az R (87) 15. sz. ajánlás 3.2. elve megköveteli.

⁴⁰ Ellentétben az R (87) 15. sz. ajánlás 2. elvével és annak értékelő jelentéseivel.

⁴¹ E jogi aktusok áttekintése megtalálható „A szabadságon, a biztonságon és a jog érvényesülésén alapuló térségben folytatott információkezelés áttekintése” című bizottsági közleményben – COM(2010) 385.

⁴² A 45/2001/EK rendelet alapján az uniós intézmények, szervek, hivatalok és ügynökségek feletti általános felügyeleti hatáskörrel rendelkező európai adatvédelmi biztos mellett a megfelelő jogi aktusok közös felügyeleti hatóságokat hoztak létre az adatvédelmi felügyelet biztosítására.

- 2011-ben **konzultációt** kezd az összes érintett érdekelttel a **büntetőügyekben folytatott rendőrségi és igazságügyi együttműködés jelenlegi felügyeleti rendszereinek** legcélszerűbb **felülvizsgálatáról** az összes unió intézmény, szerv, hivatal és ügynökség hatékony és egységes adatvédelmi felügyelete érdekében;

- megvizsgálja, hogy hosszú távon szükséges-e a **büntetőügyekben folytatott rendőrségi és igazságügyi együttműködés egyedi jogi aktusaiban uniós szinten elfogadott meglévő különféle ágazatspecifikus szabályok összehangolása** az új általános adatvédelmi kerettel.

2.4. Az adatvédelem globális dimenziója

2.4.1. A nemzetközi adattovábbítás szabályainak tisztázása és egyszerűsítése

A személyes adatoknak az EU és az EGT területén kívülre történő továbbítást lehetővé tevő egyik eszköz az ún. „**megfelelőségi értékelés**”. Jelenleg a Bizottság és a tagállamok állapíthatják meg egy harmadik ország megfelelőségét, vagyis azt, hogy az adott ország az Unió által megfelelőnek tartott szintű adatvédelmet biztosít-e.

A megfelelőség Bizottság általi megállapítása következtében a személyes adatok mind a 27 uniós tagállamból és a három EGT-tagállamból szabadon áramolhatnak az érintett harmadik országba, anélkül hogy bármely további biztosítékra lenne szükség. Az adatvédelmi irányelv azonban jelenleg nem rögzíti megfelelő részletességgel, hogy pontosan milyen követelményeket kell teljesíteni ahhoz, hogy a Bizottság elismerje a megfelelőséget. Emellett a kerethatározat nem ír elő ilyen bizottsági határozatot.

Néhány tagállamban első fokon a személyes adatokat harmadik országnak továbbító adatkezelő maga vizsgálja a megfelelőséget, némely esetben az adatvédelmi felügyelő hatóság utólagos ellenőrzése mellett. E helyzet következtében eltérő megközelítések alakulhatnak ki a harmadik országok vagy nemzetközi szervezetek megfelelőségi fokának értékelése tekintetében, valamint **az a veszély is előállhat, hogy tagállamonként eltérően ítélik meg az adott harmadik ország által az érintettek számára biztosított adatvédelem szintjét**. Emellett a mostani jogszabályok nem tartalmazznak részletes, harmonizált követelményeket arra vonatkozóan, hogy mikor tekinthető jogszerűnek az adattovábbítás. Emiatt tagállamonként eltérő gyakorlatok alakulnak ki.

Továbbá, ami a megfelelő szintű adatvédelmet nem biztosító harmadik országoknak való adattovábbítást illeti, az adatkezelőknek⁴³ és adatfeldolgozóknak⁴⁴ való személyesadat-továbbításra vonatkozó bizottsági egységes szerződési feltételek nem alkalmazhatók a szerződéses viszonyokon kívüli helyzetekre, például hatóságok közötti adattovábbításra.

⁴³ A Bizottság 2001/497/EK határozata (2001. június 15.) a 95/46/EK irányelv alapján a személyes adatok harmadik országokba irányuló továbbítására vonatkozó általános szerződési feltételekről (HL L 181., 2001.7.4., 19. o.); a Bizottság 2002/16/EK határozata (2001. december 27.) a 95/46/EK irányelv alapján a személyes adatoknak harmadik országbeli adatfeldolgozók részére történő továbbítására vonatkozó általános szerződési feltételekről (HL L 6., 2002.1.10., 52. o.); a Bizottság 2004/915/EK határozata (2004. december 27.) a 2001/497/EK határozat módosításáról a személyes adatoknak harmadik országokba irányuló továbbadására vonatkozó alternatív általános szerződési feltételek bevezetéséről (HL L 385., 2004.12.29., 74. o.).

⁴⁴ A Bizottság határozata (2010. február 5.) a 95/46/EK európai parlamenti és tanácsi irányelv alapján a személyes adatok harmadik országbeli adatfeldolgozók részére történő továbbítására vonatkozó általános szerződési feltételekről (HL L 39., 2010.2.12., 5. o.).

Ezen felül az Unió és tagállamai által megkötött nemzetközi megállapodások gyakran megkövetelik adatvédelmi elvek és különös rendelkezések felvételét. Ennek eredményeként ellentétes rendelkezéseket és jogokat megállapító, különféle szövegek születhetnek, és így megnyílik a lehetőség az érintetteket károsító eltérő értelmezések előtt. Ennek megfelelően a Bizottság bejelentette, hogy kidolgozza az Unió és a harmadik országok közötti bűnüldözési célú megállapodások személyes adatok védelmére vonatkozó alapvető szabályait⁴⁵.

Az ugyanazon vállalatcsoporthoz tartozó vállalatok közötti jogszerű személyesadat-továbbítás hasznos eszközt jelenthetik az önszabályozás formájában kidolgozott egyéb eszközök, így pl. a „kötelező erejű vállalati szabályok”⁴⁶ néven ismert vállalaton belüli magatartási kódex is. Az érdekeltek mindazonáltal úgy vélték, hogy tovább lehetne javítani ezt a mechanizmust, és megkönnyíthetnék annak végrehajtását.

A megállapított problémák orvoslása érdekében **általában véve szükség van a személyes adatok továbbítását lehetővé tévő jelenlegi mechanizmusok javítására**, ugyanakkor pedig biztosítani kell, hogy a személyes adatok megfelelő védelemben részesüljenek az EU és az EGT területén kívüli továbbításuk és feldolgozásuk során.

A Bizottság meg kívánja vizsgálni, miként valósíthatók meg az alábbi intézkedések:

a nemzetközi adattovábbítás **jelenlegi megoldásainak** – többek között a jogilag kötelező eszközöknek és a „kötelező erejű vállalati szabályoknak” – **a javítása és egyszerűsítése** a harmadik országokkal és a nemzetközi szervezetekkel szembeni **egységesebb és következetesebb uniós megközelítés** érdekében;

- **a Bizottság megfelelőségi eljárásának tisztázása**, valamint az adott harmadik ország vagy nemzetközi szervezet adatvédelmi szintjének értékelésére vonatkozó **kritériumok és követelmények** meghatározásának javítása;
- azon **alapvető uniós adatvédelmi szabályok** meghatározása, amelyeket valamennyi nemzetközi megállapodás-típus esetén fel lehetne használni.

2.4.2. Az egyetemes elvek előmozdítása

Az adatfeldolgozás globális szinten zajlik, ami szükségessé teszi az adatfeldolgozás tekintetében az egyének védelmére vonatkozó egyetemes elvek kidolgozását.

Az EU adatvédelemre vonatkozó jogi kerete gyakorta **mérceként** szolgált **harmadik országoknak az adatvédelem szabályozása során**. Az uniós jogi keret hatása és eredménye az Unión belül és kívül is kiemelkedően jelentős. **Ezért az Európai Uniónak továbbra is vezető szerepet kell betöltenie** a vonatkozó uniós és egyéb európai adatvédelmi eszközökre épülő **nemzetközi adatvédelmi jogi normák és technikai szabványok kidolgozása és előmozdítása terén**. Mindez kiváltképpen fontos az EU bővítési politikájának keretében.

⁴⁵ Stockholmi cselekvési terv, id. (36. lábjegyzet)

⁴⁶ A „kötelező erejű vállalati szabályok” az európai adatvédelmi normákra épülő gyakorlati szabályok, amelyeket a multinacionális szervezetek önként dolgoztak ki és tartanak be abból a célból, hogy megfelelő biztosítékokat nyújtsanak az azonos vállalatcsoporthoz és azonos vállalati szabályok hatálya alá tartozó vállalatok közötti személyesadat-továbbítás, illetve személyesadat-továbbítási kategóriák tekintetében. Lásd az alábbi internetcímet:
http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faqs/international_transfers_faqs.pdf.

Ami a szabványügyi szervezetek által kidolgozott nemzetközi technikai szabványokat illeti, a Bizottság úgy ítéli meg, hogy a jövőbeni jogi keret és e szabványok összhangja rendkívül fontos ahhoz, hogy az adatkezelők egységes és gyakorlatias módon hajtsák végre az adatvédelmi szabályokat.

A Bizottság:

- folytatja **magas szintű adatvédelmi jogi normák és technikai szabványok kidolgozásának előmozdítását** nemzetközi szinten és a harmadik országokban;
- **az Unió nemzetközi fellépései során a védelem viszonyossága elvének** érvényesítésére törekszik, különös tekintettel azon érintettekre, akik adatait az EU-ból harmadik országokba viszik ki;
- **ezért erősíti az együttműködését a harmadik országokkal és a nemzetközi szervezetekkel**, így az OECD-vel, az Európa Tanáccsal, az ENSZ-el és más regionális szervezetekkel;
- **szorosan nyomon követi a szabványügyi szervezetek** – így a CEN és az ISO – **nemzetközi technikai szabványainak kidolgozását** annak érdekében, hogy azok hasznosan egészítsék ki a jogi szabályokat, továbbá, hogy biztosítsa a legfontosabb adatvédelmi követelmények operatív és hatékony végrehajtását.

2.5. Erősebb intézményi struktúra az adatvédelmi szabályok hatékonyabb érvényesítése céljából

Az adatvédelmi elvek és szabályok végrehajtása és érvényesítése az egyéni jogok tiszteletben tartását garantáló kulcsfontosságú tényező.

A fentiekkel összefüggésben **az adatvédelmi hatóságok** lényegi szerepet töltenek be az adatvédelmi szabályok érvényesítése során. E hatóságok a személyes adatok védelmével kapcsolatos alapvető jogok és szabadságok független őrei, és az egyének segítségével biztosíthatják személyes adataik védelmét és a feldolgozási műveletek jogszerűségét. Ezért a Bizottság úgy gondolja, hogy – különös figyelemmel az Európai Bíróság e hatóságok függetlenségére vonatkozó közelmúltbeli ítélezési gyakorlatára⁴⁷ – meg kell erősíteni a szerepüket, valamint biztosítani kell számukra a feladataik ellátásához nemzeti szinten és az egymással folytatott együttműködés során is szükséges hatásköröket és erőforrásokat.

A Bizottság szerint ugyanakkor **az adatvédelmi hatóságoknak erősíteniük kell az együttműködésüket és jobban össze kell hangolniuk a tevékenységeiket**, különösen amikor jellegüknél fogva határokon átnyúló dimenzióval rendelkező problémákkal foglalkoznak. Ez különösen igaz akkor, ha több tagállamban is megtelepedett multinacionális vállalkozások mindegyik ilyen országban tevékenykednek, vagy ha az európai adatvédelmi biztossal összehangolt felügyelet szükséges⁴⁸.

⁴⁷ Az Európai Bíróság C-518/07 sz. Bizottság kontra Németország ügyben hozott 2010. március 9-i ítélete.

⁴⁸ Jelenleg ez a helyzet a nagyméretű IT-rendszerek – pl.: a SIS II (vö. az 1987/2006/EK rendelet 46. cikkével - HL 318., 2006.12.28., 4.o.) és a VIS (vö. a 767/2008/EK rendelet 43. cikkével - HL L 218., 2008.8.13., 60. o.) – esetében.

E tekintetben **fontos szerepet játszhat a 29. cikk alapján létrehozott munkacsoport**⁴⁹, amely tanácsadói feladata⁵⁰ mellett már jelenleg is hozzájárul az uniós adatvédelmi szabályok egységes nemzeti szintű alkalmazásához. Erősíteni kell a munkacsoport szerepét az adatvédelmi hatóságok álláspontjainak koordinálása terén, és biztosítani kell az egységesebb nemzeti szintű jogalkalmazást, és így az egyenlő szintű adatvédelmet, mivel az adatvédelmi hatóságok továbbra is eltérően alkalmazzák és értelmezik az uniós jogot még akkor is, ha az egész Unióban azonos kihívások jelentkeznek.

A Bizottság megvizsgálja, miként valósíthatók meg az alábbi intézkedések:

- **a nemzeti adatvédelmi hatóságok jogállásának és hatásköreinek erősítése, tisztázása és harmonizálása** az új jogi keretben, ideértve a „teljes függetlenség” fogalmának⁵¹ teljes körű végrehajtását;
- **az adatvédelmi hatóságok közötti együttműködés és koordináció javítása;**
- az uniós adatvédelmi szabályok belső piacon való következetesebb alkalmazásának biztosítása. Mindez felölelheti **a nemzeti adatvédelmi biztosok szerepének erősítését, munkájuk összehangolásának javítását a 29. cikk alapján létrehozott munkacsoport útján (amelynek áttekinthetőbb szervvé kell válnia), és/vagy a belső piacon belüli egységességet biztosító mechanizmus létrehozását az Európai Bizottság felügyelete alatt.**

3. KÖVETKEZTETÉS: TOVÁBBI TEENDŐK

A technológiához hasonlóan a személyes adatok felhasználásának és megosztásának módja is állandóan változik a társadalmunkban. Ez azt a kihívást támasztja a jogalkotókkal szemben, hogy olyan jogi keretet kell alkotniuk, amely kiállja az idő próbáját. A reformfolyamat végén az európai adatvédelmi szabályoknak továbbra is magas szintű védelmet kell szavatolniuk, illetve tartós jogbiztonságot kell biztosítaniuk a belső piacon az egyének, a közigazgatások és a vállalkozások számára. A helyzet bonyolultságának és a technológia kifinomultságának mértékétől függetlenül egyértelműnek kell lenniük azon alkalmazandó szabályoknak és szabványoknak, amelyeket a nemzeti hatóságoknak érvényesíteniük kell, a vállalkozásoknak és a technológiafejlesztők pedig be kell tartaniuk. Az egyéneknek szintén tisztában kell lenniük az általuk élvezett jogokkal.

A problémák orvoslására és az e közleményben hangsúlyozott legfontosabb célkitűzések megvalósítására irányuló, **átfogó bizottsági megközelítés** alapul szolgál majd a többi európai intézménnyel és az egyéb érdekelttel zajló további megbeszélésekhez, később pedig jogalkotási és nem jogalkotási jellegű konkrét javaslatokban és intézkedésekben ölthet testet. E célból a Bizottság örömmel fogadja az e közleményben említett problémákra vonatkozó visszajelzéseket.

⁴⁹ A 29. cikk alapján létrehozott munkacsoport a tagállami adatvédelmi hatóságok, az európai adatvédelmi biztos és a Bizottság (szavazati jogok nélküli) képviselőjéből álló tanácsadó szerv. A titkársági feladatok ellátását a Bizottság biztosítja. Lásd az alábbi internetcímet:
http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm.

⁵⁰ A 29. cikk alapján létrehozott munkacsoport feladata, hogy tanácsot adjon a Bizottságnak az Unió és a harmadik országokon belüli védelem szintjéről, és a személyes adatok feldolgozásával összefüggő bármely egyéb intézkedésről.

⁵¹ Lásd az Európai Bíróság C-518/07 sz. Bizottság kontra Németország ügyben hozott 2010. március 9-i ítéletét.

Ezek alapján – hatásvizsgálatot követően és az EU Alapjogi Chartájának figyelembe vételével – a Bizottság **2011-ben javaslatot tesz** az adatvédelem jogi keretének felülvizsgálatára irányuló **jogszabályra** abból a célból, hogy megerősítse az Unió helyzetét az egyének személyes adatainak az uniós politikák keretében történő védelme terén, így – az adott területek sajátosságainak szem előtt tartásával – a büntetőügyekben folytatott rendőrségi és igazságügyi együttműködés során. A fentiekkel egyidejűleg dolgozunk majd nem jogalkotási intézkedéseken (így pl.: az önszabályozás ösztönzésén és az uniós adatvédelmi címkék megvalósíthatóságának vizsgálatán).

Második lépésként a Bizottság megvizsgálja, hogy **más jogi aktusokat is hozzá kell-e igazítani** az adatvédelmi keret új generációjához. Ez mindenekelőtt a 45/2001/EK rendeletet érinti, amelynek rendelkezéseit az új általános kerethez kell majd igazítani. Későbbi szakaszban a többi ágazati jogi aktusra gyakorolt hatást is gondosan meg kell vizsgálni.

A Bizottság továbbra is biztosítani fogja az e területre vonatkozó uniós jog helyes alkalmazásának megfelelő nyomon követését azáltal, hogy **tevékeny jogsértés elleni politikát folytat** az uniós adatvédelmi szabályok helytelen végrehajtása és alkalmazása esetén. Az adatvédelmi eszközök mostani felülvizsgálata nem érinti a tagállamok kötelezettségét a személyes adatok védelmére vonatkozó, meglévő jogi aktusok végrehajtására és megfelelő alkalmazásuk biztosítására⁵².

Az Unión belüli magas szintű és egységes adatvédelem megvalósítása a legjobb módja annak, hogy világszerte támogassuk és előmozdítsuk az uniós adatvédelmi normákat.

⁵²

Ez a 2008/977/IB tanácsi kerethatározatra is kiterjed: a tagállamoknak meg kell hozniuk a szükséges intézkedéseket, hogy e kerethatározat rendelkezéseinek legkésőbb 2010. november 27-ig megfeleljenek.