

HU

HU

HU



EURÓPAI BIZOTTSÁG

Brüsszel, 2010.7.20.

COM(2010)385 végleges

**A BIZOTTSÁG KÖZLEMÉNYE AZ EURÓPAI PARLAMENTNEK ÉS A
TANÁCSNAK**

**A szabadságon, a biztonságon és a jog érvényesülésén alapuló térségben folytatott
információkezelés áttekintése**

A BIZOTTSÁG KÖZLEMÉNYE AZ EURÓPAI PARLAMENTNEK ÉS A TANÁCSNAK

A szabadságon, a biztonságon és a jog érvényesülésén alapuló térségben folytatott információkezelés áttekintése

1. BEVEZETÉS

Az Európai Unió hosszú utat tett meg azóta, hogy 1985-ben Schengenben öt európai ország vezetői megállapodtak közös határaik ellenőrzésének megszüntetéséről. Megállapodásuk alapozta meg az 1990. évi Schengeni Egyezményt, amely csírájában már tartalmazta a mostani információkezelési politikák jelentős részét. A belső határellenőrzés eltörlése felgyorsította egy sor, főként az alábbiakat érintő intézkedés megvalósítását a külső határokon: a vízumkiadás, a menekültügyi és bevándorlási politikák összehangolása, valamint a határokon átnyúló bűnözés elleni küzdelemben folytatott rendőrségi, igazságügyi és vámügyi együttműködés erősítése. Sem a schengeni térség, sem az uniós belső piac nem működhetne napjainkban a határokon átnyúló adatsere nélkül.

A 2001. évi egyesült államokbeli terrortámadások, valamint a 2004-es és 2005-ös madridi és londoni bombamerényletek további lendületet adtak az európai információkezelési politikák kidolgozásának. 2006-ban a Tanács és az Európai Parlament elfogadta az adatmegőrzési irányelvet, amely feljogosítja a tagállami hatóságokat, hogy a távközlési forgalmi és helymeghatározó adatok megőrzésével küzdjenek a súlyos bűnözés ellen¹. Ezt követően a Tanács felkarolta azt a svéd kezdeményezést, amely a bűnügyi nyomozások és operatív műveletek során zajló, határokon átnyúló információcseré egyszerűsítésére irányult. 2008-ban a Tanács jóváhagyta a prümi határozatot, amelynek célja a DNS-profilok, ujjlenyomatok és gépjármű-nyilvántartási adatok cseréjének felgyorsítása a terrorizmus és az egyéb bűnözési formák elleni küzdelem során. A schengeni térségen belüli súlyos bűnözés elleni küzdelem további eszközét jelenti a pénzügyi hírszerző egységek, vagyon-visszaszerzési hivatalok és a számítástechnikai bűnözés elleni platformok közötti határokon átnyúló együttműködés, valamint az Europol és az Eurojust tagállamok általi igénybevétele.

Közvetlenül a 2001. szeptember 11-i terrortámadást követően az Egyesült Államok kormánya létrehozta a terrorizmus finanszírozásának felderítését célzó programot, hogy a gyanús pénzügyi tranzakciók nyomon követése révén megghiúsítsa a hasonló szervezkedéseket. Az Európai Parlament a közelmúltban megadta az egyetértését az Európai Unió és az Amerikai Egyesült Államok között az Európai Unióból származó pénzügyi üzenetadatoknak a terrorizmus finanszírozásának felderítését célzó program céljából történő feldolgozásáról és

¹ A súlyos bűncselekménynek jelenleg nincs összehangolt uniós meghatározása. Például az Europol a VIS-be történő betekintésre feljogosító tanácsi határozat (a Tanács 2008/633/IB határozata, HL L 218., 2008.8.13., 129. o.) a súlyos bűncselekményeket az európai elfogatóparancsban felsorolt bűncselekményekre hivatkozással határozza meg (a Tanács 2002/584/IB határozata, HL L 190., 2002.7.18., 1. o.). Az adatmegőrzési irányelv (a 2002/58/EK irányelv, HL L 105., 2006.4.13., 54. o.) meghagyja a tagállamoknak a „súlyos bűncselekmény” meghatározását. Az Europol határozat (a Tanács 2009/371/IB határozata, HL L 121., 2009.5.15., 37. o.) a súlyos bűncselekmények meghatározásaként az európai elfogatóparancsban található felsoroláshoz rendkívül hasonló, azonban attól eltérő másik listát tartalmaz.

az Amerikai Egyesült Államok részére való átadásáról szóló megállapodás (a továbbiakban: EU-USA TFTP-megállapodás) megkötéséhez.² Az utas-nyilvántartási adatok (a továbbiakban: PNR) harmadik országokkal való cseréje szintén elősegítette az EU-nak a terrorizmus és a súlyos bűnözés egyéb formái elleni küzdelmét.³ Miután PNR-megállapodásokat kötött az Egyesült Államokkal, Ausztráliával és Kanadával, a Bizottság nemrégiben ismét tervezési munkába fogott azzal a céllal, hogy felülvizsgálja az uniós PNR-rendszer megteremtésével és az ilyen adatok harmadik országokkal történő megosztásával kapcsolatos megközelítését.

A fent körvonalazott intézkedések lehetővé tették a schengeni térségen belüli szabad mozgást, hozzájárultak a terrorista támadások és a súlyos bűncselekmények egyéb formáinak megelőzéséhez és az azok elleni küzdelemhez, és serkentették a közös vízum- és menekültügyi politika kidolgozását.

E közlemény első ízben ad teljes körű áttekintést azokról a működő, végrehajtási vagy mérlegelési szakaszban lévő uniós szintű intézkedésekről, amelyek a személyes adatok bűnüldözési és migrációkezelési célból való gyűjtését, tárolását, illetve határokon átnyúló cseréjét szabályozzák. A polgároknak jogukban áll megismerni, hogy mely személyes adataikat, kik és milyen célból dolgozzák fel és cserélik ki. E dokumentum világos választ ad az említett kérdésekre. Tisztázza ezen eszközök fő célját, felépítését, az alkalmazási körükbe tartozó személyes adatokat, felsorolja az ilyen adatokhoz hozzáféréssel rendelkező hatóságokat, és ismerteti az adatvédelmet és –megőrzést szabályozó rendelkezéseket. Emellett tartalmaz néhány példát is az említett eszközök gyakorlati működési módjának bemutatására (lásd az I. mellékletet). A közlemény végül meghatározza azokat az alapvető elveket, amely alapját kell, hogy képezzék a információkezelési eszközök kialakításának és értékelésének a szabadságon, a biztonságon és a jog érvényesülésén alapuló térségben.

E közlemény annak révén járul hozzá az érdekeltekkel folytatandó, tájékozottságon alapuló szakpolitikai párbeszédhez, hogy áttekintést ad a személyes információk kezelését szabályozó uniós szintű intézkedésekről, valamint javaslatot tesz az ilyen intézkedések kidolgozására és értékelésére vonatkozó elvekre. Egyidejűleg első alkalommal ad választ a tagállamok azon felkérésére, hogy dolgozzunk ki koherensebb megközelítést a személyes adatok bűnüldözési célú cseréjére vonatkozóan – amit az uniós információkezelési stratégia⁴ a közelmúltban tárgyalt –, illetőleg a jelenlegi információcserére vonatkozó intézkedések értékelésén alapuló, esetleges európai információcsere-modell kidolgozásának szükségességével kapcsolatos mérlegelés tekintetében⁵.

A cél korlátozása kulcsfontosságú megfontolást képez az e közleményben ismertetésre kerülő legtöbb eszköz esetében. Egy többcélú, egységes és átfogó uniós információs rendszer biztosítaná a legmagasabb szintű információmegosztást. Egy ilyen rendszer létrehozása

² Az Európai Parlament állásfoglalása, P7_TA-PROV(2010)0279, 2010.7.8..

³ A súlyos bűncselekménnyel szemben a „terrorista bűncselekmény” fogalmát a terrorizmus elleni küzdelemről szóló tanácsi kerethatározat egyértelműen meghatározza (a 2008/919/IB tanácsi kerethatározat, HL L 330., 2008.12.9., 21. o., által módosított 2002/475/IB tanácsi kerethatározat, HL L 164., 2002.6.22., 3. o.).

⁴ Az uniós belső biztonság terén alkalmazandó információkezelési stratégiájára vonatkozó tanácsi következtetések, Bel- és Igazságügyi Tanács, 2009.11.30. (uniós információkezelési stratégia); „Szabadság, biztonság, a magánélet védelme – európai belügyek egy nyitott világban”, Az európai belpolitika jövőjével foglalkozó magas szintű tanácsadó csoport („a jövő-munkacsoport”) jelentése, 2008. június.

⁵ A stockholmi program – A polgárokat szolgáló és védő, nyitott és biztonságos Európa, 5731/10. sz. tanácsi dokumentum, 2010.3.3., 4.2.2. szakasz.

azonban a magánélethez és az adatvédelemhez fűződő jog nagymértékű és jogosulatlan korlátozását jelentené, továbbá komoly fejlesztési és üzemeltetési kihívást támasztana. A gyakorlatban lépésről lépésre haladt a szabadságon, a biztonságon és a jog érvényesülésén alapuló térség politikáinak kidolgozása, és ennek eredményeként számos különféle méretű, alkalmazási körű és célú információs rendszer és eszköz látta meg a napvilágot. Az információkezelés elmúlt évtizedekben kialakult szétagolt szerkezete bármely központosított megoldásnál alkalmasabb a polgárok magánélethez fűződő jogának védelmére.

A mostani közlemény nem tér ki azokra az intézkedésekre, amelyek nem személyes adatok stratégiai célú (pl. általános kockázatelemzés vagy fenyegetettség-értékelés) cseréjére vonatkoznak; és a szóban forgó eszközök adatvédelmi rendelkezéseit sem elemzi részletesen, mivel a Bizottság az Európai Unió működéséről szóló szerződés 16. cikke alapján éppen most készít külön elemzést a személyes adatok Unión belüli védelmének új, átfogó keretszabályáról. A Tanács jelenleg mérlegeli az Európai Unió és az Amerikai Egyesült Államok közötti, a rendőrségi együttműködés és a büntetőügyekben folytatott igazságügyi együttműködés keretében a bűncselekmények – ezen belül a terrorcselekmények – megelőzése, kivizsgálása, felderítése vagy üldözése céljából továbbított és feldolgozott személyes adatok védelméről szóló megállapodásra vonatkozó tárgyalási irányelvek tervezetét. E közlemény nem tér ki az említett kezdeményezésre, mivel e tárgyalásokon várhatóan nem a személyes adatok átadásának és feldolgozásának tényleges *tartalmát* állapítják meg, hanem inkább azt, hogy a két fél *miképpen* biztosíthatja az alapvető jogok és szabadságok magas szintű védelmét az említett adatátadás és –feldolgozás során.⁶

2. A SZEMÉLYES ADATOK BŰNÜLDÖZÉSI VAGY MIGRÁCIÓKEZELÉSI CÉLBŐL TÖRTÉNŐ GYŰJTÉSÉT, TÁROLÁSÁT VAGY CSERÉJÉT SZABÁLYOZÓ EURÓPAI UNIÓS ESZKÖZÖK

E szakasz áttekintést ad a személyes adatok bűnüldözési vagy migrációkezelési célból történő gyűjtését, tárolását, illetve határokon átnyúló cseréjét szabályozó európai uniós eszközökről. A 2.1. szakasz a most hatályos, és a végrehajtási vagy mérlegelési szakaszban lévő intézkedéseket veszi górcső alá; a 2.2. szakasz pedig a stockholmi program végrehajtásáról szóló cselekvési tervben⁷ felsorolt kezdeményezésekre vonatkozik. E dokumentum az egyes eszközök alábbi vonatkozásairól nyújt tájékoztatást:

- Előzmények (a tagállamok vagy a Bizottság javasolta-e az intézkedést)⁸;
- Az a cél/azok a célok, amely(ek) miatt az adatokat gyűjtik, tárolják, illetve kicserélik,
- Szerkezet (központosított információs rendszer vagy decentralizált adatcsere);
- Az érintett személyes adatok köre;

⁶ COM(2010) 252., 2010.5.26.

⁷ COM(2010)171., 2010.4.20. (A stockholmi program végrehajtásáról szóló cselekvési terv).

⁸ Az Európai Unió büntetőügyekben folytatott rendőrségi és igazságügyi együttműködést felölelő korábbi harmadik pillérjében a tagállamok és a Bizottság is rendelkezett kezdeményezési joggal. Az Amszterdami Szerződés a külső határok ellenőrzése, a vízumpolitika, a menekültügy és a bevándorlás területét beépítette a közösségi (első) pillérbe, ahol a Bizottság kizárólagos kezdeményezési joggal rendelkezett. A Lisszaboni Szerződés megszüntette az Unió pillérstruktúráját, és megerősítve ezáltal a Bizottság kezdeményezési jogát. A büntetőügyekben folytatott rendőrségi és igazságügyi együttműködés terén (beleértve a közigazgatási együttműködést) azonban továbbra is javasolható jogszabály a tagállamok egynegyedének kezdeményezésére.

- Az adatokhoz hozzáféréssel rendelkező hatóságok;
- Adatvédelmi rendelkezések;
- Adatmegőrzési szabályok;
- A végrehajtás állapota;
- Felülvizsgálati mechanizmus.

2.1. A működő, és a végrehajtási vagy mérlegelési szakaszban lévő eszközök

A schengeni térség és a vámunió működésének javítására irányuló európai uniós eszközök

A **Schengeni Információs Rendszer** (a továbbiakban: SIS) a tagállamok azon óhajának megfelelően született, hogy belső határellenőrzés nélküli térséget hozzanak létre, és egyszersmind megkönnyítsék a külső határaikon zajló személyforgalmat.⁹ Az 1995 óta működő rendszer arra törekszik, hogy fenntartsa a közbiztonságot – így a nemzetbiztonságot – a schengeni térségen belül, továbbá hogy az e rendszeren keresztül közölt adatok felhasználásával megkönnyítse a személyek mozgását. A SIS a résztvevő tagállamokban található nemzeti részből és a franciaországi technikai támogató funkcióból álló központosított információs rendszer. A tagállamok figyelmeztető jelzéseket adhatnak ki az alábbiak tekintetében: azon személyek, akiknek kiadatási célú letartóztatását kérik; a harmadik országok azon állampolgárai, akiknek a beutazását megtagadták; eltűnt személyek; tanúk és bíróságra beidézett személyek; az általuk okozott közbiztonsági vagy a nemzetbiztonsági fenyegetésre tekintettel leplezett figyelés alá vont személyek; lopott vagy elvesztett járművek, okmányok és lőfegyverek; valamint gyanús bankjegyek. Az alábbiak tartoznak a SIS-be bevitt adatok közé: nevek és álnevek, fizikai jellemzők, a születési hely és idő, állampolgárság, továbbá, hogy az érintett személyeknél van-e fegyver és erőszakot alkalmaznak-e. A rendőri, határőrizeti, vám- és a büntetőeljárásban részt vevő igazságügyi hatóságok különálló hatásköreiken belül férhetnek hozzá fenti adatokhoz. A bevándorlási hatóságok és konzuli képviseletek a beutazási tilalmi listán található harmadik országbeli állampolgárokkal kapcsolatos adatokhoz, továbbá az elvesztett és ellopott dokumentumokra vonatkozó figyelmeztető jelzésekhez férhetnek hozzá. Az Europol hozzáférhet a SIS-adatok egyes kategóriáihoz, többek között a kiadatási célú letartóztatás céljából körözött, illetve az általuk okozott közbiztonsági vagy a nemzetbiztonsági fenyegetésre tekintettel leplezett figyelés alá vont személyekre vonatkozó figyelmeztető jelzésekhez. Az Eurojust azokhoz a figyelmeztető jelzésekhez férhet hozzá, amelyeket a kiadatási célú letartóztatás céljából körözött és a bírósági idézés hatálya alatt álló személyek ellen adtak ki. A személyes adatok kizárólag azon figyelmeztető jelzések céljára használhatóak fel, amelyre megadták azokat. A személyek felkutatása céljából a SIS-be bevitt személyes adatok csak annyi ideig tárolhatók, amennyi annak a célnak az eléréséhez szükséges, amely okán a személyes adatokat a hatóság megkapta, illetve legkésőbb a bevitelüket követő három évig. Az általuk okozott közbiztonsági vagy a nemzetbiztonsági fenyegetésre tekintettel leplezett figyelés alá vont személyekre vonatkozó adatokat egy év elteltével kell törölni. A tagállamoknak olyan nemzeti szabályokat kell elfogadniuk, amelyek legalább azonos szintű adatvédelmet írnak elő az Európa Tanács az egyéneknek a személyes adatok gépi feldolgozása során való védelméről

⁹ A Benelux Gazdasági Unió államai, a Németországi Szövetségi Köztársaság és a Francia Köztársaság kormányai között a közös határaikon történő ellenőrzések fokozatos megszüntetéséről szóló, 1985. június 14-i Schengeni Megállapodás végrehajtásáról szóló egyezmény, HL L 239., 2000.9.22., 19. o.

szóló 1981. évi egyezményéből, és az Európa Tanács Miniszteri Bizottságának a személyes adatoknak a rendőrségi ágazatban való felhasználásáról szóló 1987. évi ajánlásából következő normákkal.¹⁰ Jóllehet a Schengeni Egyezmény nem tartalmaz felülvizsgálati mechanizmust, az aláírók javaslatot tehetnek az egyezmény módosítására, majd a módosított szöveget egyhangúlag kell jóváhagyni és a nemzeti parlamenteknek ratifikálniuk kell azt. A SIS teljes körűen alkalmazandó 22 tagállamban, valamint Svájcban, Norvégiában és Izlandon. Az Egyesült Királyság és Írország részt vesz a Schengeni Egyezmény és a SIS rendőrségi együttműködési vonatkozásaiban, a beutazási tilalmi listán szereplő harmadik országbeli állampolgárokkal kapcsolatos figyelmeztető jelzések kivételével. Ciprus aláírta Schengeni Egyezményt, azonban még nem hajtotta végre. Liechtenstein várhatóan 2010-ben hajtja végre az egyezményt; Bulgária és Románia előreláthatólag 2011-ben teszi meg ezt. A SIS-ben végzett keresések akkor eredményeznek „találatot”, ha a egy keresett személy vagy tárgy adatai megfelelnek egy meglévő figyelmeztető jelzésnek. Miután találatot értek el, a bűnüldöző hatóságok a SIRENE irodák hálózata útján kiegészítő információt kérhetnek a figyelmeztető jelzés tárgyairól¹¹.

Amint új tagállamok csatlakoznak a schengeni térséghez, a SIS adatbázis mérete is ennek megfelelően növekszik: 2008 januárja és 2010 között a SIS figyelmeztető jelzéseinek teljes száma 22,9 millióról 31,6 millióra emelkedett.¹² Az adatmennyiség ilyen mértékű növekedését és a felhasználói igények változásait megelőlegezve a tagállamok 2001-ben döntöttek a **Schengeni Információs Rendszer második generációjának** (a továbbiakban: SIS II) kifejlesztéséről, és a Bizottságot bízták meg ezzel a feladattal.¹³ A jelenleg is fejlesztés alatt álló SIS II célja, hogy az első generációs rendszer funkcióinak javítása révén magas biztonsági szintet biztosítson a szabadság, a biztonság és a jog érvényesülésének térségén belül, továbbá hogy az e rendszeren keresztül közölt adatok felhasználásával megkönnyítse a személyek mozgását. Az új rendszer a SIS-ben eredetileg tárolt adatkategóriák mellett képes lesz az alábbiak kezelésére: ujjlenyomatok, fényképek, az európai elfogatóparancs másolatai, azon személyek védelmére vonatkozó rendelkezések, akiknek a személyazonosságával visszaélnék, továbbá a különféle figyelmeztető jelzések közötti kapcsolatok. A SIS II például képes lesz összekapcsolni azokat figyelmeztető jelzéseket, amelyek valamely emberrablásért körözött személyre, az elrabolt személyre, és a bűncselekmény elkövetéséhez használt járműre vonatkoznak. A hozzáférési jogok és az adatmegőrzési szabályok azonosak az első generációs rendszer szabályaival. A személyes adatok kizárólag azon figyelmeztető jelzések céljára használhatóak fel, amelyre megadták azokat. A SIS II-ben tárolt személyes adatok feldolgozását úgy kell végezni, hogy az megfeleljen a 95/46/EK irányelv elveit tisztázó, és az e rendszert szabályozó alap-jogiaktusok (az 1987/2006/EK rendelet és a 2007/533/IB tanácsi határozat) különös rendelkezéseinek, valamint a 45/2001/EK rendeletnek, az Európa Tanács 108. egyezményének és a rendőrségi ajánlásnak¹⁴. A SIS II az s-TESTA-t, a Bizottság

¹⁰ Egyezmény az egyének védelméről a személyes adatok gépi feldolgozása során (ETS 108. sz.), Európa Tanács 1981.1.28. (az Európa Tanács 108. egyezménye); A Miniszterek Tanácsa R (87) 15. sz. ajánlása a személyes adatok rendőri ágazatban való felhasználásának szabályozásáról, Európa Tanács, 1987.9.17. (rendőrségi ajánlás).

¹¹ SIRENE: Supplementary Information Request at National Entry (kiegészítő információ kérése a nemzeti területre való belépéskor).

¹² Az 5441/08. sz. tanácsi dokumentum, 2008.1.30.; a 6162/10. sz. tanácsi dokumentum, 2010.2.5.

¹³ 1986/2006/EK rendelet, HL L 381., 2006.12.28., 1. o.; 1987/2006/EK rendelet, HL L 381., 2006.12.28., 4. o.; 2007/533/IB határozat, HL L 205., 2007.8.7., 63. o.

¹⁴ 1987/2006/EK rendelet, HL L 381., 2006.12.28., 4. o.; 2007/533/IB határozat, HL L 205., 2007.8.7., 63. o.; 95/46/EK irányelv, HL L 281., 1995.11.23., 31. o.; 45/2001/EK rendelet, HL L 8., 2001.1.12., 1. o.; Egyezmény az egyének védelméről a személyes adatok gépi feldolgozása során (ETS 108. sz.), Európa Tanács 1981.1.28. (az Európa Tanács 108. egyezménye); A Miniszterek Tanácsa R (87) 15. sz. ajánlása

biztonságos adatkommunikációs hálózatát fogja használni.¹⁵ Üzembe helyezését követően az összes tagállamban, Svájcban, Liechtensteinben, Norvégiában és Izlandon alkalmazzák majd ezt a rendszert.¹⁶ A Bizottság kétévenként köteles előrehaladási jelentést tenni az Európai Parlamentnek és a Tanácsnak a SIS II fejlesztéséről és a rendszer első generációjáról való esetleges áttérésről¹⁷.

Az **EURODAC** kialakítása visszakövethető a belső határok megszüntetéséig, ami szükségessé tette a menedékjog iránti kérelmek feldolgozására vonatkozó világos szabályok megállapítását. Az EURODAC központosított és automatizált ujjlenyomat-azonosító rendszer, amely harmadik országok egyes állampolgárainak ujjlenyomat-adatait tartalmazza. A rendszer 2003 januárja óta működik. Célja segítséget nyújtani annak megállapításában, hogy a dublini egyezmény értelmében melyik tagállam illetékes egy konkrét menedékjog iránti kérelem megvizsgálására.¹⁸ Automatikusan ujjlenyomatot vesznek azoktól a 14 éves vagy idősebb személyektől, akik menedéket kérnek valamely tagállamban, amint azoktól a harmadik országbeli állampolgároktól is, akiket a külső határok jogellenes átlépése miatt fogtak el. Az említett személyek ujjlenyomatainak az EURODAC-ban tárolt adatokkal való összevetése révén a nemzeti hatóságok annak megállapítására törekednek, hogy az adott személy nyújthatott-e már be menedékjog iránti kérelmet vagy első ízben lépett az Európai Unió területére. A hatóságok az EURODAC-ban tárolt adatokat összehasonlíthatják a területükön jogellenesen tartózkodó harmadik országbeli állampolgárok ujjlenyomataival is. A tagállamoknak meg kell adniuk az ezen adatbázishoz hozzáféréssel rendelkező hatóságok jegyzékét, amely általában a menekültügyi és migrációs hatóságokat, a határőrséget és a rendőrséget öleli fel. A tagállamok nemzeti hozzáférési pontjaikon keresztül töltik fel a vonatkozó adatokat a központi adatbázisba. Az EURODAC-ban tárolt személyes adatok kizárólag a dublini rendelet alkalmazásának megkönnyítése céljából használhatók fel; bármely egyéb felhasználás büntetendő. A menedékkérők ujjlenyomatait 10 évig tárolják; az illegális migránsokét pedig két évig. A menedékkérők adatait törlik, amikor megszerezték egy tagállam állampolgárságát; az illegális migránsokét pedig akkor törlik, ha tartózkodási engedélyt vagy állampolgárságot kaptak, illetve elhagyták a tagállamok területét. A személyes adatok ezen eszköz keretében történő feldolgozására a 95/46/EK irányelv alkalmazandó.¹⁹ Az EURODAC a Bizottság s-TESTA hálózatán üzemel, és minden tagállamban, valamint Norvégiában, Izlandon és Svájcban alkalmazandó. Előkészületben van a Liechtenstein csatlakozását lehetővé tévő megállapodás megkötése. A Bizottság évente köteles jelentést benyújtani az Európai Parlamentnek és a Tanácsnak az EURODAC központi egység működéséről.

a személyes adatok rendőri ágazatban való felhasználásának szabályozásáról, Európa Tanács, 1987.9.17. (rendőrségi ajánlás).

¹⁵ Az S-TESTA – vagyis Secure Trans-European Services for Telematics between Administrations (a közigazgatási szervek közötti biztonságos transzeurópai telematikai szolgáltatások) – a Bizottság által finanszírozott adatkommunikációs hálózat, amely lehetővé teszi a nemzeti közigazgatások és az uniós intézmények, ügynökségek és testületek közötti biztonságos és titkosított információcserét.

¹⁶ Az Egyesült Királyság és Írország részt vesz majd a SIS II-ben a beutazási tilalmi listán szereplő harmadik országbeli állampolgárokkal kapcsolatos figyelmeztető jelzések kivételével.

¹⁷ 1104/2008/EK tanácsi rendelet, HL L 299., 2008.11.8., 1. o.; A Tanács 2008/839/IB határozata, HL L 299., 2008.11.8., 43. o.

¹⁸ A Tanács 343/2003/EK rendelet, HL L 50., 2003.2.25., 1. o. (dublini rendelet), a Tanács 2725/2000/EK rendelete, HL L 316., 2000.12.15., 1. o. (EURODAC rendelet). E jogi aktusok az 1990. évi dublini egyezményre épülnek (HL C 254., 1997.8.19., 1. o.), amely meg kívánta határozni, hogy melyik tagállamnak kell megvizsgálnia a menedékjog iránti kérelmeket. A menedékjog iránti kérelmek vizsgálatára irányuló rendszer „dublini rendszerként” ismert.

¹⁹ 95/46/EK irányelv, HL L 281., 1995.11.23., 31. o.

A 2001. szeptember 11-i támadásokat követően a tagállamok elhatározták, hogy a rövid távú tartózkodásra jogosító vízumokra vonatkozó információcserére szolgáló formanyomtatvány megalkotása révén felgyorsítják a vízümpolitika végrehajtását.²⁰ A belső határok megszüntetése megkönnyítette a tagállami vízümszabályozások kijátszását is. A **Vízuminformációs Rendszer (VIS)** mind a két problémát orvosolni szándékozik: célja a közös vízümpolitika végrehajtásának elősegítése a vízümkérelmek vizsgálatának és a külső határellenőrzéseknek a megkönnyítése révén, miközben hozzájárul a tagállamok belső biztonságát érő fenyegetések megelőzéséhez.²¹ A VIS az egyes résztvevő tagállamokban található nemzeti részből és a franciaországi technikai támogató funkcióból álló központosított információs rendszer lesz majd. Biometrikus adatok egyeztetésére szolgáló rendszert fog alkalmazni az ujjlenyomat-összehasonlítások megbízhatóságának biztosítására, továbbá a vízümbirtokosok személyazonosságának a külső határokon történő ellenőrzésére. A VIS rendszer tartalmaz majd vízümkérelmekre vonatkozó adatokat, fényképeket, ujjlenyomatokat, a vízümhatóságok vonatkozó határozatait és az összefüggő kérelmek közötti kapcsolatokat. A vízüm, menekültügyi, bevándorlási és határellenőrzési hatóságok a vízümbirtokosok személyazonosságának és a vízümök eredetiségének ellenőrzése céljából férhetnek majd hozzá ehhez az adatbázishoz; a rendőrség és az Europol pedig a terrorizmus és a súlyos bűnözés egyéb formái elleni küzdelem és azok megelőzése céljából tekinthet bele.²² A kérelmek iratait öt évig őrizhetik meg. A VIS-ben tárolt személyes adatok feldolgozását úgy kell végezni, hogy az megfeleljen az e rendszert szabályozó alap-jogiaktusok (a 767/2008/EK rendelet és a 2008/633/IB tanácsi határozat) különös szabályainak, amelyek kiegészítik a 95/46/EK irányelv, a 45/2001/EK rendelet, a 2008/977/IB tanácsi kerethatározat, az Európa Tanács 108. egyezménye, annak 181. kiegészítő jegyzőkönyve és a rendőrségi ajánlás rendelkezéseit.²³ A VIS-t kell majd alkalmazni mindegyik tagállamban (az Egyesült Királyság és Írország kivételével), valamint Svájcban, Norvégiában és Izlandon. A rendszer a Bizottság s-TESTA hálózatának bázisán üzemel majd. A Bizottság a rendszer elindítása után három évvel és azt követően négyévente értékeli azt.

A Tanács 2004-ben spanyol kezdeményezésre irányelvet fogadott el az **előzetes utasinformációs adatoknak** (a továbbiakban: API) a légi fuvarozók részéről a határellenőrző hatóságoknak történő átadásáról.²⁴ E jogi aktus célja a határellenőrzés javítása és az illegális migráció elleni küzdelem. A légi fuvarozóknak kérelemre közölniük kell a határellenőrző hatóságokkal a harmadik országokból az Unió területére beutazó utasok nevét, születési idejét, állampolgárságát, beszállási helyét és beutazási határátkelőhelyét. Ezek a személyes adatok általában az utasok útlevelének géppel leolvasható részéről származnak, és az

²⁰ Rendkívüli Bel- és Igazságügyi Tanács, 2001.9.20.

²¹ A Tanács 2004/512/EK határozata, HL L 213., 2004.6.15., 5. o.; 767/2008/EK rendelet, HL L 218., 2008.8.13., 60. o.; A Tanács 2008/633/IB határozata, HL L 218., 2008.8.13., 129. o. Lásd továbbá az Európai Tanács terrorizmus elleni küzdelemről szóló, 2004. március 25-i nyilatkozatát.

²² A Tanács 2008/633/IB határozata, HL L 218., 2008.8.13., 129. o.

²³ 767/2008/EK rendelet, HL L 218., 2008.8.13., 60. o.; A Tanács 2008/633/IB határozata, HL L 218., 2008.8.13., 129. o.; 95/46/EK irányelv, HL L 281., 1995.11.23., 31. o.; 45/2001/EK rendelet, HL L 8., 2001.1.12., 1. o.; A Tanács 2008/977/IB kerethatározata, HL L 350., 2008.12.30., 60. o.; Egyezmény az egyének védelméről a személyes adatok gépi feldolgozása során (ETS 108. sz.), Európa Tanács 1981.1.28. (az Európa Tanács 108. egyezménye); A személyes adatok gépi feldolgozása során az egyének védelméről szóló egyezménynek a felügyelő hatóságokról és a személyes adatok országhatárokat átlépő áramlásáról szóló kiegészítő jegyzőkönyve (181. sz. ETS), Európa Tanács, 2001.11.8. (181. kiegészítő jegyzőkönyv); A Miniszterek Tanácsa R (87) 15. sz. ajánlása a személyes adatok rendőri ágazatban való felhasználásának szabályozásáról, Európa Tanács, 1987.9.17. (rendőrségi ajánlás).

²⁴ A Tanács 2004/82/EK irányelve, HL L 261., 2004.8.6., 24.o.

utasfelvétel befejezése után továbbítják azokat a hatóságoknak. A járat megérkezése után a hatóságok és a légi fuvarozók 24 óráig őrizhetik meg az API-adatokat. Az API-rendszer decentralizált módon, a magánüzemeltetők és a hatóságok közötti információ-megosztás révén működik. Az említett jogi aktus nem teszi lehetővé az API-adatok tagállamok közötti cseréjét; viszont a határőrségtől eltérő bűnüldöző hatóságok bűnüldözési célokból hozzáférést kérhetnek ezekhez az információkhoz. A hatóságok kizárólag a határellenőrzés és az illegális migráció elleni küzdelem céljából használhatják fel az személyes adatokat, amelyeket a 95/46/EK irányelvnek megfelelően kell feldolgozni.²⁵ Ezt az egész Unióban hatályos jogi aktust csupán kevés tagállam alkalmazza. A Bizottság 2011-ben felülvizsgálja az irányelvet.

A Bizottság belső piacot létrehozó 1992-es programjának jelentős része érintette a Közösségen belül mozgó árukra vonatkozó ellenőrzések és formalitások teljes eltörlését.²⁶ Az ilyen eljárásoknak a belső határokon történő megszüntetése megnövelte a csalás kockázatát, ez pedig szükségessé tette, hogy a tagállamok egyfelől kölcsönös segítségnyújtási mechanizmust hozzanak létre a közösségi vámügyi és mezőgazdasági jogszabályokba ütköző műveletek megelőzésének, kivizsgálásának és üldözésének támogatására, másfelől pedig vámügyi együttműködést építsenek ki azzal a céllal, hogy különösen a határokon átnyúló információcsere erősítése révén lehetővé tegyék a nemzeti vámrendelkezések megsértéseinek felderítését és üldözését. A vámigazgatási szervek közötti kölcsönös segítségnyújtásról és együttműködésről szóló **II. Nápolyi Egyezmény** célja, hogy – a vámunióra vonatkozó uniós hatáskör sérelme nélkül²⁷ – feljogosítsa a nemzeti vámigazgatási szerveket a nemzeti vámrendelkezések megsértésének megelőzésére és felderítésére, továbbá hogy segítse őket a közösségi és a nemzeti vámrendelkezések megsértésének üldözése és megbüntetése során.²⁸ E jogi aktus alapján számos központi koordináló egység kérhet írásban segítséget a többi tagállambeli társszervezeteitől a nemzeti és az uniós vámszabályok megsértése ügyében folytatott bűnügyi nyomozásokhoz. Az említett egységek kizárólag a II. Nápolyi Egyezmény alkalmazásában dolgozhatnak fel személyes adatokat. Továbbíthatják ezeket az adatokat a nemzeti vámhatóságoknak, nyomozó hatóságoknak és bíróságoknak, valamint – az adatokat szolgáltató tagállam előzetes hozzájárulásával – egyéb hatóságoknak. Az adatok a megadásuk céljának eléréséhez szükséges időtartamot meg nem haladó ideig őrizhetők meg. A személyes adatok a fogadó tagállamban legalább azonos szintű védelemben részesülnek, mint a szolgáltató tagállamban, továbbá feldolgozásuknak meg kell felelnie a 95/46/EK irányelv és a 108. Európa tanácsi egyezmény rendelkezéseinek.²⁹ A II. Nápolyi Egyezményt mindegyik tagállam ratifikálta. A tagállamok javaslatot tehetnek az egyezmény módosítására, ezt követően a Miniszterek Tanácsának el kell fogadnia a módosított szöveget, a tagállamoknak pedig ratifikálniuk kell azt.

A II. Nápolyi Egyezményt kiegészítő VIR-egyezmény **váminformációs rendszert** (a továbbiakban: VIR) épít ki, hogy segítse a nemzeti jogszabályok súlyos megsértésének

²⁵ 95/46/EK irányelv, HL L 281., 1995.11.23., 31. o.

²⁶ A Tanács 2913/92/EGK rendelete, HL L 302., 1992.10.19.

²⁷ Az Európai Unióról szóló szerződés K.3. cikke alapján kidolgozott, a vámigazgatási szervek közötti kölcsönös jogsegélyről és együttműködésről szóló egyezmény, HL C 24., 1998.1.23., 2. o. (II. Nápolyi Egyezmény).

²⁸ A 766/2008/EK rendelettel, HL L 218., 2008.8.13., 48. o., módosított, a tagállamok közigazgatási hatóságai közötti kölcsönös segítségnyújtásról, valamint a vám- és mezőgazdasági jogszabályok helyes alkalmazásának biztosítása érdekében e hatóságok és a Bizottság együttműködéséről szóló, 1997. március 13-i 515/97/EK tanácsi rendelet, HL L 82., 1997.3.22., 1. o.

²⁹ 95/46/EK irányelv, HL L 281., 1995.11.23., 31. o.; Egyezmény az egyének védelméről a személyes adatok gépi feldolgozása során (ETS 108. sz.), Európa Tanács 1981.1.28. (az Európa Tanács 108. egyezménye).

megelőzését, kivizsgálását és a büntetőeljárás lefolytatását az információk gyorsabb hozzáférhetővé tétele révén és ezáltal javítva a tagállamok vámigazgatási szervei által folytatott együttműködés hatékonyságát.³⁰ A Bizottság által igazgatott VIR centralizált információs rendszer, amelyet az egyes tagállamok és a Bizottság, az Europol és az Eurojust termináljain keresztül lehet elérni. A rendszer nyersanyagokkal, szállítóeszközökkel, vállalkozásokkal, személyekkel, valamint a visszatartott, lefoglalt vagy elkobozott árukkal és készpénzzel kapcsolatos személyes adatokat tartalmaz. A személyes adatok közé az alábbiak tartoznak: nevek és felvett nevek, születési idő és hely, állampolgárság, nem, fizikai jellemzők, személyazonosító okmányok, cím, korábbi erőszakos cselekmény, a VIR-be történő adatfelvétel oka, javasolt intézkedés, a szállítóeszköz rendszáma. Visszatartott, lefoglalt vagy elkobozott áruk és készpénz esetén csak a születési adatok és a cím vihető be a VIR-be. Az említett információk kizárólag az alábbi célokból használhatók fel: megfigyelés és jelentéstétel, leplezett megfigyelés vagy célzott ellenőrzés, illetve stratégiai vagy operatív elemzés olyan személyre vonatkozóan, aki a nemzeti vámügyi jogszabályok megsértésével gyanúsítható. A nemzeti vám-, adó-, mezőgazdasági, közegészségügyi és rendőri hatóságok, az Europol és az Eurojust férhetnek hozzá a VIR-adatokhoz³¹. A személyes adatok feldolgozásának meg kell felelnie a VIR-egyezmény által megállapított különös szabályoknak, valamint a 95/46/EK irányelv, a 45/2001/EK rendelet, a 108. Európa tanácsi egyezmény és a rendőrségi ajánlás rendelkezéseinek.³² A VIR-be felvett személyes adatok kizárólag a kockázatkezelő vagy operatív elemzési adatkezelő rendszerekbe másolhatók át, és csak a tagállamok által kijelölt elemzők férhetnek hozzá azokhoz. A VIR-ből másolt személyes adatokat csak a kimásolás céljának eléréséhez szükséges ideig, és legfeljebb 10 évig szabad tárolni. A VIR létrehozta továbbá a **vámügyirat-azonosítási adatbázist** (a továbbiakban: FIDE), hogy elősegítse a nemzeti jogszabályok súlyos megsértésének megelőzését, felderítését és üldözését.³³ A FIDE lehetővé teszi, hogy amikor a vámügyi nyomozások lefolytatására hatáskörrel rendelkező nemzeti hatóságok vizsgálatot indítanak, azonosítani tudják azokat az egyéb hatóságokat, amelyek vizsgálatot folytatnak vagy folytattak az érintett egyénnel vagy vállalkozásokkal kapcsolatban. Az említett hatóságok vizsgálati ügyirataikból adatokat vehetnek fel a FIDE-be, beleértve a vizsgálat alatt álló személy születési adatait, és a vizsgált vállalkozás nevét, kereskedelmi nevét, hea-azonosító számát és címét. Amennyiben nem derült fény vámcsalásra, a vizsgálati ügyiratokból származó adatok legfeljebb három évig tárolhatók; ha pedig vámcsalást lepleztek le, legfeljebb hat évig; illetve amennyiben büntetőítélet vagy bírság kiszabására is sor került, akkor legfeljebb 10 évig. A VIR és a FIDE közös kommunikációs hálózatot, közös rendszerinterfész-hálózatot vagy a Bizottság által nyújtott biztonságos internet-hozzáférést

³⁰ A 2009/917/IB tanácsi határozattal, HL L 323., 2009.12.10., 20. o., módosított, az informatika vámügyi alkalmazásáról szóló, az Európai Unióról szóló szerződés K. 3. cikke alapján létrehozott egyezmény, HL C 316., 1995.11.27., 34. o.

³¹ 2011 májusától az Europol és az Eurojust betekinthez a VIR-be a 2009/917/IB tanácsi határozat alapján (HL L 323., 2009.12.10., 20. o.).

³² A 2009/917/IB tanácsi határozattal, HL L 323., 2009.12.10., 20. o., módosított, az informatika vámügyi alkalmazásáról szóló, az Európai Unióról szóló szerződés K. 3. cikke alapján létrehozott egyezmény, HL C 316., 1995.11.27., 34. o.; a 95/46/EK irányelv, HL L 281., 1995.11.23., 31. o.; 45/2001/EK rendelet, HL L 8., 2001.1.12., 1. o.; a személyes adatok gépi feldolgozása során az egyének védelméről szóló (ETS 108. sz.) egyezmény, Európa Tanács, 1981.1.28. (az Európa Tanács 108. egyezménye); A Miniszterek Tanácsa R (87) 15. sz. ajánlása a személyes adatok rendőri ágazatban való felhasználásának szabályozásáról, Európa Tanács, 1987.9.17. (rendőrségi ajánlás).

³³ A FIDE – vagyis a *Fichier d'Identification des Dossiers d'Enquêtes douanières* – a 766/2008/EK tanácsi rendeletre, valamint az Európai Unióról szóló szerződés 34. cikkének megfelelően az informatika vámügyi alkalmazásáról szóló egyezménynek egy vámügyirat-azonosítási adatbázis létrehozása tekintetében történő módosításáról szóló egyezményre, HL C 139., 2003.6.13., 1. o., épül.

alkalmaz. A VIR valamennyi tagállamban hatályban van. A Bizottság a tagállamokkal együttműködve évente jelentést tesz az Európai Parlamentnek és a Tanácsnak a VIR működéséről.

A terrorizmus és a határokon átnyúló súlyos bűnözés egyéb formáinak megelőzésére és leküzdésére irányuló uniós eszközök

A 2004. márciusi madridi terrortámadás következtében több új, uniós szintű kezdeményezés jött létre. Az Európai Tanács felkérésére a Bizottság 2005-ben javaslatot terjesztett elő az információcserét a hozzáférhetőség elve alapján szabályozó eszközre.³⁴ E javaslat jóváhagyása helyett a Tanács 2006-ban azt a **svéd kezdeményezést** fogadta el, amely leegyszerűsíti bármely olyan meglévő információ vagy bűnüldözési operatív információ megosztását a tagállamok között, amely szükséges lehet nyomozások vagy bűnüldözési operatív műveletek lefolytatásához.³⁵ Ez a jogi aktus az „egyenlő hozzáférés” szakpolitikai elvére épül, amelynek értelmében a határokon átnyúló adatcserére alkalmazandó feltételek nem lehetnek szigorúbbak a belföldi hozzáférést szabályozóknál. A svéd kezdeményezés decentralizált módon működik, valamint lehetővé teszi a bűncselekmények kivizsgálására hatáskörrel rendelkező rendőrségi, vám- és egyéb hatóságok számára (a hírszerző szolgálatok kivételével, amelyek általában a nemzet- vagy állambiztonsággal kapcsolatos operatív információkat kezelik), hogy megosszák az információkat és a bűnüldözési operatív információkat az EU-n belüli társhatóságokkal. A tagállamoknak nemzeti kapcsolattartó pontokat kell kijelölniük a sürgős információkérések kezelésére. Az említett intézkedés világos határidőket szab az információcsere számára, és előírja, hogy a tagállamoknak adatkéréskor formanyomtatványt kell kitölteniük. A tagállamok kötelesek az információ vagy operatív információ iránti kérelmeket sürgős esetekben 8 órán belül, nem sürgős esetekben egy héten belül, illetve minden egyéb esetben két héten belül megválaszolni. Az ezen eszköz útján megkapott információk és operatív információk felhasználása a belföldi adatvédelmi jogszabályok hatálya alá tartozik, amennyiben a tagállamok nem alkalmazhatnak eltérő bánásmódot a belföldről, illetve a más tagállamokból származó adatok esetében. Az adatokat átadó tagállam azonban feltételekhez kötheti az információk és operatív információk felhasználását a többi tagállamban. A személyes adatok feldolgozását a nemzeti adatvédelmi jogszabályokkal, valamint az Európa Tanács 108. egyezményével, annak 181. kiegészítő jegyzőkönyvével és a rendőrségi ajánlással összhangban kell végezni.³⁶ A szóban forgó intézkedés 31 aláírója (beleértve az uniós tagállamokat, valamint Norvégiát, Izlandot, Svájcot, és Liechtensteint) közül 12 nemzeti jogszabályt fogadott el annak végrehajtására; öt állam az információkéréshez rendszeresen kitölti a formanyomtatványt, viszont csak két állam használja azt rendszeresen információcserére.³⁷ A Bizottságnak 2010 végéig kell benyújtania értékelő jelentését a Tanácsnak.

³⁴ COM(2005) 490, 2005.10.12.; Elnökségi következtetések – A Hágai Program, 2004.11.5., 4.o. Lásd továbbá az Európai Tanács terrorizmus elleni küzdelemről szóló, 2004. március 25-i nyilatkozatát.

³⁵ A Tanács 2006/960/IB kerethatározata, HL L 386., 2006.12.29., 89. o.;

³⁶ Egyezmény az egyének védelméről a személyes adatok gépi feldolgozása során (ETS 108. sz.), Európa Tanács 1981.1.28. (az Európa Tanács 108. egyezménye); A személyes adatok gépi feldolgozása során az egyének védelméről szóló egyezménynek a felügyelő hatóságokról és a személyes adatok országhatárokat átlépő áramlásáról szóló kiegészítő jegyzőkönyve (181. sz. ETS), Európa Tanács, 2001.11.8. (181. kiegészítő jegyzőkönyv); A Miniszterek Tanácsa R (87) 15. sz. ajánlása a személyes adatok rendőri ágazatban való felhasználásának szabályozásáról, Európa Tanács, 1987.9.17. (rendőrségi ajánlás).

³⁷ Ez az információ egy kérdőívre adott válaszokra alapul. Ennek eredményeit a Tanács spanyol elnöksége mutatta be az információcserével foglalkozó ad hoc tanácsi munkacsoport 2010. június 22-i ülésén.

A **prümi határozat** a Németország, Franciaország, Spanyolország, a Benelux államok és Ausztria által megkötött 2005. évi megállapodásra épül, amelynek célja a terrorizmus, a határokon átnyúló bűnözés és az illegális migráció elleni küzdelem terén folytatott együttműködés erősítése. Németország 2007. évi tanácsi elnöksége alatt javaslatot tett a megállapodás uniós jogi aktussá történő átalakítására, mivel több tagállam kifejezésre juttatta, hogy érdeklődik az említett megállapodáshoz való csatlakozás iránt. A 2011. augusztusig végrehajtandó 2008-as prümi határozat meghatározza a DNS-profilok, az ujjlenyomatok, a gépjármű-nyilvántartási adatok, és a terrortámadások tervezésével gyanúsított személyekre vonatkozó információk határokon átnyúló cseréjére vonatkozó szabályokat.³⁸ A jogszabály arra törekszik, hogy javítsa a bűncselekmények – különösen a terrorizmus és a határokon átnyúló bűnözés – megelőzését, valamint a nagyszabású események kapcsán a közrend fenntartását. Ez a rendszer decentralizált módon működik majd akképpen, hogy a nemzeti kapcsolattartó pontokon keresztül összekapcsolják egymással a részt vevő államok DNS, ujjlenyomat, és gépjármű-nyilvántartási adatbázisait. A kapcsolattartó pontok a Bizottság s-TESTA hálózatát alkalmazva kezelik majd a DNS-profilok, ujjlenyomatok és gépjármű-nyilvántartási adatok határokon átnyúló összehasonlítása iránti beérkező és kimenő kéréseket. Az ilyen adatok végfelhasználók számára történő továbbítására vonatkozó hatáskörök tekintetében a nemzeti jog az irányadó. 2011 augusztusától az adat összehasonlítás teljesen automatizáltan működik. Mindazonáltal a tagállamokat szigorú értékelési eljárásnak (amely kiváltképpen azt vizsgálja, hogy megfelelnek-e az adatvédelmi és technikai követelményeknek) vetik alá ahhoz, hogy engedélyt kapjanak az automatizált adatmegosztásra. Az eszköz keretében személyes adatok nem cserélhetők ki mindaddig, amíg a tagállamok nem garantálnak legalább azonos adatvédelmi szintet az Európa Tanács 108. egyezményéből, annak 181. kiegészítő jegyzőkönyvéből és a rendőrségi ajánlásból következő normákkal.³⁹ A Tanács egyhangúlag határoz majd arról, hogy e feltétel teljesült-e. A személyes adatok csak arra célra használhatók fel, amelyre megkapták azokat, kivéve ha az adatokat szolgáltató tagállam beleegyezik az eltérő célokra való felhasználásukba. Egyének a 95/46/EK irányelv alapján kijelölt nemzeti adatvédelmi tisztviselőhöz is fordulhatnak, hogy érvényt szerezzenek a jogaiknak a személyes adatok ezen eszköz keretében történő feldolgozása során. A DNS-profilok és ujjlenyomatok összehasonlítása „találat/nincs találat” alapon (névtelenül) történik majd, ezáltal a hatóságok csak akkor kérhetnek további személyes adatokat az érintettől, ha az eredeti keresés találatot eredményezett. Az ilyen tovább információk iránti kérésekre általában a svéd kezdeményezés keretében kerül majd sor. Az EU 27 tagállama most hajtja végre a prümi határozatot, Norvégia és Izland pedig megkezdte a csatlakozási folyamatot.⁴⁰ A Bizottságnak 2012-ben kell benyújtania jelentését a Tanácsnak.

³⁸ A Tanács 2008/615/IB határozata, HL L 210., 2008.8.6., 1. o.; A Tanács 2008/616/IB határozata, HL L 210., 2008.8.6., 12. o.

³⁹ Egyezmény az egyének védelméről a személyes adatok gépi feldolgozása során (ETS 108. sz.), Európa Tanács 1981.1.28. (az Európa Tanács 108. egyezménye); A személyes adatok gépi feldolgozása során az egyének védelméről szóló egyezménynek a felügyelő hatóságokról és a személyes adatok országhatárokat átlépő áramlásáról szóló kiegészítő jegyzőkönyve (181. sz. ETS), Európa Tanács, 2001.11.8. (181. kiegészítő jegyzőkönyv); A Miniszterek Tanácsa R (87) 15. sz. ajánlása a személyes adatok rendőri ágazatban való felhasználásának szabályozásáról, Európa Tanács, 1987.9.17. (rendőrségi ajánlás).

⁴⁰ Mostanáig tíz tagállam kapott engedélyt a DNS-profilok, öt az ujjlenyomatok, hét pedig a gépjármű-nyilvántartási adatok automatizált cseréjének megkezdésére. Németország, Ausztria, Spanyolország és Hollandia részleges statisztikai adatokat szolgáltatott a Bizottságnak arról, hogy miként használják ezt az eszközt.

A 2005. évi londoni bombatámadásra válaszul Nagy Britannia, Írország, Svédország és Franciaország az adatmegőrzésre alkalmazandó nemzeti szabályokat összehangoló uniós jogi aktusra tett javaslatot. A 2006. évi **adatmegőrzési irányelv** arra kötelezi a telefon- és az internetszolgáltatókat, hogy a súlyos bűncselekmények megelőzése, kivizsgálása, felderítése és üldözése céljából őrizzék meg az elektronikus kommunikációs forgalmi és helymeghatározó adatokat, valamint az előfizetőkkel kapcsolatos információkat (ideértve a telefonszámukat, IP címüket és a mobilberendezési azonosítót).⁴¹ Az adatmegőrzési irányelv sem a nemzeti hatóságok által megőrzött adatokhoz való hozzáférést, sem azok felhasználását nem szabályozza. Kifejezetten kizárja alkalmazási köréből az elektronikus közlés tartalmát; más megfogalmazásban, e jogi aktus alapján nincs lehetőség lehallgatásra. Ezen intézkedés meghagyja a tagállamoknak a „súlyos bűncselekmény” fogalmának meghatározását. A tagállamok határozzák meg továbbá, hogy esetenként mely nemzeti hatóságok férhetnek hozzá az említett adatokhoz, továbbá hogy milyen eljárásban és feltételekkel biztosítanak hozzáférést az információkhoz. Az adatmegőrzési időszak 6-tól 24 hónapig terjed. A személyes adatok e jogi aktus keretében történő védelmét a 95/46/EK irányelv és a 2002/58/EK irányelv szabályozza.⁴² Hat tagállam még nem ültette át teljes mértékben ezt az intézkedést, a német és a román alkotmánybíróság pedig alkotmányellenesnek nyilvánította a nemzeti végrehajtási jogszabályokat. A német alkotmánybíróság megállapítása szerint az adatokhoz való hozzáférést és az azok felhasználását szabályozó, nemzeti jogszabályban megállapított szabályok alkotmányellenesek.⁴³ A román alkotmánybíróság kimondta, hogy az adatmegőrzés önmagában is az emberi jogok és alapvető szabadságok védelméről szóló európai egyezményének (a továbbiakban: az emberi jogok európai egyezménye) 8. cikkébe ütközik, és ennélfogva alkotmányellenes.⁴⁴ A Bizottság jelenleg értékeli ezt a jogi aktust, és várhatóan 2010 végén nyújtja be értékelő jelentését az Európai Parlamentnek és a Tanácsnak.

A jelenleg kialakítás alatt álló **Európai Bűnügyi Nyilvántartási Információs Rendszer** (ECRIS) visszavezethető ahhoz a 2004. évi belga kezdeményezéshez, amely azt tűzte ki célul, hogy az elítélt szexuális bűnözőket a többi tagállamban is eltiltsák a gyermekekkel kapcsolatos munkától. A tagállamok korábban az Európa Tanács kölcsönös bűnügyi jogsegélyről szóló egyezményét alkalmazták a nemzeti büntetőítéletekkel kapcsolatos információk kicserélésére, ez a rendszer azonban nem bizonyult hatékonynak.⁴⁵ A Tanács megtette az első reformlépést a 2005/876/IB tanácsi határozat elfogadásával, amely előírja, hogy minden tagállam állítson fel egy központi hatóságot, amely rendszeresen megküldené a külföldiek ügyében hozott büntető ítéleteket az állampolgárságuk szerinti tagállamnak.⁴⁶ E jogi aktus első alkalommal és a nemzeti jogtól függően azt is lehetővé teszi a tagállamok számára, hogy megkapják a saját állampolgáraikkal szemben más tagállamokban hozott korábbi büntetőítéleteket. A tagállamok a kölcsönös jogsegélyre vonatkozó eljárás igénybevétele helyett formanyomtatvány kitöltésével kérhetnék meg ezeket az információkat. 2006-ban és 2007-ben a Bizottság az alábbi három jogi aktusból álló, átfogó jogalkotási csomagot terjesztett elő: a Tanács 2008/675/IB kerethatározata az Európai Unió más tagállamaiban hozott ítéleteknek egy új büntetőeljárásban való figyelembevételéről; a Tanács 2009/315/IB kerethatározata a bűnügyi nyilvántartásból származó információk tagállamok

⁴¹ 2006/24/EK irányelv, HL L 105., 2006.4.13., 54. o.

⁴² 95/46/EK irányelv, HL L 281., 1995.11.23., 31. o; 2002/58/EK irányelv, HL L 201., 2002.7.31., 37. o. (e-magánélet irányelv).

⁴³ A német alkotmánybíróság ítélete, Bundesverfassungsgericht 1 BvR 256/08., 2008.3.11.

⁴⁴ A román alkotmánybíróság 1258. sz. határozata, 2009.10.8.

⁴⁵ A kölcsönös bűnügyi jogsegélyről szóló európai egyezmény (ETS 30. sz.), Európa Tanács, 1959.4.20. Lásd továbbá: COM(2005)10., 2005.1.25.

⁴⁶ A Tanács 2005/876/IB határozata, HL L 322., 2005.12.9., 33. o.

közötti cseréjének megszervezéséről és azok tartalmáról; valamint a Tanács 2009/316/IB határozata az Európai Bűnügyi Nyilvántartási Információs Rendszer (ECRIS) létrehozásáról a bűnügyi nyilvántartásokból származó információk kicserélésének technikai eszközeként.⁴⁷ A 2012. áprilisig átültetendő 2009/315/IB és 2009/316/IB tanácsi kerethatározatok célja azon módszerek meghatározása, amelyek szerint az ítélethozatal szerinti tagállamnak egy új ítélettel kapcsolatos információt továbbítani kell az elítélt személy állampolgársága szerinti tagállamnak, továbbá a megőrzési kötelezettségek és a információcserét szolgáló számítógépes rendszer keretének megállapítása. Az ECRIS decentralizált információs rendszer lesz, amely a Bizottság s-TESTA hálózatán keresztül összekapcsolja a tagállamok bűnügyi nyilvántartási adatbázisait. A központi hatóságok kicserélik majd az állampolgárok ügyében hozott új büntetőítéletekkel kapcsolatos adatokat és a bűnügyi nyilvántartásokban szereplő korábbi adatokat. Titkosítják, és az előre meghatározott formátumnak megfelelően strukturálják az adatokat, amelyek az alábbiakat ölelik fel: születési adatok; a büntető ítélet, a büntetés és az azt megalapozó bűncselekmény; valamint kiegészítő információk (beleértve az ujjlenyomatokat, amennyiben rendelkezésre állnak). 2012. áprilistól a folyamatban lévő büntetőeljárásokhoz bűnügyi nyilvántartásból származó információkat kell szolgáltatni, és meg kell azokat küldeni a bíróságoknak vagy az illetékes közigazgatási hatóságoknak, így például az érzékeny foglalkoztatás vagy lőfegyverek birtoklása céljából személyek átvilágítására felhatalmazott testületeknek. A büntetőeljárás céljából szolgáltatott személyes adatok csak az adott célra használhatóak fel; bármely egyéb célra történő felhasználásukhoz az adatokat szolgáltató tagállam hozzájárulása szükséges. A személyes adatok feldolgozását a 2005/876/IB tanácsi határozat szabályait is tartalmazó 2009/315/IB tanácsi határozatban megállapított különös szabályoknak megfelelően, valamint a 2008/977/IB tanácsi kerethatározattal és az Európa Tanács 108. egyezményével összhangban kell végezni.⁴⁸ Az uniós intézmények által az ECRIS felhasználásával végzett bármely – például adatbiztonsági célú – adatfeldolgozásra a 45/2001/EK rendelet alkalmazandó.⁴⁹ E jogalkotási csomag nem foglal magába adatmegőrzésre vonatkozó szabályokat, mivel a büntető ítéletekkel kapcsolatos információk tárolását a nemzeti jog szabályozza. Tizenöt tagállam részt vesz egy most folyó kísérleti programban, közülük kilenc megkezdte a bűnügyi nyilvántartásból származó adatok elektronikus cseréjét. A Bizottságnak két értékelő jelentést kell benyújtania az Európai Parlamentnek és a Tanácsnak e jogalkotási csomag érvényesüléséről: a 2008/675/IB kerethatározatot 2011-ben, a 2009/315/IB kerethatározatot pedig 2015-ben kell felülvizsgálni. 2016-tól a Bizottságnak az ECRIS működéséről is rendszeresen beszámolót kell közzétennie.

A Tanács 2000-ben finn kezdeményezésre jogi aktust fogadott el a tagállamok **pénzügyi hírszerző egységeinek** (FIU-k) a pénzmosás, illetve később a terrorizmus finanszírozása elleni küzdelem céljából zajló információcsere terén folytatott együttműködésének megszervezéséről.⁵⁰ A pénzügyi hírszerző egységeket általában a bűnüldöző szerveken, a bíróságokon vagy a pénzügyi hatóságoknak beszámoló közigazgatási testületeken belül hozzák létre. Az egységek kötelesek megosztani uniós társszervezeteikkel a szükséges pénzügyi vagy bűnüldözési adatokat, ideértve a pénzügyi tranzakciók adatait, kivéve ha az

⁴⁷ A Tanács 2008/675/IB kerethatározata, HL L 220., 2008.8.15., 32. o.; A Tanács 2009/315/IB kerethatározata, HL L 93., 2009.4.7., 23. o.; A Tanács 2009/316/IB határozata, HL L 93., 2009.4.7., 33. o. Lásd továbbá: COM(2005)10., 2005.1.25.

⁴⁸ A Tanács 2009/315/IB kerethatározata, HL L 93., 2009.4.7., 23. o.; A Tanács 2005/876/IB határozata, HL L 322., 2005.12.9., 33. o.; A Tanács 2008/977/IB kerethatározata, HL L 350., 2008.12.30., 60. o.; Egyezmény az egyének védelméről a személyes adatok gépi feldolgozása során (ETS 108. sz.), Európa Tanács 1981.1.28. (az Európa Tanács 108. egyezménye).

⁴⁹ 45/2001/EK rendelet, HL L 8., 2001.1.12., 1. o.

⁵⁰ A Tanács 2000/642/IB határozata, HL L 271., 2000.10.24., 4. o.

információk felfedése aránytalanul hátrányosan érintené egy természetes vagy jogi személy érdekeit. A pénzmosásnak vagy a terrorizmus finanszírozásának elemzése vagy vizsgálata céljából szolgáltatott információk bünyügyi nyomozások vagy büntetőeljárások során is felhasználhatók, kivéve ha az információkat szolgáltató tagállam az ilyen irányú felhasználást megtiltja. A személyes adatok feldolgozása során tiszteletben kell tartani a 2008/977/IB tanácsi kerethatározat, az Európa Tanács 108. egyezménye, és annak rendőrségi ajánlása rendelkezéseit.⁵¹ 2002-ben több tagállam létrehozta a FIU-net-et, egy olyan decentralizált hálózati alkalmazást, amely a pénzügyi hírszerző egységek közötti adatcserét kezeli, és a Bizottság s-TESTA hálózatán üzemel.⁵² E kezdeményezésnek húsz FIU tagja. Jelenleg megbeszélések folynak arról, hogy az Europol biztonságos SIENA alkalmazását vegyék igénybe a FIU-net működtetésére.⁵³ Miután megvizsgálta, hogy a tagállamok megfelelnek-e az említett jogi aktusnak, a Tanács a harmadik pénzmosás elleni irányelvben felhatalmazta a pénzügyi hírszerző egységeket a gyanús, lehetséges pénzmosásra és terrorizmus finanszírozására utaló ügyletekre vonatkozó bejelentések fogadására, elemzésére és továbbítására.⁵⁴ Pénzügyi szolgáltatásokról szóló cselekvési tervének részeként a Bizottság 2009 óta folytatja a harmadik pénzmosás elleni irányelv végrehajtásának felülvizsgálatát.⁵⁵

Egy Ausztria, Belgium és Finnország által javasolt kezdeményezést felkarolva a Tanács 2007-ben olyan jogi aktust fogadott el, amely a **vagyon-visszaszerzési hivatalok** közötti, a bűncselekményből származó jövedelmek felkutatása és azonosítása terén való együttműködés erősítésére törekszik.⁵⁶ A vagyon-visszaszerzési hivatalok a pénzügyi hírszerző egységekhez hasonlóan decentralizáltan működnek együtt, ámbar nem vehetik igénybe online platform segítségét. A hivatalok kötelesek a svéd kezdeményezést használni az információcserére, megadva a célzott tulajdon (pl.: bankszámlák, ingatlan és személygépkocsik) adatait, valamint a keresett természetes vagy jogi személy adatait, beleértve a nevet, címet, születési időt, részvényesekre vonatkozó vagy céges adatokat. Az ezen eszköz útján kicserélt információk felhasználása a belföldi adatvédelmi jogszabályok hatálya alá tartozik, amennyiben a tagállamok nem alkalmazhatnak eltérő bánásmódot a belföldről, illetve a más tagállamokból származó adatok esetében. A személyes adatok feldolgozását az Európa Tanács 108. egyezménye, annak 181. kiegészítő jegyzőkönyve és a rendőrségi ajánlás rendelkezéseinek megfelelően kell végezni.⁵⁷ Mostanáig húsznál több tagállam hozott létre vagyon-

⁵¹ A Tanács 2008/977/IB kerethatározata, HL L 350., 2008.12.30., 60. o.; Egyezmény az egyének védelméről a személyes adatok gépi feldolgozása során (ETS 108. sz.), Európa Tanács 1981.1.28. (az Európa Tanács 108. egyezménye); A Miniszterek Tanácsa R (87) 15. sz. ajánlása a személyes adatok rendőri ágazatban való felhasználásának szabályozásáról, Európa Tanács, 1987.9.17. (rendőrségi ajánlás).

⁵² <http://www.fiu.net/>

⁵³ SIENA: Secure Information Exchange Network Application (biztonságos információcsere-hálózati alkalmazás).

⁵⁴ 2005/60/EK irányelv, HL L 309., 2005.11.25., 15. o. (harmadik pénzmosás elleni irányelv).

⁵⁵ Lásd például: Evaluation of the economic impacts of the Financial Services Action Plan — Final report (for European Commission, DG MARKT) [A pénzügyi szolgáltatásokról szóló cselekvési terv gazdasági hatásainak értékelése – Zárójelentés (az Európai Bizottság Belső Piaci és Szolgáltatási Főigazgatósága számára)], CRA International, 2009. március

⁵⁶ A Tanács 2007/845/IB határozata, HL L 332., 2007.12.18., 103. o.

⁵⁷ Egyezmény az egyének védelméről a személyes adatok gépi feldolgozása során (ETS 108. sz.), Európa Tanács 1981.1.28. (az Európa Tanács 108. egyezménye); A személyes adatok gépi feldolgozása során az egyének védelméről szóló egyezménynek a felügyelő hatóságokról és a személyes adatok országhatárokat átlépő áramlásáról szóló kiegészítő jegyzőkönyve (181. sz. ETS), Európa Tanács, 2001.11.8. (181. kiegészítő jegyzőkönyv); A Miniszterek Tanácsa R (87) 15. sz. ajánlása a személyes adatok rendőri ágazatban való felhasználásának szabályozásáról, Európa Tanács, 1987.9.17. (rendőrségi ajánlás).

visszaszerzési hivatal. A kicserélt információk érzékeny jellegére figyelemmel jelenleg megbeszélések folynak arról, hogy az Europol biztonságos SIENA alkalmazását vegyék igénybe a vagyon-visszaszerzési hivatalok közötti adatmegosztásra. Egy 2010. májusban elindult kísérleti projekt keretében tizenkét vagyon-visszaszerzési hivatal kezdte használni a SIENA-t a vagyontárgyak nyomkövetésére vonatkozó információk megosztására. A Bizottságnak 2010-ben kell értékelő jelentést benyújtania a Tanácsnak.

2008-ban a Tanács francia elnöksége felkérte a tagállamokat, hogy hozzanak létre **számítástechnikai bűnözésre figyelmeztető** nemzeti **platformokat**, az Europol pedig arra, hogy hozzon létre hasonló európai szintű platformot az interneten elkövetett bűncselekményekkel kapcsolatos adatok összegyűjtése, elemzése és kicserélése céljából.⁵⁸ A polgárok bejelenthetik a nemzeti platformjuknak, ha jogellenes tartalomra vagy viselkedésre bukkannak az interneten. A számítástechnikai bűnözés elleni küzdelem Europol által kezelt európai platformja adatgyűjtő központként járna le, elemezné és kicserélné a nemzeti bűnüldöző hatóságoknak az Europol megbízatása körébe tartozó számítástechnikai bűnözéssel kapcsolatos információit.⁵⁹ Mostanáig majdnem az összes tagállam létrehozta a számítástechnikai bűnözésre figyelmeztető nemzeti platformját. Az Europol az európai platform technikai végrehajtásán dolgozik, és előfordulhat, hogy a SIENA alkalmazását veszi majd igénybe a nemzeti platformok közötti adatmegosztás fokozása érdekében. Amennyiben ez az információ-megosztás személyes adatok Europol általi feldolgozását érinti, az Europol-határozatba (2009/371/IB tanácsi határozat) foglalt különös adatvédelmi szabályokat, valamint a 45/2001/EK rendeletet, az Európa Tanács 108. egyezményét, annak 181. kiegészítő jegyzőkönyvét és a rendőrségi ajánlást kell alkalmazni.⁶⁰ A személyes adatoknak a tagállamok és az Europol közötti cseréjét a 2008/977/IB tanácsi kerethatározat rendelkezései szabályozzák.⁶¹ Mivel nem született jogi aktus, a számítástechnikai bűnözésre figyelmeztető platformok esetében nincs hivatalos felülvizsgálati mechanizmus. Az Europol tevékenysége azonban már jelenleg is lefedi ezt a fontos területet, a jövőben pedig be fog számolni a platformok tevékenységéről a jóváhagyás céljából a Tanács, és tájékoztatás céljából az Európai Parlament elé terjesztett éves jelentéseiben.

⁵⁸ A Tanács következtetései az internetes bűncselekmények bejelentésére szolgáló nemzeti figyelmeztető platformok és az európai figyelmeztető platform létrehozásáról, Bel- és Igazságügyi Tanács, 2008.10.24.; A Tanács következtetései a bűnözés elleni küzdelem összehangolt stratégiájának végrehajtásáról szóló cselekvési tervről, Általános Ügyek Tanácsa, 2010.4.26. Az Europol átkeresztelte projektjét „a számítástechnikai bűnözés elleni küzdelem európai platformja” névre.

⁵⁹ Az Europol célja a szervezett bűnözés, a terrorizmus és a két vagy több tagállamot érintő súlyos bűncselekmények egyéb formáinak megelőzése és az ellenük folytatott küzdelem. Lásd a 2009/371/IB tanácsi kerethatározatot, HL L 121., 2009.5.15., 37. o.

⁶⁰ A Tanács 2009/371/IB határozata, HL L 121., 2009.5.15., 37. o.; 45/2001/EK rendelet, HL L 8., 2001.1.12., 1. o.; Egyezmény az egyének védelméről a személyes adatok gépi feldolgozása során (ETS 108. sz.), Európa Tanács 1981.1.28. (az Európa Tanács 108. egyezménye); A személyes adatok gépi feldolgozása során az egyének védelméről szóló egyezménynek a felügyelő hatóságokról és a személyes adatok országhatárokat átlépő áramlásáról szóló kiegészítő jegyzőkönyve (181. sz. ETS), Európa Tanács, 2001.11.8. (181. kiegészítő jegyzőkönyv); A Miniszterek Tanácsa R (87) 15. sz. ajánlása a személyes adatok rendőri ágazatban való felhasználásának szabályozásáról, Európa Tanács, 1987.9.17. (rendőrségi ajánlás).

⁶¹ A Tanács 2008/977/IB kerethatározata, HL L 350., 2008.12.30., 60. o.;

A határokon átnyúló súlyos bűnözés megelőzésében és az ellene folytatott küzdelemben a tagállamok támogatásával megbízott uniós ügynökségek és testületek

Az 1995-ben létrehozott **Európai Rendőrségi Hivatal** (Europol) 1999-ben kezdte meg működését, és 2010 januárjában vált uniós ügynökséggé⁶². Célja a szervezett bűnözés, a terrorizmus és a két vagy több tagállamot érintő súlyos bűncselekmények egyéb formáinak megelőzése és az ellenük folytatott küzdelem terén a tagállamok támogatása. Fő feladatai közé tartozik az információk és bűnüldözési operatív információk összegyűjtése, tárolása, feldolgozása, elemzése és cseréje; a nyomozások segítése; valamint bűnüldözési operatív információk és elemzési támogatás nyújtása a tagállamoknak. Az Europol és a tagállamok közötti legfontosabb kapcsolattartó szervek az Europol nemzeti egységek (a továbbiakban: ENU-k), amelyek összekötő tisztviselőket küldenek ki az Europolhoz. Az ENU-k vezetői rendszeresen találkoznak, hogy operatív ügyekben támogatást nyújtsanak az Europolnak, az ügynökség működését pedig annak igazgatótanácsa és az igazgatója felügyeli. Az alábbiak tartoznak Europol információkezelési eszközei közé: az Europol Információs Rendszer (a továbbiakban: EIS), az elemzési célú munkafájlok (a továbbiakban: AWF), valamint a SIENA alkalmazás. Az EIS személyes adatokat tartalmaz, többek között az alábbiakat: biometrikus azonosítók, az Europol megbízatásának hatálya alá tartozó bűncselekményekkel gyanúsított személyek büntető ítéletei és a szervezett bűnözéshez fűződő kapcsolataik. A hozzáférés az ENU-kra, az összekötő tisztviselőkre, az Europol felhatalmazott személyzetére és az igazgatóra korlátozódik. A bűnügyi nyomozások segítése céljából megnyitott AWF-k személyekre vonatkozó adatokat tartalmaznak, továbbá bármely egyéb információt, amelyek felvételéről az ENU-k dönthetnek. Az összekötő tisztviselők számára biztosítják a hozzáférést, de csak az Europol elemzői vihetnek be adatokat ezekbe a fájlokba. Tárgymutatórendszer teszi lehetővé az ENU-k és az összekötő tisztviselők számára annak ellenőrzését, hogy az adott AWF tartalmaz-e a tagállamuk érdeklődésére számot tartó információkat. A tagállamok egyre növekvő mértékben veszik igénybe az Europol SIENA alkalmazását érzékeny adatok bűnüldözési célú megosztására. Az Europol feladatai ellátása során feldolgozhat információkat és bűnüldözési operatív információkat, köztük személyes adatokat is; a tagállamok pedig az Europol adatfájljaiból lekérdezett információkat csak a határokon átnyúló jellegű bűnözés megelőzése az ellen folytatott küzdelem céljából használhatják. Az információk felhasználásával kapcsolatban az adatokat szolgáltató tagállam által megszabott bármely korlátozást szintén alkalmazni kell az Europol adatfájljaiból ilyen adatokat lekérdező egyéb felhasználókkal szemben. Az Europol azokkal a harmadik országokkal is cserélhet személyes információkat, amelyek operatív megállapodást kötöttek az Europollal, továbbá megfelelő szintű adatvédelmet garantálnak. Az ügynökség a feladatainak ellátásához szükséges ideig őrizheti meg az adatokat. Az AWF-k legfeljebb három évig tárolhatók, és további hároméves meghosszabbítás lehetséges. A személyes adatok Europol általi feldolgozásának meg kell felelnie a saját működését szabályozó jogi aktusban (2009/371/IB tanácsi határozat) foglalt különös adatvédelmi szabályoknak, valamint a 45/2001/EK rendeletnek, az Európa Tanács 108. egyezményének, annak 181. kiegészítő jegyzőkönyvének és a rendőrségi ajánlásnak.⁶³ A személyes adatoknak a tagállamok és az

⁶² A Tanács 2009/371/IB határozata, HL L 121., 2009.5.15., 37. o., amely az Európai Unióról szóló szerződés K.3. cikke alapján az Európai Rendőrségi Hivatal létrehozásáról szóló egyezmény, HL C 316., 1995.11.27. 2. o., helyébe lépett.

⁶³ A Tanács 2009/371/IB határozata, HL L 121., 2009.5.15., 37. o.; 45/2001/EK rendelet, HL L 8., 2001.1.12., 1. o.; Egyezmény az egyének védelméről a személyes adatok gépi feldolgozása során (ETS 108. sz.), Európa Tanács 1981.1.28. (az Európa Tanács 108. egyezménye); A személyes adatok gépi feldolgozása során az egyének védelméről szóló egyezménynek a felügyelő hatóságokról és a személyes adatok országhatárokat átlépő áramlásáról szóló kiegészítő jegyzőkönyve (181. sz. ETS),

Europol közötti cseréjére a 2008/977/IB tanácsi kerethatározat rendelkezései alkalmazandók.⁶⁴ A nemzeti felügyeleti testületek tagjaiból álló közös ellenőrző szerv ellenőrzi a személyes adatok Europol általi feldolgozását, valamint a személyes adatok Europol általi átadását egyéb felek részére. A testület rendszeresen jelentést terjeszt az Európai Parlament és a Tanács elé. Az Europol a tevékenységéről szóló éves jelentést nyújt be jóváhagyás céljából a Tanács, és tájékoztatás céljából az Európai Parlament elé.

A 2001. szeptember 11-i terrortámadás az **Európai Unió Igazságügyi Együttműködési Egységének** (Eurojust) 2002. évi létrehozatalát is felgyorsította amellelt, hogy több eszközre is hatást gyakorolt a fentiekben ismertetett módon.⁶⁵ Az Eurojust uniós szerv, amelynek célja a tagállamokban a nyomozások és a büntetőeljárások összehangolásának javítása, valamint az illetékes nemzeti hatóságok közötti együttműködés fokozása. Tevékenysége ugyanarra a fajta bűnözésre és ugyanazokra a bűncselekményekre terjed ki, mint az Europolé. Az Eurojust testületét alkotó 27 nemzeti tag e megbízatás keretei között és feladatuk ellátása során hozzáfér a gyanúsítottak és az elkövetők személyes adataihoz. Többek között az alábbiak tartoznak ezen adatok közé: születési adatok, elérhetőségek, gépjármű-nyilvántartási adatok, DNS-profilok, fényképek, ujjlenyomatok, valamint a távközlési szolgáltatók által megadott forgalmi, helymeghatározó és előfizetői adatok. A tagállamoknak meg kell osztaniuk ezeket az információkat az Eurojusttal, hogy a szervezet képes legyen ellátni a feladatait. Az ügyekhez kapcsolódó valamennyi személyes adatot be kell vinni az Eurojust automatizált ügyviteli rendszerébe, amely a Bizottság s-TESTA hálózatán üzemel. A folyamatban lévő vizsgálatokkal kapcsolatos személyes és nem személyes adatokat tárgymutató rendszerben őrzik meg. Az Eurojust feladatai ellátása céljából feldolgozhat személyes adatokat, azonban az ilyen műveleteknek meg kell felelniük az Eurojust saját szabályozó jogi aktusába (2009/426/IB tanácsi határozat) foglalt különös szabályoknak, valamint az Európa Tanács 108. egyezményének, annak 181. kiegészítő jegyzőkönyvének, és a rendőrségi ajánlásnak. A személyes adatoknak a tagállamok és az Europol közötti cseréjére a 2008/977/IB tanácsi kerethatározat rendelkezései alkalmazandók.⁶⁶ Az Eurojust adatokat cserélhet a nemzeti hatóságokkal, és azon harmadik országokkal, amelyekkel megállapodást kötött, feltéve hogy az adatokat közlő nemzeti tag hozzájárult az ilyen átadáshoz, továbbá a harmadik ország megfelelő szintű adatvédelmet garantál. A személyes adatok az Eurojust céljainak eléréséhez szükséges ideig őrizhetők meg, az adott ügy lezárása után viszont törölni kell azokat. A tagállamoknak 2011. júniusig kell végrehajtaniuk az Eurojust módosított jogalapját. 2014 júniusáig a Bizottságnak felülvizsgálatot kell végeznie, és amennyiben szükségesnek látszik, javaslatot tehet az Eurojust nemzeti tagjai közötti információcserével kapcsolatos változtatásokra. 2013 júniusáig az Eurojustnak jelentést kell tennie a Tanácsnak és a Bizottságnak az ügyviteli rendszeréhez való nemzeti szintű hozzáférés biztosításából leszűrt tapasztalatokról. A tagállamok ennek alapján felülvizsgálhatják a nemzeti hozzáférési jogosultságokat. A tagállamok által kinevezett bíróból álló közös ellenőrző szerv ellenőrzi a személyes adatok Eurojust általi feldolgozását, és évente jelentést tesz a Tanácsnak. A testület elnöke az Eurojust tevékenységéről szóló éves jelentést nyújt be a Tanácsnak, amelyet az továbbít az Európai Parlament számára.

Európa Tanács, 2001.11.8. (181. kiegészítő jegyzőkönyv); A Miniszterek Tanácsa R (87) 15. sz. ajánlása a személyes adatok rendőri ágazatban való felhasználásának szabályozásáról, Európa Tanács, 1987.9.17. (rendőrségi ajánlás).

⁶⁴ A Tanács 2008/977/IB kerethatározata, HL L 350., 2008.12.30., 60. o.;

⁶⁵ A 2009/426/IB tanácsi határozattal, HL L 138., 2009.6.4., 14. o. módosított 2002/187/IB tanácsi határozat, HL L 63., 2002.3.6., 1. o. Lásd még: Rendkívüli Bel- és Igazságügyi Tanács, 2001.9.20.

⁶⁶ A Tanács 2008/977/IB kerethatározata, HL L 350., 2008.12.30., 60. o.

A terrorizmus és a súlyos transznacionális bűnözés egyéb formáinak megelőzésére és leküzdésére irányuló nemzetközi megállapodások

A 2001. szeptember 11-i terrortámadás következtében az Egyesült Államok olyan jogszabályt fogadott el, amely előírja a területéről induló vagy oda érkező járatokat üzemeltető légi fuvarozók számára, hogy biztosítsanak hozzáférést az automatizált foglalási rendszerekben tárolt **utas-nyilvántartási adatállományokhoz** (PNR). Hamarosan Kanada és Ausztrália is követte az Egyesült Államok példáját. Mivel a vonatkozó uniós jogszabályok megkövetelik a harmadik ország által biztosított adatvédelmi szint előzetes ellenőrzését, a Bizottság elvállalta ezt a feladatot, és PNR-megállapodásokról folytatott tárgyalásokat az említett országokkal.⁶⁷ A Bizottság az Egyesült Államokkal 2007. júliusban, Ausztráliával 2008. júniusban írt alá ilyen megállapodást, továbbá Kanadával 2005. októberben API/PNR megállapodást írt alá.⁶⁸ Az Egyesült Államokkal és Ausztráliával kötött megállapodások átmenetileg alkalmazandók, a Kanadával megkötött megállapodás pedig – a kanadai adatvédelmi normák megfelelőségére vonatkozó bizottsági határozatából kifolyólag – annak ellenére is hatályban marad, hogy 2009. szeptemberében lejárt.⁶⁹ Az Európai Parlament bírálta a három megállapodás tartalmát, és felszólította a Bizottságot, hogy világos elvek alapján tárgyalja újra azokat.⁷⁰ A jóval az adott járat indulása előtt elküldött PNR-adatok elősegítik, hogy a bűnüldöző hatóságok kiszűrjék azokat az utasokat, akik összefüggésbe hozhatók terrorizmussal vagy a súlyos bűnözés más formáival. Ennek megfelelően mindegyik megállapodás célja a terrorizmus és a súlyos bűnözés egyéb transznacionális formáinak megelőzése, és az azok elleni küzdelem. Az Unióból származó PNR-adatokért cserébe az Egyesült Államok Belbiztonsági Minisztériuma (a továbbiakban: DHS) megosztja az uniós bűnüldöző hatóságokkal, az Európával és az Eurojusttal a PNR-adatok elemzéséből származó nyomozati információkat; továbbá Kanada és az Egyesült Államok a megállapodásokban egyaránt ígéretet tett arra, hogy együttműködnek az Unióval saját PNR-rendszerének felállításában. Az Egyesült Államokkal és Ausztráliával kötött megállapodások 19 adatkategóriára, köztük születési, foglalási, fizetési és kiegészítő információkra terjednek ki; a Kanadával kötött megállapodás pedig 25 hasonló adatelemet tartalmaz. Többek között az alábbiak tartoznak a kiegészítő információk közé: az egy útra szóló repülőjegyekre, valamint a készenléti és a „no-show” (jegykezelésre nem jelentkező utas) állapotra vonatkozó adatok. Az Egyesült Államokkal kötött megállapodás bizonyos feltételekkel lehetővé teszi továbbá az érzékeny adatok felhasználását. A DHS akkor használhatja fel az ilyen információkat, ha az érintett vagy mások élete veszélyben forog, azonban 30 napon belül törölnie kell azokat. Számos központi egységnek megküldik a PNR-adatokat a DHS-en, a Kanadai Határügynökségen és az Ausztrál Vámhatóságon belül. Az említett egységek továbbíthatják az adatokat a bűnüldözésért vagy terrorelhárításért felelős, más belföldi hatóságoknak. Az Egyesült Államokkal kötött megállapodás szerint a DHS azt várja, el, hogy az Unióból származó PNR-adatok feldolgozására vonatkozó adatvédelem szintje „ne legyen szigorúbb” annál, mint amelyet az uniós hatóságok saját belföldi PNR-

⁶⁷ 95/46/EK irányelv (adatvédelmi irányelv), HL L 281., 1995.23.11., 31. o.

⁶⁸ A kanadai csomag az alábbiakból áll: Kanada API/PNR adatok kezelésére vonatkozó kötelezettségvállalása, a Bizottságnak a kanadai adatvédelmi normákra vonatkozó megfelelőségi határozata, valamint egy nemzetközi megállapodás (lásd: HL L 91., 2006.3.29., 49. o.; HL L 82., 2006.3.21., 14. o.) Az Egyesült Államokkal kötött megállapodás a Hivatalos Lap alábbi számában található meg: HL L 204., 2007.8.4., 16. o.; Az Ausztráliával kötött megállapodás pedig a következőben: HL L 213., 2008.8.8., 47. o.

⁶⁹ 2009-ben Kanada kötelezettséget vállalt a Bizottság, a Tanács elnöksége és az uniós tagállamok felé, hogy továbbra is alkalmazni fogja a korábbi 2005-ös kötelezettségvállalását az uniós PNR-adatok felhasználására vonatkozóan. A Bizottság e korábbi kötelezettségvállalás alapján hozta meg a megfelelőségi döntését.

⁷⁰ Az Európai Parlament állásfoglalása, P7_TA(2010)0144., 2010.5.5.

rendszerükben alkalmazzák. Ha nem teljesül ez az elvárás, az amerikai minisztérium a megállapodás egyes részeit felfüggesztheti. Az Unió úgy ítéli meg, hogy amennyiben teljesítik a velük megkötött megállapodások feltételeit, Kanada és Ausztrália „megfelelő” szintű adatvédelmet biztosít az Unióból származó PNR-adatoknak. Az Egyesült Államokban hét évig őrzik meg az aktív, és további nyolc évig a háttéradatbázisban az Unióból származó PNR-adatokat. Ausztráliában 3,5 évre viszik be azokat az aktív, majd két évre a háttéradatbázisba. A háttéradatbázis minkét ország esetében csak különleges engedéllyel hozzáférhető. Kanadában 3,5 évig őrzik meg az adatokat, amelyeket 72 óra elteltével névtelenné tesznek. Mindegyik megállapodás rendszeres felülvizsgálatot ír elő, a Kanadával és Ausztráliával kötött megállapodások pedig felmondási záradékot is tartalmaznak. Az Unióban egyedül az Egyesült Királyság rendelkezik PNR-rendszerrel. Franciaország, Dánia, Belgium, Svédország és Hollandia már törvénybe iktatta a vonatkozó jogszabályokat, vagy jelenleg teszteli a PNR-adatok felhasználását a PNR-rendszerek felállítása céljából. Több másik tagállam is fontolgatja ilyen rendszerek létrehozását, és esetenként az összes tagállam használ PNR-adatokat bűnüldözési célokra.

2011. szeptember 11-ét követően az Egyesült Államok Pénzügyminisztériuma kidolgozta a **terrorizmus finanszírozásának felderítését célzó programot** (a továbbiakban: TFTP), amely a terroristák és pénzügyi támogatóik azonosítására, nyomon követésére és üldözésére szolgál. A TFTP alapján az Egyesült Államok Pénzügyminisztériuma adminisztratív adatbekérésekkel arra kötelezte egy belga vállalat egyesült államokbeli leányvállalatát, hogy korlátozott körben adja át a Pénzügyminisztériumnak a hálózatán továbbított pénzügyi üzenetadatokat. 2010 januárjában a szóban forgó vállalat megváltoztatta rendszerarchitektúráját, és így több mint a felével csökkentette az Egyesült Államok joghatósága alá tartozó olyan adatok mennyiségét, amelyek általában a pénzügyminisztériumi adatbekérések tárgyát képezik. 2009 novemberében az Európai Unió Tanácsának elnöksége és az Egyesült Államok kormánya ideiglenes megállapodást írt alá a pénzügyi üzenetadatoknak TFTP célokból az Unióból az Egyesült Államokba történő továbbításáról és ottani feldolgozásáról. Az Európai Parlament nem hagyta jóvá a megállapodást.⁷¹ Új megbízatása alapján az Európai Bizottság tárgyalásokat folytatott az Egyesült Államokkal egy új megállapodás-tervezetről, és 2010. június 18-án a Tanács elé terjesztette az Európai Unió és az Amerikai Egyesült Államok között az Európai Unióból származó pénzügyi üzenetadatoknak a terrorizmus finanszírozásának felderítését célzó program céljából történő feldolgozásáról és az Amerikai Egyesült Államok részére való átadásáról szóló megállapodás megkötéséről szóló tanácsi határozati javaslatot (EU-USA TFTP-megállapodás).⁷² Az Európai Parlament 2010. július 8-án megadta az egyetértését e megállapodás megkötéséhez.⁷³ A Tanács most várhatóan elfogadja az e megállapodás megkötéséről szóló tanácsi határozatot, ezt követően pedig a megállapodás a két fél közötti levélváltás útján lép hatályba. Az EU-USA TFTP-megállapodás célja a terrorizmus és az azt finanszírozó tevékenység megelőzése, felderítése, kivizsgálása vagy üldözése. Arra kötelezi a pénzügyi üzenetadatok kijelölt szolgáltatóit, hogy a konkrét földrajzi fenyegetés értékelésén alapuló pontos kérésekre adjanak át az Egyesült Államok Pénzügyminisztériumának számos pénzügyi üzenetadatot, amelyek többek között az alábbi adatokra terjednek ki: név, bankszámlaszám, valamint a pénzügyi tranzakciók megbízójának és jogosultjának(ainak) címe és azonosító száma. A Pénzügyminisztérium csak a TFTP céljából és kizárólag abban az esetben kereshet ezekben az adatokban, ha alapos oka van azt hinni, hogy egy meghatározott személy összefüggésbe

⁷¹ Az Európai Parlament állásfoglalása, P7_TA(2010)0029, 2010.2.11.

⁷² COM(2010) 316, 2010.6.15.

⁷³ Az Európai Parlament állásfoglalása, P7_TA-PROV(2010)0279, 2010.7.8.

hozható a terrorizmussal vagy annak finanszírozásával. Tilos az adatbányászat, valamint az egységes eurofizetési térségen belüli ügyletekre vonatkozó adatok átadása. Az Egyesült Államok megad az uniós tagállamoknak, az Europolnak és az Eurojustnak az Unión belüli potenciális terrorista szervezkedésekre vonatkozó valamennyi nyomozati adatot, továbbá segítséget nyújt az Uniónak a TFTP-vel egyenértékű saját rendszerének kiépítéséhez. Amennyiben az Unió ilyen programot hoz létre, a két fél kiigazíthatja az említett megállapodás feltételeit. Az adatátadást megelőzően az Europolnak át kell vizsgálnia minden amerikai kérést, hogy meggyőződjön arról, hogy az megfelel a megállapodás feltételeinek. A pénzügyi üzenetekből lehívott információk nem őrizhetők meg tovább, mint ami a konkrét nyomozás vagy büntetőeljárás lefolytatásához szükséges. A le nem hívott adatok legfeljebb 5 évig őrizhetők meg. Ha a terrorizmus, illetve az azt finanszírozó tevékenység felderítése, megelőzése vagy üldözése céljából szükséges, a Pénzügyminisztérium a pénzügyi üzenetekből lehívott személyes adatokat átadhatja az Egyesült Államok bűnüldöző, közbiztonsági vagy terror-elhárítási hatóságainak, az uniós tagállamoknak, az Europolnak vagy az Eurojustnak. Továbbá harmadik országokkal is megoszthatja az uniós állampolgárokkal és lakosokkal kapcsolatos nyomozati információkat, amennyiben az érintett tagállam ehhez hozzájárul. Független felügyelők – köztük egy Bizottság által kinevezett személy – ellenőrzi, hogy a felek megfelelnek-e a megállapodás szigorú terrorelhárítási célhoz kötöttségének és az egyéb biztosítékoknak. A megállapodás öt éves időtartamra szól, és bármelyik fél felmondhatja vagy felfüggesztheti. A Bizottság által vezetett, és két adatvédelmi hatóság képviselőiből, valamint egy bíróból álló uniós felülvizsgálati csoport hat hónappal a hatályba lépését követően felülvizsgálja az említett megállapodást, kiváltképpen azt vizsgálva, hogy a felek végrehajtják-e a cél korlátozására és az arányosságra vonatkozó rendelkezéseket, továbbá hogy eleget tesznek-e az adatvédelmi kötelezettségeiknek. A Bizottság jelentését benyújtják majd az Európai Parlamentnek és a Tanácsnak.

2.2. A stockholmi program végrehajtásáról szóló cselekvési terv keretébe illeszkedő kezdeményezések

A Bizottság által előterjesztendő jogalkotási javaslatok

A stockholmi programban az Európai Tanács felszólította a Bizottságot, hogy az alábbiakra vonatkozóan terjessze elő három, e közleményhez közvetlenül kapcsolódó javaslatot: a terrorizmus és a súlyos bűnözés megelőzésére, felderítésére és üldözésére szolgáló uniós PNR-rendszer; határregisztrációs rendszer; valamint regisztráltutas-program. Az utóbbi kettővel kapcsolatosan az Európai Tanács hangsúlyozta, hogy azokat „mihamarabb” elő kell terjeszteni. A Bizottság mind a három kérést belefoglalta a stockholmi program végrehajtásáról szóló cselekvési tervébe.⁷⁴ Most az a célja, hogy eleget tegyen az említett kéréseknek, valamint hogy a jövőben a 4. szakaszban megállapított politikafejlesztési elvek alapján értékelje ezeket a jogi aktusokat.

2007 novemberében a Bizottság a PNR-adatok bűnüldözési célú felhasználásáról szóló tanácsi kerethatározati javaslatot terjesztett elő.⁷⁵ Ez a javaslat támogatást kapott a Tanácsban, majd ezt követően az Európai Parlament által javasolt módosítások és az európai adatvédelmi biztos állásfoglalásának a figyelembe vételével módosították. A javaslat a Lisszaboni Szerződés hatálybalépése miatt elévült. Amint a stockholmi program végrehajtásáról szóló

⁷⁴ A stockholmi program – A polgárokat szolgáló és védő, nyitott és biztonságos Európa, 5731/10. sz. tanácsi dokumentum, 2010.3.3., COM(2010)171., 2010.4.20. (A stockholmi program végrehajtásáról szóló cselekvési terv).

⁷⁵ COM(2007) 654, 2007.11.6.

cselekvési tervben jeleztük, a Bizottság jelenleg azon dolgozik, hogy 2011 elején az alábbi dokumentumokból álló **utas-nyilvántartási adatállomány csomagot** terjesszen elő: az EU külső PNR stratégiájáról szóló közlemény, amely körvonalazza a harmadik országokkal megtárgyalandó megállapodásokra irányadó alapelveket; az Egyesült Államokkal és Ausztráliával megkötött PNR-megállapodások újratárgyalására vonatkozó tárgyalási irányelvek; valamint a Kanadával megkötendő új megállapodás tárgyalási irányelvei. A Bizottság előkészíti továbbá az új uniós PNR-ra vonatkozó javaslatot.

2008-ban a Bizottság több javaslatot tett közzé az EU integrált határigazgatásának fejlesztésére a harmadik országbeli állampolgárok utazásának megkönnyítése révén, és egyszersmind a belső biztonságot is erősítve.⁷⁶ Felhívta rá a figyelmet, hogy az „engedélyezett tartózkodási idejüket túllépő személyek” közül kerül ki az Unión belüli illegális migránsok legnagyobb csoportja, és javaslatot tett a legfeljebb három hónapos rövid távú tartózkodás céljából az EU területére beutazó harmadik országbeli állampolgárokra vonatkozó **határregisztrációs rendszer** (EES) esetleges bevezetésére. E rendszer nyilvántartaná a belépés időpontját és helyét, valamint az engedélyezett tartózkodás hosszát, továbbá automatizált figyelmeztető jelzéseket továbbítana az illetékes hatóságoknak, amelyek „engedélyezett tartózkodási idejüket túllépőként” határoznák meg az érintett személyeket. A biometrikus adatok ellenőrzésére épülő rendszer a SIS II-vel és a VIS-el azonos biometrikus adatok egyeztetésére szolgáló rendszert és operatív berendezéseket venne igénybe. A Bizottság jelenleg hatásvizsgálatot végez, és a stockholmi program végrehajtásáról szóló cselekvési tervben közölteknek megfelelően arra törekszik, hogy 2011-ben jogalkotási javaslatot nyújtson be.

A harmadik mérlegelendő javaslat a **regisztráltutas-programra** (a továbbiakban: RTP) irányult.⁷⁷ Ez a program lehetővé tenné a harmadik országok állampolgárainak egyes gyakran utazó csoportjai számára, hogy – megfelelő előzetes átvilágítást követően – automatizált kapukon keresztül egyszerűsített határellenőrzés alkalmazásával lépjenek az Unió területére. Az RTP a személyazonosság biometrikus adatok alkalmazásával történő ellenőrzésére is épülne, továbbá lehetőséget teremtene arra, hogy a jelenlegi általános határellenőrzéstől elmozduljunk az egyéni kockázaton alapuló megközelítés irányába. A Bizottság jelenleg hatásvizsgálatot végzett, és a stockholmi program végrehajtásáról szóló cselekvési tervnek megfelelően 2011-ben várhatóan jogalkotási javaslatot terjeszt elő.

A Bizottság által tanulmányozandó kezdeményezések

A stockholmi programban az Európai Tanács felszólította a Bizottságot, hogy az e közleményhez kapcsolódó három kezdeményezéssel összefüggésben tanulmányozza az alábbiakat: a terrorizmus finanszírozásának Unión belüli felderítését célzó lehetőségek; egy európai utazásengedélyezési rendszer kialakításának lehetősége és hasznossága; valamint az Európai Rendőrségi Nyilvántartási Indexrendszer létrehozásának szükségessége és hozzáadott értéke. A Bizottság e kezdeményezéseket is belefoglalta stockholmi program végrehajtásáról szóló cselekvési tervébe. Most fogjuk megvizsgálni azok megvalósíthatóságát, és eldönteni, hogy a 4. szakaszban kiemelt politikafejlesztési elvek alapján miként dolgozhatók ki.

Az EU-USA TFTP-megállapodás felszólítja az Európai Bizottságot, hogy készítsen tanulmányt egy, az adatok EU-ból az USA-ba történő célzottabb továbbítását lehetővé tévő, az egyesült államokbeli TFTP-rendszerhez hasonló **uniós rendszer** esetleges bevezetéséről.

⁷⁶ COM(2008) 69, 2008.2.13.

⁷⁷ COM(2008) 69, 2008.2.13.

Az e megállapodás megkötéséről szóló tanácsi határozattervezet felkéri továbbá a Bizottságot, hogy a megállapodás hatályba lépésétől számított egy éven belül nyújtsa be az Európai Parlament és a Tanács részére az adatlehívás uniós területen történő jogi és műszaki keretét.⁷⁸ Az említett megállapodás hatályba lépését követő három éven belül a Bizottságnak előrehaladási jelentést kell előterjesztenie az egyenértékű uniós rendszer fejlesztéséről. Ha a megállapodás hatályba lépését követő öt éven belül az egyenértékű uniós rendszer nem jött létre, az Unió megfontolhatja a megállapodás felmondását. Az EU-USA TFTP-megállapodás arra kötelezi továbbá az Egyesült Államokat, hogy működjön együtt az Unióval, valamint nyújtson segítséget és tanácsot, amennyiben az Unió e rendszer felállítása mellett dönt. Függetlenül attól, hogy milyen végső döntés születik, a Bizottság megkezdte az említett feladat adatvédelmi, forrásoldali és gyakorlati vonzatainak tanulmányozását. Amint a stockholmi program végrehajtásáról szóló cselekvési tervben jeleztük, a Bizottság 2011-ben a terrorizmus finanszírozásának felderítését célzó uniós program (a továbbiakban: EU TFTP) létrehozatalának megvalósíthatóságáról szóló közleményt tesz közzé.

Az integrált határigazgatásról szóló 2008. évi közleményében a Bizottság javaslatot tett a harmadik országok vízumkötelezettség alá nem tartozó állampolgárai **elektronikus utazásengedélyezési rendszerének** (a továbbiakban: ESTA) lehetséges bevezetésére.⁷⁹ E program keretében a jogosult harmadik országbeli állampolgároknak az utazás megkezdése előtt elektronikus kérelmet kellene benyújtaniuk, születési, útlevél és utazási adataik megadásával. A vízumeljáráshoz képest az ESTA gyorsabb és egyszerűbb módszert kínálna annak ellenőrzésére, hogy az érintett személy megfelel-e a szükséges beutazási feltételeknek. A Bizottság jelenleg az ESTA bevezetésének előnyeit, hátrányait és gyakorlati következményeit tanulmányozza. Amint a stockholmi program végrehajtásáról szóló cselekvési tervben utaltunk rá, az a célunk, hogy 2011-ben közleményt terjesszünk elő e program létrehozatalának megvalósíthatóságáról.

2007. évi tanácsi elnöksége alatt Németország vitát indított az **Európai Rendőrségi Nyilvántartási Indexrendszer** (a továbbiakban: EPRIS) esetleges létrehozásáról.⁸⁰ Az EPRIS segítené a bűnüldözési tisztviselőket a (különösen a szervezett bűnözéssel gyanúsított személyek közötti kapcsolatokra vonatkozó) információk Unión belüli lokalizálásában. A Bizottság 2010-ben a Tanács elé fogja terjeszteni az EPRIS megvalósíthatósági tanulmányának elvégzésére vonatkozó megbízásának tervezetét. Amint a stockholmi program végrehajtásáról szóló cselekvési tervben említettük, a Bizottság arra törekszik, hogy 2012-ben közleményt terjesszen elő e rendszer felállításának megvalósíthatóságáról.

3. A MŰKÖDŐ, ÉS A VÉGREHAJTÁSI VAGY MÉRLEGELÉSI SZAKASZBAN ESZKÖZÖK ELEMZÉSE

A fenti áttekintés alapján az alábbi előzetes megállapítások tehetők:

Decentralizált struktúra

A jelenleg működő és a végrehajtási vagy mérlegelési szakaszban levő eszközök közül csupán hat jár személyes adatok uniós szintű gyűjtésével vagy tárolásával, nevezetesen a SIS (és a SIS II), a VIS, az EURODAC, az Europol és az Eurojust. Az összes többi eszköz a hatóságok

⁷⁸ 11222/1/10 REV 1. sz. tanácsi dokumentum, 2010.6.24., 11222/1/10 REV1 COR1. sz. tanácsi dokumentum, 2010.6.24.

⁷⁹ COM(2008) 69., 2008.2.13.

⁸⁰ Lásd a 15526/1/09. sz. tanácsi dokumentumot, 2009.12.2.

vagy magánvállalkozások által nemzeti szinten gyűjtött információk decentralizált, határokon átnyúló cseréjére vagy harmadik országokba történő továbbítására vonatkozik. A személyes adatok többségét nemzeti szinten gyűjtik és tárolják; az EU ezen adatok uniós partnerek és harmadik országok közötti cseréjének bizonyos feltételek melletti lehetővé tételével kíván hozzáadott értéket teremteni. A Bizottság nemrég benyújtotta az Európai Parlamentnek és a Tanácsnak a szabadságon, a biztonságon és a jog érvényesülésén alapuló térség nagyméretű IT-rendszereinek üzemeltetési igazgatását végző ügynökség létrehozásáról szóló módosított javaslatát⁸¹. A jövőbeli ügynökség a SIS II, a VIS és az EURODAC, valamint a szabadságon, a biztonságon és a jog érvényesülésén alapuló térségben működő esetleges egyéb jövőbeli IT-rendszerek üzemeltetési igazgatását látja majd el, biztosítva e rendszerek állandó működését, és ily módon az adatcsere folyamatos és megszakítatlan voltát.

Korlátozott cél

A fentebb elemzett eszközök nagy része egyetlen célt szolgál: az EURODAC a dublini rendszer működésének javítását; az API a határellenőrzés javítását; a svéd kezdeményezés a bűnügyi nyomozások és operatív műveletek elősegítését; a II. Nápolyi Egyezmény a vámcsalások megelőzésének, felderítésének, az ilyen ügyekben való vádemelésnek és a büntetésnek az elősegítését; a VIR a nemzeti vámigazgatási szervek közötti együttműködés hatékonyságának javítása útján a nemzeti jogszabályok megsértése súlyos eseteinek megelőzését, kivizsgálását és a büntetőeljárás lefolytatását; az ECRIS, a pénzügyi hírszerző egységek és a vagyon-visszaszerzési hivatalok a határokon átnyúló adatmegosztás egyszerűsítését egyes területek tekintetében; a prümi határozat, az adatmegőrzési irányelv, a TFTP és a PNR pedig a terrorizmus és a súlyos bűncselekmények elleni küzdelmet. Úgy tűnik, ez alól a SIS, a SIS II és a VIS jelenti a fő kivételt: a VIS eredeti célja az volt, hogy megkönnyítse a vízumadatok határokon átnyúló cseréjét, de ezt később kiterjesztették a terrorizmus és a súlyos bűncselekmények megelőzésére és az ellenük való küzdelemre is. A SIS és a SIS II célja – az e rendszer útján szolgáltatott információk felhasználásával – a szabadságon, a biztonságon és a jog érvényesülésén alapuló térségen belül egy magas biztonsági szint biztosítása, valamint a személyek mozgásának megkönnyítése. E centralizált információs rendszerek kivételével a célhoz kötöttség meghatározó tényezőnek tűnik az uniós szintű információkezelési intézkedések kialakítása szempontjából.

A funkciók közötti esetleges átfedések

Ugyanazon személyes adatokat több különböző eszköz révén gyűjthetik, de az adatokat egy adott eszköz keretében csak korlátozott célra használhatják fel (a VIS, a SIS és a SIS II kivételével). Egy magánszemély születési adatai, így neve, születési ideje és helye, valamint állampolgársága feldolgozható a SIS, a SIS II, a VIS, az API, a VIR, a svéd kezdeményezés, a prümi határozat, az ECRIS, a pénzügyi hírszerző egységek és a vagyon-visszaszerzési hivatalok, az Europol, az Eurojust, a PNR és a TFTP megállapodások keretében. Ezeket az adatokat azonban az API esetében csak a határellenőrzés céljából lehet feldolgozni; a VIR esetében a vámcsalások megelőzése, kivizsgálása és a vádemelés céljából; a svéd kezdeményezés esetében bűnügyi nyomozások és operatív műveletek céljából; a prümi határozat esetében a terrorizmus és határokon átnyúló bűnözés megelőzése érdekében; az ECRIS esetében valamely személy büntetett előéletének megvizsgálása céljából; a pénzügyi hírszerző egységek esetében valamely személynek a szervezett bűnözéssel és a terrorista hálózatokkal való kapcsolatai felderítése érdekében; a vagyon-visszaszerzési hivatalok

⁸¹ COM(2010) 93, 2010.3.19.

esetében a vagyon felkutatása céljából; az Europol és az Eurojust esetében a határokon átnyúló súlyos bűncselekmények nyomozása és a büntetőeljárás elősegítése céljából; a PNR esetében a terrorizmus és a nemzetközi bűnözés egyéb súlyos formáinak megelőzése és az ellenük való küzdelem céljából; a TFTP esetében pedig a terroristák és az őket finanszírozó személyek azonosítása és üldözése céljából. A biometrikus adatokat, így az ujjlenyomatokat és a fényképeket a SIS II, a VIS, az EURODAC, a svéd kezdeményezés, a prümi határozat, az ECRIS, az Europol és az Eurojust keretében lehet feldolgozni, szintén az adott intézkedés korlátozott céljára. A prümi határozat az egyetlen olyan eszköz, amely lehetővé teszi anonim DNS-profilok határokon átnyúló cseréjét (bár ilyen adatokat az Europolhoz és az Eurojusthoz is lehet továbbítani). Más intézkedések alapján személyi adatok pontosan meghatározott, az egyes intézkedések egyedi célkitűzései szempontjából releváns körének feldolgozására kerül sor: a PNR rendszerek az utasok repülőjegy-foglalásainak adatait dolgozzák fel; a FIDE a vámcsalások felderítése szempontjából releváns adatokat; az adatmegőrzési irányelv az IP-címeket és a mobilberendezési azonosítókat; az ECRIS a bűnügyi nyilvántartásokat; a vagyon-visszaszerzési hivatalok a magánvagyon és a vállalkozások adatait; a számítástechnikai bűnözés elleni platformok az internetes bűncselekményeket; az Europol a bűnözői hálózatokkal való kapcsolatokat; a TFTP pedig a pénzügyi üzenetadatokat. Az egyes funkciók közötti jelentős átfedés egyetlen esetét az információk és bűnüldözési operatív információk bűnügyi nyomozás céljából történő határokon átnyúló cseréje jelenti. Jogi szempontból a svéd kezdeményezés elegendő lenne az ilyen nyomozások szempontjából releváns bármilyen típusú információk cseréjéhez (feltéve, hogy az ilyen személyes adatok cseréje a nemzeti jog alapján megengedett). Operatív szempontból azonban a prümi határozat alkalmasabb lehet a DNS-profilok és ujjlenyomat-adatok megosztásához, mivel „találat/nincs találat” rendszere azonnali választ biztosít, automatizált adatmegosztási módszere pedig magas szintű adatbiztonságot garantál⁸². Hasonlóképpen, a pénzügyi hírszerző egységek, a vagyon-visszaszerzési hivatalok és a számítástechnikai bűnözés elleni platformok számára adott esetben hatékonyabb lehet a megfelelő uniós partnerszervezeteikkel való közvetlen kapcsolatfelvétel, a svéd kezdeményezés által az információkéréshez előírt formanyomtatványok kitöltése nélkül.

Ellenőrzött hozzáférési jogok

A terrorizmus és a súlyos bűncselekmények elleni küzdelem logikájával indokolt eszközök esetében a hozzáférési jogosultságok általában a szűkebb értelemben vett bűnüldöző szervekre korlátozódnak, vagyis a rendőrségre, a határellenőrzési szervekre és a vámhatóságokra. A „schengeni” logikával indokolt intézkedések esetében hozzáférési jogosultságot általában a bevándorlási hatóságoknak, és bizonyos feltételek mellett a rendőrségnek, a határellenőrzési szerveknek és a vámhatóságoknak biztosítanak. Az információáramlást a központosított SIS és VIS esetében nemzeti interfészek, a decentralizált eszközök, így a prümi határozat, a svéd kezdeményezés, a II. Nápolyi Egyezmény, az ECRIS, a TFTP, a PNR megállapodások, a pénzügyi hírszerző egységek, a vagyon-visszaszerzési hivatalok és a számítástechnikai bűnözés elleni platformok esetében pedig nemzeti kapcsolattartó pontok vagy központi koordináló egységek ellenőrzik.

⁸² A prümi határozathoz (2008/615/IB tanácsi határozat, HL L 210., 2008.8.6., 1. o.) megfelelő végrehajtási határozat kapcsolódik (2008/616/IB tanácsi határozat, HL L 210., 2008.8.6., 12. o.), amelynek célja a legkorszerűbb műszaki intézkedések biztosítása az adatvédelem és az adatbiztonság garantálása érdekében, valamint hitelesítési eljárás és titkosítás használata az adatokhoz való hozzáférés során, és a keresések elfogadhatóságára vonatkozó külön szabályokat is tartalmaz.

Változatos adatmegőrzési szabályok

Az adatmegőrzési időszakok az egyes eszközök céljától függően nagymértékben eltérően alakulnak. Az Egyesült Államokkal kötött PNR-megállapodás rendelkezik a leghosszabb – 15 éves – adatmegőrzési időszakról, míg a legrövidebb – 24 órás – időszakot az API írja elő. A PNR-megállapodások érdekes megkülönböztetést vezetnek be az aktív és a passzív használatban levő adatok között: bizonyos időszak elteltével az információkat archiválni kell, ezt követően azokhoz csak különleges engedéllyel lehet hozzáférni. Az uniós PNR-adatok Kanada általi használata jó példát nyújt erre: az információkat 72 óra elteltével anonimizálni kell, de az erre feljogosított tisztviselők még 3,5 évig hozzáférhetnek.

Hatékony személyazonosság-kezelés

A fentiekben elemzett intézkedések közül több – így a jövőbeli SIS II és a VIS is – lehetővé teszi a személyazonosság ellenőrzését biometrikus adatok felhasználásával. A SIS II végrehajtása várhatóan javítja majd a biztonságot a szabadságon, biztonságon és a jog érvényesülésén alapuló térségben, például azzal, hogy – a személyazonosító okmányok rendelkezésre állásától vagy eredetiségétől függetlenül – lehetővé teszi azon személyek azonosítását, akik ellen európai elfogatóparancsot adtak ki, továbbá akiknek a schengeni térségbe való belépését nem engedélyezték, és akiket egyéb különleges nyomozati okból keresnek (például eltűnt személyek vagy tanúk bírósági eljárásban). A VIS végrehajtása megkönnyíti majd a vízumkiadási és -kezelési eljárást.

Adatbiztonság uniós megoldásokon keresztül

Az érzékeny információk európai határokon átnyúló cseréje során a tagállamok az uniós megoldásokat részesítik előnyben. Számos különböző méretű, szerkezetű és célú eszköz támaszkodik a Bizottság által finanszírozott s-TESTA adatközlési hálózatra az érzékeny információk megosztásához, így a központosított rendszerek közül a SIS II, a VIS és az EURODAC, a decentralizált eszközök közül a prümi határozat, az ECRIS és a pénzügyi hírszerző egységek, valamint az Europol és az Eurojust. A VIR és a FIDE a közös kommunikációs hálózatot, a közös rendszerinterfészt, illetve a Bizottság által szolgáltatott biztonságos internet-hozzáférést használják. Ugyanakkor úgy tűnik, a biztonságos adatátvitelre támaszkodó újabb kezdeményezések előszeretettel választják az Europol SIENA információcsere-hálózati alkalmazását: jelenleg megbeszélések zajlanak arról, hogy a pénzügyi hírszerző egységek hálózata (FIU-net), a vagyon-visszaszerzési hivatalok és a számítástechnikai bűnözés elleni platformok ezen alkalmazás alapján működjenek.

Eltérő felülvizsgálati mechanizmusok

A fentiekben elemzett eszközök különböző felülvizsgálati mechanizmusokat tartalmaznak. Összetett információs rendszerek esetében, mint amilyen a SIS II, a VIS és az EURODAC, a Bizottságnak évente vagy kétfévente jelentést kell benyújtania az Európai Parlamentnek és a Tanácsnak a rendszer működéséről, illetve a végrehajtás helyzetéről. A decentralizált információcsere-eszközök tekintetében a Bizottságnak egyetlen értékelő jelentést kell benyújtania a többi intézményhez a végrehajtás után néhány évvel: az adatmegőrzési irányelvet, a svéd kezdeményezést és a vagyon-visszaszerzési hivatalokkal kapcsolatos intézkedéseket 2010-ben kell értékelnie; a prümi határozatot 2012-ben; és az ECRIS-t 2016-ban. A három PNR-megállapodás időszakonkénti és ad hoc felülvizsgálatról is rendelkezik, és kettő a hatályvesztésre vonatkozó rendelkezést is tartalmaz. Az Europol és az Eurojust éves jelentést nyújt be a Tanácsnak, amely azokat tájékoztatásul az Európai Parlamentnek is

megküldi. E megfontolások azt sugallják, hogy az információkezelés jelenlegi struktúrája az EU-ban nem alkalmas arra, hogy az összes eszközre kiterjedő, egységes értékelési mechanizmust fogadjunk el. E sokféleségre tekintettel alapvető jelentőséggel bír, hogy az információkezelés területén bármely eszköz jövőbeli módosítása figyelembe vegye a szabadságon, biztonságon és a jog érvényesülésén alapuló térségben a személyes adatok gyűjtését, tárolását vagy cseréjét szabályozó összes többi eszközre gyakorolt esetleges hatását.

4. A SZAKPOLITIKÁK KIDOLGOZÁSÁNAK ELVEI

A 2. szakaszban több olyan kezdeményezést mutattunk be, amelyet az Európai Bizottság a közelmúltban végrehajtott, benyújtott vagy vizsgált. Az új ötletek nagy száma, valamint a belső biztonság és a migrációkezelés területén a joganyag kiterjedtebbé válása szükségessé teszi olyan alapelvek meghatározását, amelyet az elkövetkező években a szakpolitikai javaslatok kezdeményezése és értékelése során mérceként szolgálhatnak. Ezek az elvek az EU alapszerződéseiben, az Európai Bíróság és az Emberi Jogok Európai Bírósága ítélkezési gyakorlatában, valamint az Európai Parlament, a Tanács és az Európai Bizottság közötti vonatkozó intézményközi megállapodásokban rögzített általános elveken alapulnak és azokat kívánják kiegészíteni. A Bizottság az elvek alábbi két csoportja alapján kíván új kezdeményezéseket kidolgozni és végrehajtani, valamint a jelenlegi eszközöket értékelni:

Tartalmi elvek

Az alapvető jogok, így különösen a magánélethez való jog és az adatvédelem biztosítása

Az Európai Unió Alapjogi Chartájában foglalt alapvető jogok, így különösen a magánélethez való jog és a személyes adatok védelme, elsődleges szempontot jelent majd a Bizottság számára a belső biztonság vagy a migrációkezelés területén a személyes adatok feldolgozásával járó új javaslatok kidolgozása során. A Charta 7. és 8. cikke rögzíti, hogy mindenkinek joga van ahhoz, hogy „magán- és családi életét [...] tiszteletben tartsák”, valamint „a rá vonatkozó személyes adatok védelméhez”⁸³. Az Európai Unió működéséről szóló szerződés (a továbbiakban: EUMSZ.) – amely a tagállamok, az uniós intézmények, ügynökségek és szervek tevékenységei tekintetében kötelező erővel bír – 16. cikkében megerősíti, hogy mindenkinek joga van „a rá vonatkozó személyes adatok védelméhez”⁸⁴. Az információs technológia használatára építő új eszközök kidolgozása során a Bizottság az ún. „beépített adatvédelem” megközelítését kívánja követni. Ez arra utal, hogy a személyes adatok védelmét beépítik a javasolt eszköz műszaki alapjaiba, az adatfeldolgozást a javasolt célhoz szükséges mértékre korlátozzák, és csak azoknak a személyeknek biztosítanak hozzáférést az adatokhoz, akiknek szükségük van arra⁸⁵.

Szükségesség

⁸³ Az Európai Unió Alapjogi Chartája, HL C 83., 2010.3.30., 389. o.

⁸⁴ Az Európai Unióról szóló szerződés és az Európai Unió működéséről szóló szerződés egységes szerkezetbe foglalt változata, HL C 83., 2010.3.30., 1. o.

⁸⁵ A „beépített adatvédelem” átfogó leírásához lásd az európai adatvédelmi biztos véleményét az adatvédelem és a magánélet védelmének ösztönzése révén az információs társadalomba vetett bizalom erősítéséről, európai adatvédelmi biztos, 2010.3.18.

A nemzetbiztonság, a közbiztonság vagy a bűncselekmények megelőzése érdekében szükség lehet arra, hogy egy hatóság beavatkozzon az egyének magánélet védelméhez való jogába⁸⁶. Az Európai Emberi Jogi Bíróság ítélkezési gyakorlatában három feltételt állapított meg, amelyek teljesülése esetén az ilyen korlátozások indokoltak lehetnek: ha korlátozás jogszerű, jogos célt követ és demokratikus társadalomban szükséges. A magánéletbe való beavatkozás akkor tekinthető szükségesnek, ha kényszerítő társadalmi igényt elégít ki, ha arányos az elérni kívánt céllal, és ha a nemzeti hatóságok által az igazolására felhozott indokok relevánsak és kielégítőek⁸⁷. Jövőbeli javaslataiban a Bizottság értékelni fogja a kezdeményezés várható hatását az egyének magánélethez való jogára és a személyes adatok védelmére, és meg fogja állapítani, hogy ez a hatás miért szükséges, továbbá hogy a javasolt megoldás miért arányos az Európai Unióban a belső biztonság fenntartására, a bűncselekmények megelőzésére vagy a migrációkezelésre irányuló jogos cél szempontjából. A személyes adatok védelmére vonatkozó szabályok betartását – nemzeti vagy uniós szinten – minden esetben független hatóság fogja ellenőrizni.

Szubszidiaritás

A Bizottság új javaslatait a szubszidiaritás és az arányosság elvei tekintetében külön indokolni fogja, az Európai Unióról szóló szerződéshez csatolt 2. jegyzőkönyv 5. cikkének megfelelően. Minden új jogalkotási javaslat külön feljegyzésben tartalmazni fogja azokat az adatokat, amelyek az Európai Unióról szóló szerződés 5. cikkében megállapított szubszidiaritás elvével való összhang megítéléséhez szükségesek. Ez a feljegyzés adatokat fog tartalmazni a tervezet előrelátható pénzügyi, gazdasági és társadalmi hatásairól, továbbá – irányelv esetében – a tagállamok által annak végrehajtására elfogadandó jogszabályokra vonatkozó hatásairól⁸⁸. Az annak megállapításához vezető okokat, hogy egy uniós cél az Unió szintjén jobban megvalósítható, minőségi mutatókkal kell alátámasztani. A jogalkotási javaslatok figyelembe fogják venni annak szükségességét, hogy az Unióra, a nemzeti kormányokra, a regionális hatóságokra, a gazdasági szereplőkre és a polgárookra háruló terheket a lehető legkisebbre csökkentsék, és hogy azok arányban álljanak az elérendő célkitűzésekkel. Új nemzetközi egyezmény megkötésére vonatkozó javaslat esetében a feljegyzés a javaslatnak az érintett harmadik országokkal való kapcsolatokra gyakorolt várható hatását fogja vizsgálni.

Megfelelő kockázatkezelés

A szabadságon, biztonságon és a jog érvényesülésén alapuló térségben az információcserére általában a biztonságot érintő fenyegetések elemzése, a bűnözés terén mutatkozó tendenciák azonosítása, vagy a kapcsolódó szakpolitikai területeken kockázatok értékelése céljából kerül sor⁸⁹. A kockázatok gyakran, bár nem szükségszerűen, olyan személyekhez kapcsolódnak, akiknek múltbeli magatartása vagy magatartásmintái a jövőre nézve további kockázat fennállására utalnak. A kockázatnak azonban bizonyítékokon, nem pedig feltételezéseken kell alapulnia. A szükségességre vonatkozó vizsgálatok és a célhoz kötöttség nélkülözhetetlen

⁸⁶ Lásd az emberi jogok és alapvető szabadságok védelméről szóló európai egyezmény 8. cikkét (Európai szerződések sorozat 5. szám), Európa Tanács, 1950.11.4.

⁸⁷ Lásd az Emberi Jogok Európai Bíróságának *Marper kontra Egyesült Királyság* ügyben hozott ítéletét, Strasbourg, 2008.12.4.

⁸⁸ A hatásvizsgálatok alapvető elveit az Európai Bizottság hatásvizsgálati iránymutatása tartalmazza (SEC(2009) 92, 2009.1.15.)

⁸⁹ A sikeres kockázatkezelés gyakorlati példái között szerepel többek között az egyik tagállamban súlyos bűncselekményt elkövetett és kiutasított személy megakadályozása abban, hogy más tagállamon keresztül visszatérjen a schengeni térségbe (SIS), vagy annak megakadályozása, hogy egy személy több tagállamban kérelmezzen menedékjogot (EURODAC).

mindenfajta információkezelési intézkedés esetében. E tekintetben releváns a kockázati profilok kezelése, amely nem keverendő össze a faji alapon történő vagy egyébként diszkriminatív profilok létrehozásával, ami nem összeegyeztethető az alapvető jogokkal. A kockázati profilok segíthetnek abban, hogy az erőforrásokat egyes személyekre koncentráljuk a biztonságot érintő fenyegetések azonosítása és a bűncselekmények áldozatainak védelme érdekében.

Eljárásorientált elvek⁹⁰

Költséghatékonyság

Az információs technológián alapuló közszolgáltatásoknak lehetővé kell tenniük jobb szolgáltatások nyújtását és az adófizetők számára nagyobb érték biztosítását. A jelenlegi gazdasági helyzetre tekintettel minden új javaslat esetében, különösen, ha az információs rendszerek létrehozására vagy frissítésére vonatkozik, a lehető legnagyobb mértékű költséghatékonyságra fogunk törekedni. E megközelítés keretében figyelembe vesszük a már létező megoldásokat az átfedések lehető legkisebbre csökkentése és a lehetséges szinergiahatások maximális kihasználása érdekében. A Bizottság értékelné fogja, megvalósítható-e a javaslat célkitűzése a meglévő eszközök jobb kihasználása révén. Emellett mérlegeli majd a fennálló információs rendszerek új funkciókkal való kiegészítését, mielőtt új rendszerek létrehozását javasolná.

Alulról felfelé építkező megközelítés a szakpolitikák kialakítása során

Az új kezdeményezések kidolgozása során a lehető legkorábbi szakaszban be kell vonni az érdekelteket, ideértve a végrehajtásért felelős nemzeti hatóságokat, a gazdasági szereplőket és a civil társadalmat. A végfelhasználók érdekeit figyelembe vevő szakpolitikák kialakításához horizontális gondolkodásmód és széleskörű konzultáció szükséges⁹¹. Ezért a Bizottság törekedni fog arra, hogy a tanácsi struktúrákon, irányítóbizottságokon és *ad hoc* szerveken keresztül állandó kapcsolatot alakítson ki a nemzeti tisztviselőkkel és gyakorlati szakemberekkel.

A felelősségek világos megosztása

A szabadságon, biztonságon és a jog érvényesülésén alapuló térségben az információgyűjtési és információcsere-projektek technikai műszaki összetettsége miatt különös figyelmet kell fordítani az irányítási struktúrák kezdeti kialakítására. A SIS II projekt tapasztalatai azt mutatják, hogy a világos és stabil átfogó célkitűzések, szerepek és felelősségek korai meghatározásának elmulasztása jelentős költségtúllépéshez és végrehajtási késedelmekhez vezethet. A prűmi határozat végrehajtását illetően szerzett tapasztalatok előzetes értékelése azonban arra enged következtetni, hogy a decentralizált irányítási struktúra sem old meg minden problémát, mivel itt nincs projektvezető, akihez a tagállamok tanácsért fordulhatnának a projekt végrehajtásának pénzügyi vagy műszaki aspektusaival kapcsolatban. A jövőbeli informatikai ügynökség esetleg tud majd műszaki tanácsokat adni a szabadságon, a biztonságon és a jog érvényesülésén alapuló térség informatikai rendszereit kezelőknek. Emellett fórumként szolgálhat az IT-rendszerek üzemeltetési igazgatása és fejlesztése terén az

⁹⁰ Ezek az elvek az uniós belső biztonság terén alkalmazandó információkezelési stratégiáról szóló tanácsi következtetéseken alapulnak, Bel- és Igazságügyi Tanács, 2009.11.30.

⁹¹ A nyilvános konzultációk általános elveit és minimumkövetelményeit a COM(2002) 704, 2002.12.11. dokumentum tartalmazza.

érdekeltek széleskörű bevonásához. A költségűllépésekkel és a módosítási kérésekből eredő késedelemmel szembeni esetleges biztosítékként a szabadságon, a biztonságon és a jog érvényesülésén alapuló térségben új információs rendszer – különösen, ha nagyméretű IT-rendszert is érint – mindaddig nem kerül kifejlesztésre, amíg az alapjául szolgáló, célkitűzését, alkalmazási körét, funkcióit és műszaki adatait tartalmazó jogi aktusokat véglegesen el nem fogadták.

Felülvizsgálat és a hatályvesztésre vonatkozó rendelkezések

A Bizottság az e közleményben tárgyalt összes eszközt értékelni fogja. Erre az információkezelés területén létező összes eszközre tekintettel kerül sor. Ez megbízható képet ad majd arról, hogy az egyes eszközök hogyan illeszkednek a belső biztonság és a migrációkezelés tágabb összefüggéseibe. A jövőbeli javaslatok szükség esetén éves jelentéstételi kötelezettséget, időszakos és *ad hoc* felülvizsgálatokat, valamint a hatályvesztésre vonatkozó rendelkezést is tartalmaznak majd. A már létező eszközöket csak akkor tartjuk fenn, ha továbbra is azt a jogos célt szolgálják, amelyre szánták őket. A II. melléklet tartalmazza az e közleményben tárgyalt eszközök felülvizsgálatának időpontját és a felülvizsgálati mechanizmust.

5. TOVÁBBI TEENDŐK

Ez a közlemény először foglalja össze világosan és átfogó jelleggel a bűnüldözési és migrációkezelési célból a személyes adatok gyűjtését, tárolását vagy határokon átnyúló cseréjét szabályozó, működő, illetve végrehajtási vagy mérlegelési szakaszban levő uniós szintű intézkedéseket.

A közlemény áttekintést nyújt a polgároknak arról, hogy ki, milyen célból, milyen adatokat gyűjt vagy tárol róluk, illetve milyen információkat cserél. Átlátható referenciaeszközt jelent az érdekeltek számára, akik az e területre vonatkozó uniós szakpolitika jövőbeli irányáról folyó vitában kívánnak részt venni. Ugyanakkor egy első választ is jelent az Európai Tanács azon felhívására, amely az uniós információkezelési stratégiával⁹² összhangban álló uniós szintű információkezelési eszközök létrehozására, valamint egy európai információcsere-modell szükségességének vizsgálatára⁹³ irányult.

A Bizottság e közleményt követően 2012-ben az európai információcsere-modellről szóló közleményt kíván közzétenni⁹⁴. Ennek érdekében a Bizottság 2010. januárban információfeltérképezési folyamatot indított a tagállamok közötti, bűnüldözési operatív információkra és egyéb információkra vonatkozó információcsere jogalapjaira és gyakorlati működésére vonatkozóan, amelynek eredményeit 2011-ben kívánja bemutatni a Tanácsnak és az Európai Parlamentnek⁹⁵.

⁹² A Tanács következtetései az uniós belső biztonság terén alkalmazandó információkezelési stratégiáról, Bel- és Igazságügyi Tanács, 2009.11.30. (uniós információkezelési stratégia).

⁹³ A stockholmi program – A polgárokat szolgáló és védő, nyitott és biztonságos Európa, 5731/10 sz. tanácsi dokumentum, 2010.3.3., 4.2.2 szakasz.

⁹⁴ Ezt a Bizottságnak a stockholmi program végrehajtásáról szóló cselekvési terve rögzíti (COM(2010) 171, 2010.4.20.).

⁹⁵ A Bizottság az információfeltérképezési folyamat során szorosan együttműködik az uniós és EFTA tagállamok, az Europol, az Eurojust és a Frontex képviselőiből és az európai adatvédelmi biztosból álló információfeltérképezési projektcsoporttal.

Végül ez a közlemény először vázolja a Bizottság elképzeléseit azokról az átfogó elvekről, amelyeket az adatgyűjtésre, -tárolásra és -cserére vonatkozó eszközök továbbfejlesztése során követni kíván. Ezeket az elveket a Bizottság a fennálló eszközök értékelése során is alkalmazni fogja. A szakpolitikák kidolgozásának és értékelésének ezen elvi alapokon álló megközelítése várhatóan javítani fogja a jelenlegi és jövőbeli eszközök koherenciáját és eredményességét, az állampolgárok alapvető jogainak teljes tiszteletben tartása mellett.

I. MELLÉKLET

Az alábbi adatok és példák a jelenleg működő információkezelési intézkedések gyakorlati működésének bemutatására szolgálnak.

Schengeni Információs Rendszer (SIS)

| A központi SIS (C.SIS) adatbázisba bevitt SIS figyelmeztető jelzések teljes száma⁹⁶ | | | |
|-------------------------------------------------------------------------------------------------------|-------------------|-------------------|-------------------|
| Figyelmeztető jelzés kategóriája | 2007 | 2008 | 2009 |
| Bankjegyek | 177,327 | 168,982 | 134,255 |
| Kitöltetlen okmányok | 390,306 | 360,349 | 341,675 |
| Lőfegyverek | 314,897 | 332,028 | 348,353 |
| Kiadott okmányok | 17,876,227 | 22,216,158 | 25,685,572 |
| Járművek | 3,012,856 | 3,618,199 | 3,889,098 |
| Keresett személyek (álnevek) | 299,473 | 296,815 | 290,452 |
| Keresett személyek (fő név) | 859,300 | 927,318 | 929,546 |
| Ebből: | | | |
| Olyan személyek, akiknek a letartóztatását kiadatás céljából kéri | 19,119 | 24,560 | 28,666 |
| A beutazási tilalmi listán szereplő harmadik országbeli állampolgárok | 696,419 | 746,994 | 736,868 |
| Eltűnt felnőttek | 24,594 | 23,931 | 26,707 |
| Eltűnt kiskorúak | 22,907 | 24,628 | 25,612 |
| Tanúk vagy bíróságra beidéztetett személyek | 64,684 | 72,958 | 78,869 |
| A közbiztonság veszélyeztetése megakadályozásának céljából leplezett figyelés alatt álló személyek | 31,568 | 34,149 | 32,571 |
| A nemzetbiztonság veszélyeztetése megakadályozásának céljából leplezett figyelés alatt álló személyek | 9 | 98 | 253 |
| Összesen | 22,933,370 | 27,919,849 | 31,618,951 |

⁹⁶ A 6162/10. sz. tanácsi dokumentum, 2010.2.5.; az 5764/09. sz. tanácsi dokumentum, 2009.1.28.; az 5441/08. sz. tanácsi dokumentum, 2008.1.30.

EURODAC – Az ugyanazon tagállamban vagy más tagállamban új kérelmet benyújtott menedékkérők mozgása (2008)

| | | Az első menedékjog iránti kérelem benyújtása szerinti tagállam ⁹⁷ | | | | | | | | | | | | | | | | | | | | | | | | | | | | 2. kérelmek összesen | | | |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|------------------------------------------------------------------------------|------------|----------|------------|--------------|--------------|------------|----------|--------------|------------|------------|--------------|--------------|------------|-----------|--------------|-----------|------------|----------|------------|--------------|--------------|--------------|-----------|------------|--------------|------------|--------------|----------------------|---------------|---------------|------------|
| | | AT | BE | BG | CH | CY | CZ | DE | DK | EE | EL | ES | FI | FR | HU | IE | IS | IT | LT | LU | LV | MT | NL | NO | PL | PT | RO | SE | SI | SK | UK | Home hits | Total hits |
| Az ujjenyomokat összehasonlítás céljából továbbító és olyan tagállamból (oszlopok) találatot kapó tagállamok, ahol az érintett korábban menedékkijog iránti kérelmet nyújtott be | AT | 1,725 | 74 | 2 | 0 | 1 | 87 | 274 | 5 | 2 | 31 | 12 | 25 | 115 | 212 | 5 | 0 | 134 | 3 | 14 | 0 | 9 | 52 | 49 | 1,371 | 1 | 42 | 111 | 17 | 260 | 61 | 1,725 | 4,694 |
| | BE | 180 | 5,450 | 4 | 0 | 3 | 38 | 408 | 17 | 0 | 41 | 17 | 28 | 378 | 67 | 28 | 0 | 69 | 3 | 37 | 0 | 2 | 180 | 73 | 625 | 6 | 3 | 192 | 17 | 58 | 205 | 5,450 | 8,129 |
| | BG | 5 | 2 | 116 | 0 | 1 | 1 | 5 | 1 | 0 | 7 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 2 | 0 | 0 | 1 | 3 | 0 | 0 | 6 | 8 | 0 | 0 | 4 | 116 | 164 |
| | CH | 32 | 52 | 1 | 4 | 3 | 5 | 35 | 0 | 0 | 17 | 17 | 8 | 39 | 19 | 1 | 0 | 355 | 0 | 1 | 0 | 13 | 15 | 37 | 3 | 1 | 0 | 41 | 4 | 4 | 25 | 4 | 732 |
| | CY | 1 | 0 | 0 | 0 | 68 | 0 | 1 | 0 | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 68 | 73 |
| | CZ | 55 | 12 | 0 | 0 | 0 | 637 | 48 | 4 | 0 | 0 | 3 | 4 | 13 | 0 | 1 | 0 | 8 | 2 | 1 | 0 | 0 | 7 | 6 | 17 | 1 | 0 | 13 | 0 | 1 | 6 | 637 | 839 |
| | DE | 260 | 268 | 12 | 0 | 4 | 79 | 1,852 | 42 | 0 | 174 | 39 | 56 | 256 | 106 | 9 | 2 | 200 | 5 | 26 | 2 | 5 | 174 | 137 | 149 | 4 | 43 | 567 | 30 | 89 | 128 | 1,852 | 4,718 |
| | DK | 44 | 43 | 3 | 0 | 0 | 13 | 126 | 119 | 0 | 27 | 13 | 44 | 36 | 13 | 4 | 0 | 47 | 0 | 7 | 0 | 0 | 30 | 225 | 55 | 2 | 4 | 436 | 2 | 7 | 41 | 119 | 1,341 |
| | EE | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 3 | 0 | 0 | 9 | 0 | 23 |
| | EL | 66 | 88 | 27 | 0 | 12 | 9 | 131 | 10 | 0 | 766 | 8 | 8 | 35 | 3 | 9 | 0 | 48 | 0 | 1 | 0 | 0 | 33 | 24 | 3 | 0 | 13 | 141 | 0 | 8 | 316 | 766 | 1,759 |
| | ES | 16 | 18 | 2 | 0 | 1 | 3 | 37 | 1 | 0 | 11 | 108 | 0 | 29 | 4 | 5 | 0 | 35 | 0 | 0 | 0 | 0 | 9 | 9 | 4 | 6 | 0 | 21 | 5 | 1 | 16 | 108 | 341 |
| | FI | 37 | 44 | 1 | 0 | 1 | 10 | 115 | 25 | 0 | 48 | 5 | 229 | 14 | 30 | 10 | 1 | 194 | 0 | 3 | 0 | 90 | 49 | 107 | 44 | 2 | 4 | 362 | 3 | 3 | 81 | 229 | 1512 |
| | FR | 365 | 339 | 0 | 0 | 8 | 97 | 502 | 29 | 0 | 92 | 78 | 31 | 860 | 161 | 8 | 0 | 336 | 11 | 26 | 1 | 29 | 106 | 74 | 1,739 | 8 | 9 | 286 | 37 | 75 | 190 | 860 | 5,497 |
| | HU | 297 | 53 | 4 | 0 | 1 | 3 | 169 | 4 | 0 | 2 | 3 | 19 | 70 | 791 | 1 | 0 | 27 | 1 | 10 | 0 | 0 | 28 | 32 | 0 | 0 | 76 | 79 | 19 | 14 | 14 | 791 | 1,717 |
| | IE | 20 | 21 | 0 | 0 | 4 | 2 | 24 | 1 | 0 | 9 | 8 | 0 | 23 | 4 | 309 | 0 | 35 | 0 | 4 | 0 | 4 | 16 | 7 | 0 | 0 | 0 | 22 | 2 | 2 | 187 | 309 | 704 |
| | IS | 4 | 3 | 0 | 0 | 0 | 0 | 3 | 0 | 0 | 3 | 1 | 1 | 6 | 2 | 1 | 0 | 3 | 0 | 1 | 0 | 1 | 3 | 10 | 1 | 0 | 0 | 11 | 1 | 0 | 3 | 0 | 58 |
| | IT | 390 | 111 | 5 | 0 | 6 | 33 | 349 | 11 | 0 | 270 | 47 | 27 | 192 | 60 | 23 | 5 | 3,290 | 0 | 11 | 0 | 58 | 78 | 116 | 9 | 2 | 6 | 201 | 59 | 224 | 680 | 3,290 | 6,263 |
| | LT | 3 | 1 | 0 | 0 | 1 | 3 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 5 | 0 | 0 | 0 | 4 | 14 | 0 | 0 | 5 | 0 | 2 | 0 | 5 | 40 |
| LU | 7 | 21 | 4 | 0 | 0 | 0 | 12 | 2 | 0 | 0 | 0 | 1 | 9 | 6 | 0 | 1 | 8 | 0 | 2 | 0 | 1 | 6 | 4 | 0 | 0 | 0 | 10 | 3 | 1 | 3 | 2 | 101 | |
| LV | 3 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 2 | 0 | 0 | 15 | |
| MT | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 5 | 1 | 0 | 0 | 0 | 6 | 0 | 0 | 0 | 16 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 16 | 32 | |
| NL | 109 | 223 | 16 | 0 | 1 | 27 | 198 | 21 | 0 | 113 | 16 | 29 | 109 | 33 | 7 | 1 | 226 | 0 | 14 | 0 | 58 | 1,240 | 95 | 16 | 8 | 9 | 289 | 8 | 22 | 129 | 1,240 | 3,017 | |
| NO | 84 | 103 | 6 | 0 | 2 | 13 | 256 | 76 | 0 | 199 | 55 | 57 | 78 | 23 | 8 | 0 | 524 | 8 | 13 | 1 | 83 | 86 | 276 | 164 | 1 | 9 | 826 | 10 | 21 | 96 | 276 | 3,078 | |
| PL | 188 | 65 | 0 | 0 | 0 | 30 | 68 | 15 | 0 | 0 | 2 | 4 | 75 | 1 | 1 | 0 | 0 | 3 | 3 | 0 | 0 | 7 | 27 | 1,208 | 1 | 1 | 43 | 1 | 13 | 4 | 1,208 | 1,760 | |
| PT | 1 | 10 | 0 | 0 | 0 | 0 | 4 | 1 | 0 | 0 | 11 | 0 | 9 | 0 | 0 | 0 | 2 | 0 | 2 | 0 | 0 | 2 | 2 | 0 | 3 | 0 | 2 | 0 | 1 | 2 | 3 | 52 | |
| RO | 43 | 2 | 5 | 0 | 1 | 9 | 33 | 0 | 0 | 3 | 0 | 5 | 14 | 11 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 9 | 1 | 1 | 0 | 64 | 17 | 0 | 4 | 4 | 64 | 227 | |
| SE | 243 | 133 | 30 | 0 | 4 | 36 | 516 | 173 | 0 | 143 | 29 | 143 | 145 | 80 | 16 | 3 | 276 | 0 | 16 | 0 | 130 | 98 | 430 | 147 | 5 | 13 | 1,914 | 11 | 26 | 122 | 1,914 | 4,882 | |
| SI | 14 | 4 | 0 | 0 | 0 | 1 | 10 | 1 | 0 | 1 | 1 | 2 | 15 | 6 | 0 | 0 | 5 | 0 | 1 | 0 | 0 | 2 | 3 | 0 | 0 | 0 | 5 | 45 | 3 | 2 | 45 | 121 | |
| SK | 105 | 4 | 0 | 0 | 0 | 7 | 33 | 0 | 1 | 0 | 0 | 1 | 2 | 12 | 0 | 0 | 3 | 0 | 0 | 1 | 0 | 4 | 4 | 4 | 0 | 0 | 9 | 2 | 195 | 6 | 195 | 393 | |
| UK | 109 | 153 | 7 | 0 | 3 | 12 | 276 | 30 | 0 | 108 | 6 | 38 | 209 | 25 | 217 | 2 | 768 | 0 | 8 | 0 | 43 | 128 | 76 | 7 | 4 | 11 | 174 | 6 | 46 | 3,141 | 3,141 | 5,607 | |
| 1. kérelmek összesen | 4,407 | 7,298 | 245 | 4 | 125 | 1,155 | 5,487 | 589 | 4 | 2,067 | 480 | 773 | 2,734 | 1,670 | 663 | 15 | 6,600 | 46 | 204 | 5 | 542 | 2,363 | 1,833 | 5,581 | 55 | 313 | 5,791 | 283 | 1,082 | 5,475 | 24,433 | 57,889 | |

⁹⁷ COM(2009) 494, 2009.9.25. A „hazai találatok” arra utalnak, hogy az érintett ugyanabban a tagállamban nyújtott be új menedékjog iránti kérelmet, mint amelyikben az előző kérelmet is benyújtotta.

Az előzetes utasinformációs rendszer (API)

**Az előzetes utasinformációk Egyesült Királyság általi használata
a határellenőrzés javítása és az illegális migráció elleni küzdelem céljára⁹⁸**

Az intézkedések száma 2009-ben

| | |
|------------------------------------------------------------------------|-----|
| Múltbeli negatív események (beutazás megtagadva) | 379 |
| Elveszett, ellopott vagy érvénytelenített útlevelek (okmány elkobozva) | 56 |

⁹⁸ Ezeket az információkat az Egyesült Királyság határellenőrzési hivatala bocsátotta a Bizottság rendelkezésére e közlemény céljára.

A váminformációs rendszer (VIR)

A VIR adatbázisba bevitt ügyek teljes száma (2009)⁹⁹

| Intézkedés | VIR (a VIR-egyezmény alapján) |
|-------------------|--------------------------------------|
| Létrehozott ügyek | 2,007 |
| Aktív ügyek | 274 |
| Lekérdezett ügyek | 11,920 |
| Törölt ügyek | 1,355 |

⁹⁹ Ezeket az információkat a Bizottság bocsátotta rendelkezésre.

A svéd kezdeményezés

Példák a svéd kezdeményezés használatára bűncselekmények nyomozása céljából¹⁰⁰

Emberölés 2009-ben az egyik tagállam fővárosában emberölési kísérlet történt. A rendőrség biológiai mintát vett egy pohárról, amiből a gyanúsított ivott. A mintából DNS kivonását követően kriminalisztikai szakemberek DNS-profilot hoztak létre. E profil összehasonlítása a nemzeti DNS-adatbázisban szereplő más referenciaprofilokkal nem eredményezett találatot. Ezért a nyomozást folytató rendőrség prümi kapcsolattartó pontján keresztül kérte a prümi határozat vagy a prümi megállapodás alapján ilyen adatok cseréjére feljogosított más tagállamok referenciaprofiljaival való összehasonlítást. Ez a határon átnyúló összehasonlítás találatot eredményezett. A nyomozást folytató rendőrség a svéd kezdeményezés alapján további adatokat kért a gyanúsítottól. Nemzeti kapcsolattartó pontja 36 órán belül több tagállamtól is választ kapott, ami lehetővé tette a rendőrség számára a gyanúsított azonosítását.

Nemi erőszak 2003-ban egy azonosítatlan gyanúsított megerőszakolt egy nőt. A rendőrség mintákat vett az áldozattól, de a mintából generált DNS-profil nem egyezett meg a nemzeti DNS-adatbázisban szereplő egyik referenciaprofillal sem. A DNS-összehasonlítás iránti kérés, amelyet a prümi kapcsolattartó pont a prümi határozat vagy a prümi megállapodás alapján ilyen adatok cseréjére feljogosított más tagállamokhoz intézett, találatot eredményezett. A nyomozást folytató rendőrség ezt követően a svéd kezdeményezés alapján további információkat kért a gyanúsítottól. Nemzeti kapcsolattartó pontja nyolc órán belül választ kapott, ami lehetővé tette a rendőrség számára a gyanúsított azonosítását.

¹⁰⁰ Ezeket a példákat az egyik tagállam rendőrsége bocsátotta a Bizottság rendelkezésére e közlemény céljára.

A prümi határozat

Németország találatai a DNS-profilok határokon átnyúló összehasonlítása esetén, a bűncselekmény típusa szerint (2009)¹⁰¹

| Találatok a bűncselekmény típusa szerint | Ausztria | Spanyolország | Luxemburg | Hollandia | Szlovénia |
|-------------------------------------------|----------|---------------|-----------|-----------|-----------|
| Közérdek elleni bűncselekmények | 32 | 4 | 0 | 5 | 2 |
| Személyi szabadság elleni bűncselekmények | 9 | 3 | 5 | 2 | 0 |
| Nemi erkölcs elleni bűncselekmények | 40 | 22 | 0 | 31 | 4 |
| Személy elleni bűncselekmények | 49 | 24 | 0 | 15 | 2 |
| Egyéb bűncselekmények | 3,005 | 712 | 18 | 1,105 | 71 |

¹⁰¹ A német kormány válasza Ulla Jelpke, Inge Höger és Jan Korte parlamenti kérdésére (hivatkozási szám: 16/14120), Bundestag, 16. ülészak, hivatkozási szám 16/14150, 2009.10.22. Ezek az adatok arra az időszakra vonatkoznak, amely akkor kezdődött, amikor az adott tagállam megkezdte az adatok cseréjét Németországgal, és 2009. szeptember 30-ig tart.

Az adatmegőrzési irányelv

Példák arra, amikor a tagállamok az adatmegőrzés segítségével derítettek fel súlyos bűncselekményeket¹⁰²

| | |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Szándékos emberölés | Egy tagállami rendőri szervnek sikerült nyomon követnie személyek egy csoportját, akik faji indítékok alapján hat személyt öltek meg. Az elkövetők SIM-kártyáik kicserélésével próbálták elkerülni, hogy elfogják őket, de híváslistáik és mobilberendezési azonosítóik alapján sikerült őket azonosítani. |
| Emberölés | Egy rendőri szervnek az áldozat mobiltelefonjához kapcsolódó forgalmi adatok elemzése útján sikerült bizonyítania két gyanúsított érintettségét egy emberölési ügyben. Ez lehetővé tette a nyomozók számára az útvonal rekonstrukcióját, amelyen az áldozat és a két gyanúsított együtt utazott. |
| Betöréses lopás | A hatóságoknak egy 17 betöréses lopás elkövető személyt az anonim SIM feltöltőkártyájához kapcsolódó forgalmi adatok vizsgálata segítségével sikerült felkutatniuk. Barátnője azonosítása után az elkövetőt is sikerült megtalálniuk. |
| Csalás | A nyomozók felderítettek egy csalást, amelynek keretében egy személyek egy csoportja drága gépjárműveket kínált „készpénzért” az interneten, és rendszeresen kirabolták a gépjármű átvételére megjelent személyeket. Egy IP-cím lehetővé tette a rendőrség számára az előfizető azonosítását és a tettesek letartóztatását. |

¹⁰² Ezek az anonim példák egy 2009-es, a 2006/24/EK irányelv (adatmegőrzési irányelv) átültetésére vonatkozó bizottsági kérdőívre adott tagállami válaszokon alapulnak.

A pénzügyi hírszerző egységek közötti együttműködés

A nemzeti pénzügyi hírszerző egységek által a FIU-neten keresztül benyújtott információkérések teljes száma¹⁰³

| Év | Információkérések | Aktív felhasználók |
|------|-------------------|--------------------|
| 2007 | 3,133 | 12 tagállam |
| 2008 | 3,084 | 13 tagállam |
| 2009 | 3,520 | 18 tagállam |

¹⁰³ Ezeket az információkat a FIU-net hivatala bocsátotta a Bizottság rendelkezésére e közlemény céljára.

A vagyon-visszaszerzési hivatalok közötti együttműködés

A tagállamok által benyújtott és az Europol által kezelt, jövedelem felkutatása iránti megkeresések száma¹⁰⁴

| Év | 2004 | 2005 | 2006 | 2007 |
|----------------------------------------------------|------|------|------|------|
| Megkeresés | 5 | 57 | 53 | 133 |
| Ebből: | | | | |
| Csaláshoz kapcsolódó ügyek | | | | 29 |
| Pénzmosáshoz kapcsolódó ügyek | | | | 26 |
| Kábítószerhez kapcsolódó ügyek | | | | 25 |
| Egyéb bűncselekményekhez kapcsolódó ügyek | | | | 18 |
| Kábítószerhez és pénzmosáshoz kapcsolódó ügyek | | | | 19 |
| Csaláshoz és pénzmosáshoz kapcsolódó ügyek | | | | 7 |
| Egyéb bűncselekménykombinációkhoz kapcsolódó ügyek | | | | 9 |

Az Eurojust által kezelt vagyonelkobzási ügyek (2006–2007)¹⁰⁵

| Ügytípusok | | Az ügyet indította | |
|-------------------------------------------------------------------------|----|--------------------|-----|
| Környezeti bűncselekményhez kapcsolódó ügyek | 1 | Németország | 27% |
| Bűnszervezetben való részvételhez kapcsolódó ügyek | 5 | Hollandia | 21% |
| Kábítószerkereskedelemhez kapcsolódó ügyek | 15 | Egyesült Királyság | 15% |
| Adócsaláshoz kapcsolódó ügyek | 8 | Finnország | 13% |
| Csaláshoz kapcsolódó ügyek | 8 | Franciaország | 8% |
| Héa-csaláshoz kapcsolódó ügyek | 1 | Spanyolország | 6% |
| Pénzmosáshoz kapcsolódó ügyek | 9 | Portugália | 4% |
| Korrupcióhoz kapcsolódó ügyek | 1 | Svédország | 2% |
| Vagyon elleni bűncselekményekhez kapcsolódó ügyek | 2 | Dánia | 2% |
| Fegyverkereskedelemhez kapcsolódó ügyek | 1 | Lettország | 2% |
| Iparjogvédelmi jog megsértéséhez és termékhamisításhoz kapcsolódó ügyek | 2 | | |
| Előleget érintő csaláshoz kapcsolódó ügyek | 2 | | |
| Hivatalos okmányok hamisításához kapcsolódó ügyek | 1 | | |
| Gépjárművekkel kapcsolatos bűncselekményhez kapcsolódó ügyek | 1 | | |
| Terrorizmushoz kapcsolódó ügyek | 1 | | |
| Okirathamisításhoz kapcsolódó ügyek | 2 | | |
| Emberkereskedelemhez kapcsolódó ügyek | 1 | | |

¹⁰⁴ A bűncselekményből származó jövedelmek azonosítása, felkutatása, befagyasztása és elkobzása terén az uniós tagállamokban fennálló gyakorlatok eredményességének értékelése – Zárójelentés (az Európai Bizottság, DG JLS részére), Matrix Insight, 2009.6.

¹⁰⁵ Uo.

A számítástechnikai bűnözésre figyelmeztető platformok

Példák arra, amikor a számítástechnikai bűnözésre figyelmeztető francia platform, a Pharos számítástechnikai bűncselekményeket vizsgált ki¹⁰⁶

| | |
|--------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Gyermekpornográfia | Egy internethasználó felhívta a Pharos figyelmét egy gyermekek szexuális zaklatását ábrázoló fényképeket és rajzfilm-stílusú képeket tartalmazó blogra. A blog szerzője, aki az egyik fényképen meztelenül volt látható, blogján keresztül maga is felvette a kapcsolatot gyermekekkel. A nyomozók fő gyanúsítottként egy matematikatanárt azonosítottak. Az otthonának átkutatása során 49 videót találtak, amelyek gyermekpornográfiát ábrázoló képeket tartalmaztak. A nyomozás emellett kiderítette, hogy otthoni óraadásra irányuló előkészületeket is tett. A vádlottat később felfüggesztett börtönbüntetésre ítélték. |
| Gyermekek szexuális zaklatása | A francia rendőrség információkat kapott arról, hogy egy személy az interneten pénzt kínál a gyermekekkel való szexuális érintkezésért. A Pharos nyomozója kiskorúnak adta ki magát és kapcsolatot vett fel a gyanúsítottal, aki szexuális érintkezésért cserébe készpénzt kínált neki. Az ebből kialakuló internetes csevegés lehetővé tette a Pharos számára a gyanúsított IP-címének azonosítását, és ennek alapján megállapították, hogy egy olyan városban tartózkodik, ahol nagy számban fordultak elő gyermekek szexuális zaklatásával járó ügyek. A vádlottat később felfüggesztett börtönbüntetésre ítélték. |

¹⁰⁶ A Pharos a „plate-forme d’harmonisation, d’analyse, de recoupement et d’orientation des signalements” rövidítése.

Europol

Példák az Europolnak a határokon átnyúló súlyos bűncselekmények elleni küzdelemhez való hozzájárulására¹⁰⁷

| | |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Andromeda művelet | 2009 decemberében az Europol segített egy 42 országban kapcsolatokkal rendelkező kábítószerkereskedelmi hálózat elleni nagyszabású határon átnyúló rendőri művelet végrehajtásában. A hálózat központja Belgiumban és Norvégiában volt, és Peruból származó kábítószerrel kereskedtek, amelyet Hollandián át szállítottak Belgiumba, az Egyesült Királyságba, Olaszországba és más tagállamokba. A rendőrségi együttműködést az Europol koordinálta; az igazságügyi együttműködést az Eurojust. A részt vevő hatóságok mobil irodát hoztak létre Pisában; az Europol pedig műveleti termet jelölt ki Hágában. Az Europol kereszthivatkozásokat hozott létre a gyanúsítottakra vonatkozó információk között, és a bűnözői hálózatot bemutató jelentést készített. |
| Résztvevők | Olaszország, Hollandia, Németország, Belgium, az Egyesült Királyság, Litvánia, Norvégia és az Eurojust. |
| Eredmények | A részt vevő rendőri erők lefoglaltak 49 kg kokaint, 10 kg heroint, 6000 ecstasy tablettát, két lőfegyvert, öt hamis személyazonosító okmányt és 43 000 euro készpénzt, valamint letartóztattak 15 főt. |
| Typhon művelet | 2008. április és 2010. február között az Europol elemzési támogatást nyújtott a Typhon műveletben részt vevő 20 ország rendőri erőinek. E nagyszabású művelet során, amely egy osztrák honlap útján gyermekpornográfiát ábrázoló képeket terjesztő pedofil hálózat ellen irányult, az Europol műszaki támogatást nyújtott és bűnüldözési operatív információk elemzését látta el az Ausztriától kapott képek alapján. Ezt követően értékelte az adatok megbízhatóságát és átstrukturálta az adatokat, majd elkészítette saját operatív információs anyagát. Kereszthivatkozásokat hozott létre az adatok és az elemzési célú munkafájlijában található információk között, és ennek alapján 30 operatív információkról szóló jelentést készített, amelyek alapján számos tagállamban indult nyomozás. |
| Résztvevők | Ausztria, Belgium, Bulgária, Kanada, Dánia, Franciaország, Németország, Magyarország, Olaszország, Litvánia, Luxemburg, Málta, Hollandia, Lengyelország, Románia, Szlovákia, Szlovénia, Spanyolország, Svájc és az Egyesült Királyság. |
| Eredmények | A részt vevő rendőri erők 286 gyanúsítottat azonosítottak, 118 gyanúsítottat letartóztattak és négy országban öt áldozatot mentettek meg, akik az ügyben zaklatást szenvedtek el. |

¹⁰⁷ Ezeket az információkat az Europol bocsátotta a Bizottság rendelkezésére e közlemény céljára. Az Andromeda műveletről további információk találhatóak a <http://www.eurojust.europa.eu/> címen.

Példák a súlyos bűncselekmények elleni, nagyszabású határokon átnyúló igazságügyi műveletek Eurojust általi koordinálására¹⁰⁸

| | |
|----------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Emberkereskedelem és a terrorizmus finanszírozása | 2010 májusában az Eurojust koordinált egy határokon átnyúló műveletet, amely egy Afganisztánban, Pakisztánban, Romániában, Albániában és Olaszországban tevékenykedő szervezett bűnözői hálózat öt tagjának letartóztatásához vezetett. A csoport afgán és pakisztáni állampolgárokat hamisított okmányokkal látott el, és Iránon, Törökországon és Görögországon keresztül Olaszországba csempészte őket. Olaszországba érkezésüket követően a migránsokat Németországba, Svédországba, Belgiumba, az Egyesült Királyságba és Norvégiába szállították. Az emberkereskedelemből származó jövedelmet a terrorizmus finanszírozására szánták. |
| Bankkártyacsalás | A határokon átnyúló rendőrségi és igazságügyi együttműködés koordinálása révén az Europol és az Eurojust segítette felszámolni egy bankkártyacsalással foglalkozó, Írországból, Olaszországból, Hollandiából, Belgiumból és Romániából tevékenykedő hálózatot. A hálózat körülbelül 15 000 bankkártya azonosító adatait lopta el, 6,5 millió eurós veszteséget okozva. E művelet előtt, amely 24 letartóztatást eredményezett 2009 júliusában, belga, ír, olasz, holland és román bírák megkönnyítették európai elfogatóparancsok kiadását és a gyanúsítottakkal szembeni lehallgatási kérelmek elbírálását. |
| Emberkereskedelem és kábítószerkereskedelem | Az Eurojust által 2009 márciusában szervezett koordinációs megbeszélés nyomán az olasz, a holland és a kolumbiai hatóságok 62 emberkereskedelemmel és kábítószerkereskedelemmel gyanúsított személyt tartóztattak le. A hálózat kiszolgáltató helyzetben levő nőket csempészett Nigériából Hollandiába, és Olaszországban, Franciaországban és Spanyolországban prostitúcióra kényszerítették őket. A prostitúcióból származó jövedelemből a hálózat Kolumbiában kokain vásárolt, amelyet az EU-ba szállítottak fogyasztás céljára. |

¹⁰⁸ Ezek a példák a <http://www.eurojust.europa.eu/> honlapról származnak.

Az utas-nyilvántartási adatállomány (PNR)

Példák arra, hogy a PNR-elemzés határokon átnyúló súlyos bűncselekmények nyomozása szempontjából releváns információkat eredményezett¹⁰⁹

| | |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Gyermekkereskedelem | A PNR-elemzés kimutatta, hogy három kísérlet nélküli gyermek utazik egy uniós tagállamból egy harmadik országba, annak megjelölése nélkül, hogy érkezéskor ki fogadja őket. Miután a tagállami rendőrség az indulást követően riasztotta a harmadik országbeli hatóságokat, a hatóságok letartóztatták a gyermekek fogadására érkező személyt – a tagállamban nyilvántartott, szexuális bűncselekményt elkövetett személyt. |
| Emberkereskedelem | PNR-elemzés kimutatta, hogy emberkereskedők egy csoportja mindig ugyanazon az útvonalon utazott. Hamis okmányok felhasználásával jelentkeztek egy EU-n belüli járatra utasfelvételre, ugyanakkor azonban valódi okmányokkal egy másik, harmadik országba tartó járatra is bejelentkeztek, a repülőtéri váróba bejutva pedig az EU-n belüli járatra szálltak fel. |
| Hitelkártyacsalás | Egy tagállamba több család utazott lopott hitelkártyákkal vásárolt jegyekkel. A vizsgálat kimutatta, hogy egy bűnözői csoport használta ezeket a hitelkártyákat a jegyvásárláshoz, majd a jegyeket telefonközpontokon keresztül továbbértékesítették. Az utazókat PNR-adatok segítségével sikerült a hitelkártyákkal és az eladókkal kapcsolatba hozni. |
| Kábítószerkereskedelem | Egy tagállami rendőrségnek információi voltak arról, hogy egy adott személy harmadik országból való kábítószerkereskedelemben érintett, de a határőrök az EU-ba érkezésekor soha nem találtak nála semmit. A PNR-elemzés kimutatta, hogy mindig egy bűntársával együtt utazott. A bűntárs átkutatása során nagy mennyiségű kábítószerrel találtak. |

¹⁰⁹

Ezeket a példákat az információforrás védelem érdekében anonimizáltuk.

A terrorizmus finanszírozásának felderítését célzó program (TFTP)

Példák arra, hogy a TFTP egyes terrorcselekmények nyomozása szempontjából releváns információkat eredményezett¹¹⁰

A 2008-as barcelonai merényletkísérlet

2008 januárjában Barcelonában tíz gyanúsítottat tartóztattak le a város tömegközlekedési hálózatát célzó megghiúsított merényletkísérlettel összefüggésben. TFTP-adatok segítségével azonosították a gyanúsítottak ázsiai, afrikai és észak-amerikai kapcsolatait.

A 2006-os transzatlanti folyékony robbanóanyaggal elkövetett merényletkísérlet

TFTP-információk felhasználásával folyt a nyomozás és került sor az érintettek elítélésére egy 2006 augusztusi megghiúsított merényletkísérlettel összefüggésben, amelynek során tíz transzatlanti – az Egyesült Királyságból az Egyesült Államokba, illetve Kanadába tartó – járatot próbáltak felrobbantani.

A 2005-ös londoni bombamerényletek

A TFTP-adatok új nyomokat szolgáltatottak a nyomozóknak, megerősítették a gyanúsítottak személyazonosságát és felfedték a támadásért felelős egyének közötti kapcsolatokat.

A 2004-es madridi bombamerényletek

Több uniós tagállamnak bocsátottak rendelkezésre TFTP-adatokat a merényletet követően indított nyomozások segítése érdekében.

¹¹⁰ Második jelentés az EU-ból származó személyes adatoknak az Egyesült Államok Pénzügyminisztériuma általi, terrorizmusellenes célokat szolgáló feldolgozásáról, Jean-Louis Bruguière bíró, 2010. január

II. MELLÉKLET

A működő, és a végrehajtási vagy mérlegelési szakaszban eszközök áttekintése táblázatos formában

| Eszköz | Előzmények | Cél(ok) | Szerkezet | Az érintett személyes adatok köre | Az adatokhoz való hozzáférés | Adatvédelem | Adatmegőrzés | A végrehajtás állapota | Felülvizsgálat |
|---------------------------------------------|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Schengeni Információs Rendszer (SIS) | A tagállamok kezdeményezték. | A közbiztonság és ezen belül a nemzetbiztonság fenntartása a schengeni térségen belül, továbbá a személyek mozgásának megkönnyítése az e rendszeren keresztül közölt adatok felhasználásával. | Központosított: N.SIS (nemzeti részek), amelyeket interfész kapcsol össze a C.SIS-szel (központi rész). | Nevek és álnév, fizikai jellemzők, születési hely és idő, állampolgárság, továbbá, hogy a személy fegyvert visel-e vagy erőszakos-e. A SIS figyelmeztető jelzések személyek több különböző csoportjához kapcsolódnak. | A rendőrség, a határőrség, a vámhatóságok és az igazságügyi hatóságok minden adathoz hozzáférhetnek; a bevándorlási és konzuli hatóságok a belépési tilalmi listához, valamint az ellopott és elveszett okmányok jegyzékéhez. Az Europol és az Eurojust egyes adatokhoz férhet hozzá. | Az Európa Tanács 108. sz. egyezménye és R (87) 15. sz. rendőrségi ajánlása. | A személyek felkutatása céljából a SIS-be bevitt személyes adatok csak annyi ideig tárolhatók, amennyi annak a célnak az eléréséhez szükséges, amely okán a személyes adatokat a hatóság megkapta, illetve legfejlebb három évig. Az általuk okozott közbiztonsági vagy a nemzetbiztonsági fenyegetésre tekintettel leplezett figyelés alá vont személyekre vonatkozó adatokat egy év elteltével kell törölni. | A SIS teljes körűen alkalmazandó 22 tagállamban, valamint Svájcban, Norvégiában és Izlandon. Az Egyesült Királyság és Írország részt vesz a SIS-ben a beutazási tilalmi listán szereplő harmadik országbeli állampolgárokkal kapcsolatos figyelmeztető jelzések kivételével. Bulgária, Románia és Liechtenstein várhatóan hamarosan végrehajtja ezt az intézkedést. | Az aláírók javasolhatják a Schengeni Egyezmény módosítását. A módosított szöveget egyhangúlag kell elfogadni, és a parlamenteknek ratifikálniuk kell azt. |

A működő, és a végrehajtási vagy mérlegelési szakaszban eszközök áttekintése táblázatos formában

| Eszköz | Előzmények | Cél(ok) | Szerkezet | Az érintett személyes adatok köre | Az adatokhoz való hozzáférés | Adatvédelem | Adatmegőrzés | A végrehajtás állapota | Felülvizsgálat |
|---------------------------------------------------|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Schengeni Információs Rendszer II (SIS II) | A Bizottság kezdeményezte. | A szabadságon, a biztonságon és a jog érvényesülésén alapuló térségen belül egy magas biztonsági szint biztosítása, valamint a személyek mozgásának megkönnyítése, a rendszer útján szolgáltatott információk felhasználásával. | Központosított: N.SIS II (nemzeti részek), amelyeket interfész kapcsol össze a CS-SIS-szel (központi rész). A SIS II a biztonságos s-TESTA hálózaton fog üzemelni. | A SIS-ben szereplő adatok, valamint újjelnyomatok, fényképek, az európai elfogatóparancs másolatai, a személyazonosságga l való visszaélésre vonatkozó figyelmeztető jelzések, továbbá a figyelmeztető jelzések közötti kapcsolatok. A SIS II figyelmeztető jelzések személyek több különböző csoportjához kapcsolódnak. | A rendőrség, a határőrség, a vámhatóságok és az igazságügyi hatóságok minden adathoz hozzáférhetnek majd; a bevándorlási és konzuli hatóságok a belépési tilalmi listához, valamint az ellopott és elvesztett okmányok jegyzékéhez. Az Eurojust és az adatokhoz férhet majd hozzá. | A SIS II-t szabályozó alap jogi aktusok által megállapított különös szabályok, a 95/46/EK irányelv, a 45/2001/EK rendelet, a 2008/977/IB tanácsi kerethatározat, az Európa Tanács 108. sz. egyezménye és az R (87) 15. sz. rendőrségi ajánlás. | A személyek felkutatása céljából a SIS-be bevitt személyes adatok csak annyi ideig tárolhatók, amennyi annak a célnak az eléréséhez szükséges, amely okán a személyes adatokat a hatóság megkapta, illetve legfeljebb három évig. Az általuk okozott közbiztonsági vagy a nemzetbiztonsági fenyegetésre tekintettel leplezett figyelés alá vont személyekre vonatkozó adatokat egy év elteltével kell törölni. | A SIS II végrehajtás alatt áll. Üzembe helyezését követően az EU 27 tagállamában, Svájcban, Liechtensteinben, Norvégiában és Izlandon alkalmazzák majd. Az Egyesült Királyság és Írország részt vesz majd a SIS II-ben a beutazási tilalmi listán szereplő harmadik országbeli állampolgárokkal kapcsolatos figyelmeztető jelzések kivételével. | A Bizottságnak két évente előrehaladási jelentést kell tennie az Európai Parlamentnek (EP) és a Tanácsnak a SIS II fejlesztéséről és a SIS-ről való esetleges áttérésről |

A működő, és a végrehajtási vagy mérlegelési szakaszban eszközök áttekintése táblázatos formában

| Eszköz | Előzmények | Cél(ok) | Szerkezet | Az érintett személyes adatok köre | Az adatokhoz való hozzáférés | Adatvédelem | Adatmegőrzés | A végrehajtás állapota | Felülvizsgálat |
|----------------|----------------------------|------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| EURODAC | A Bizottság kezdeményezte. | Segítséget nyújtani annak megállapításában, hogy melyik tagállamnak kell megvizsgálnia egy adott menedékjog iránti kérelmet. | Központosított, az EURODAC központi egységhez interfészen keresztül kapcsolódó nemzeti hozzáférési pontokkal. Az EURODAC az s-TESTA hálózaton üzemel. | Ujjlenyomat-adatok, nem, a menedékkérelem benyújtásának helye és időpontja, a származási hely szerinti tagállam által használt referenciaszám, az ujjlenyomattétel dátuma, az adatok továbbításának és bevitelének dátuma. | A tagállamoknak meg kell adniuk az ezen adatokhoz hozzáféréssel rendelkező hatóságok jegyzékét, amely általában a menekültügyi és migrációs hatóságokat, a határőrséget és a rendőrséget öleli fel. | 95/46/EK irányelv. | 10 év a menedékkérők ujjlenyomatai esetében; 2 év a külső határok jogellenes átlépése miatt elfogott harmadik országbeli állampolgárok ujjlenyomatai esetében. | Az EURODAC rendelet valamennyi tagállamban, valamint Norvégiában, Izlandon és Svájcban és hatályos. Előkészületben van a Liechtenstein csatlakozását lehetővé tévő megállapodás megkötése. | A Bizottságnak évente kell jelentést benyújtania az EP-nek és a Tanácsnak az EURODAC központi egység működéséről. |

A működő, és a végrehajtási vagy mérlegelési szakaszban eszközök áttekintése táblázatos formában

| Eszköz | Előzmények | Cél(ok) | Szerkezet | Az érintett személyes adatok köre | Az adatokhoz való hozzáférés | Adatvédelem | Adatmegőrzés | A végrehajtás állapota | Felülvizsgálat |
|------------------------------------------------|------------------------------|--------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| Vízuminformációs rendszer (VIS) | A Bizottság kezdeményezte. | A közös vízümpolitika a végrehajtásának elősegítése és a tagállamok belső biztonságát érő fenyegetések megelőzése. | Központosított, a központi részhez interfészen keresztül kapcsolódó nemzeti részekkel. Az VIS az s-TESTA hálózaton fog üzemelni. | Vízumkérelmek, ujjlenyomatok, fényképek, vízumügyekben hozott kapcsolódó határozatok és az összefüggő kérelmek közötti kapcsolatok. | A vízum-, menekültügyi, bevándorlási és határellenőrzési hatóságok minden adathoz hozzáférhetnek majd. A rendőrség és az Europol súlyos bűncselekmények megelőzése, felderítése és kivizsgálása érdekében betekinthez a VIS-be. | A VIS II-t szabályozó alap jogi aktusok által megállapított különös rendelkezések, a 95/46/EK irányelv, a 45/2001/EK rendelet, a 2008/977/IB tanácsi kerethatározat, az Európa Tanács 108. sz. egyezménye és annak 181. sz. kiegészítő jegyzőkönyve, valamint az R (87) 15. sz. rendőrségi ajánlás. | 5 év. | A VIS végrehajtás alatt áll, és alkalmazni kell majd mindegyik tagállamban (az Egyesült Királyság és Írország kivételével), valamint Norvégiában, Izlandon és Svájcban. | A Bizottságnak a VIS elindítása után három évvel és azt követően négyévente jelentést kell tennie az EP-nek és a Tanácsnak a VIS működéséről. |
| Előzetes utasinformációs rendszer (API) | Spanyolország kezdeményezte. | A határellenőrzés javítása és az illegális migráció elleni küzdelem. | Decentralizált. | Az útlevelekből származó személyes adatok, a beszállás helye és az EU-ba való belépés helye. | A határellenőrzési hatóságok, és kérelem alapján a bűnüldöző hatóságok. | 95/46/EK irányelv. | Az adatokat 24 órával a járat EU-ba érkezését követően törölni kell. | Az API minden tagállamban hatályos, de csak kevés tagállam használja. | A Bizottság 2011-ben értékelni fogja az API-rendszert. |

A működő, és a végrehajtási vagy mérlegelési szakaszban eszközök áttekintése táblázatos formában

| Eszköz | Előzmények | Cél(ok) | Szerkezet | Az érintett személyes adatok köre | Az adatokhoz való hozzáférés | Adatvédelem | Adatmegőrzés | A végrehajtás állapota | Felülvizsgálat |
|------------------------------|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------|---------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|-----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| II. Nápolyi Egyezmény | A tagállamok kezdeményezték. | A nemzeti vámhatóságok segítése a nemzeti vámrendelkezések megsértésének megelőzése és felkutatása, valamint a közösségi és a nemzeti vámrendelkezések megsértésének üldözése és megbüntetése során. | Decentralizált, egy sor központi koordináló egységen keresztül üzemel. | Valamely azonosított vagy azonosítható személyhez kapcsolódó összes információ. | A központi koordináltó egységek továbbítják az adatokat a nemzeti vámhatóságoknak, nyomozó hatóságoknak és bíróságoknak, valamint – az adatokat szolgáltató tagállam előzetes hozzájárulásával – egyéb hatóságoknak. | A 95/46/EK irányelv és az Európa Tanács 108. egyezménye. Az adatoknak a fogadó tagállamban legalább azonos szintű védelemben kell részesülniük, mint az azokat szolgáltató tagállamban. | Az adatok a megadásuk céljának eléréséhez szükséges időtartamot meg nem haladó ideig őrizhetők meg. | Az egyezményt mindegyik tagállam ratifikálta. | Az aláírók javasolhatják a II. Nápolyi Egyezmény módosítását. A módosított szöveget a Tanácsnak el kell fogadnia, és a tagállamoknak ratifikálniuk kell azt. |

A működő, és a végrehajtott vagy mérlegelési szakaszban eszközök áttekintése táblázatos formában

| Eszköz | Előzmények | Cél(ok) | Szerkezet | Az érintett személyes adatok köre | Az adatokhoz való hozzáférés | Adatvédelem | Adatmegőrzés | A végrehajtás állapota | Felülvizsgálat |
|--------------------------------------|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|-------------------------------------------------------------------------------------------------------------|
| Váminformációs rendszer (VIR) | A tagállamok kezdeményezték. | Az illetékes hatóságok segítése a nemzeti vámjogszabályok megsértése súlyos eseteinek megelőzése, kivizsgálása és a büntetőeljárás lefolytatása során. | Központosított, elérhető az egyes tagállamok és a Bizottság termináljain keresztül. A VIR és a FIDE az AFIS alapján üzemel, amely a közös kommunikációs hálózatot, a közös rendszerinterfészt, illetve a Bizottság által szolgáltatott biztonságos internet-hozzáférést használja. | Nevek és felvett nevek, születési idő és hely, állampolgárság, nem, fizikai jellemzők, személyazonosító okmányok, cím, korábbi erőszakos cselekmény, a VIR-be történő adatfelvétel oka, javasolt intézkedés, a szállítóeszköz rendszáma. | A VIR adataihoz a nemzeti vámhatóságok, az Europol és az Eurojust férhet hozzá. | A VIR-egyezmény által megállapított különös szabályok, a 95/46/EK irányelv, a 45/2001/EK rendelet, az Európa Tanács 108. sz. egyezménye és az R (87) 15. sz. rendőrségi ajánlás. | A VIR-ből más rendszerekbe kockázatkezelés vagy operatív elemzés céljából átmásolt személyes adatokat csak a kimásolás céljának eléréséhez szükséges ideig, és legfeljebb 10 évig szabad tárolni. | Minden tagállamban hatályos. | A Bizottság a tagállamokkal együttműködve évente jelentést tesz az EP-nek és a Tanácsnak a VIR működéséről. |

A működő, és a végrehajtási vagy mérlegelési szakaszban eszközök áttekintése táblázatos formában

| Eszköz | Előzmények | Cél(ok) | Szerkezet | Az érintett személyes adatok köre | Az adatokhoz való hozzáférés | Adatvédelem | Adatmegőrzés | A végrehajtás állapota | Felülvizsgálat |
|---------------------------|---------------------------|--------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|
| Svéd kezdeményezés | Svédország kezdeményezte. | A bűnügyi nyomozások és bűnüldözési operatív műveletek célját szolgáló információcsere egyszerűsítése. | Decentralizált, a tagállamoknak nemzeti kapcsolattartó pontokat kell kijelölniük a sürgős információkérések kezelésére. | A bűnüldöző hatóságok rendelkezésére álló bármely bűnüldözési információ vagy bűnüldözési operatív információ. | A rendőrség, vámhatóság és a bűncselekmények kivizsgálására hatáskörrel rendelkező bármely egyéb hatóság (a hírszerző szolgálatok kivételével). | Nemzeti adatvédelmi szabályok, továbbá az Európa Tanács 108. sz. egyezménye és annak 181. sz. kiegészítő jegyzőkönyve, valamint az R (87) 15. sz. rendőrségi ajánlás. | Az ezen eszköz alapján rendelkezésre bocsátott információk és operatív információk csak arra a célra használhatók fel, amelyre azokat átadták, és az átadó tagállam által meghatározott külön feltételek betartásával. | A 31 aláíró (EU és EFTA-államok) közül 12 nemzeti jogszabályt fogadott el az eszköz végrehajtására; öt állam az adatkéréshez kitölti a formanyomtatványt; és két állam gyakran használja az eszközt információcsere céljára. | A Bizottságnak 2010-ben kell benyújtania értékelő jelentését a Tanácsnak. |

A működő, és a végrehajtási vagy mérlegelési szakaszban eszközök áttekintése táblázatos formában

| Eszköz | Előzmények | Cél(ok) | Szerkezet | Az érintett személyes adatok köre | Az adatokhoz való hozzáférés | Adatvédelem | Adatmegőrzés | A végrehajtás állapota | Felülvizsgálat |
|--------------------------|------------------------------|-------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|
| A prümi határozat | A tagállamok kezdeményezték. | A bűncselekmények, elsősorban a terrorizmus megelőzésének elősegítése és a közrend fenntartása. | Decentralizált, az összekapcsolást az s-TESTA hálózat biztosítja. Az adatok összehasonlítása iránti beérkező és kimenő kéréseket nemzeti kapcsolattartó pontok kezelik. | Anonim DNS-profilok és ujjlenyomatok, gépjármű-nyilvántartási adatok, és a terrorizmushoz fűződő kapcsolatokkal gyanúsított személyekre vonatkozó információk. | A kapcsolattartó pontok továbbítják a kéréseket; a belöldi hozzáférést a nemzeti jog szabályozza. | A prümi határozattal megállapított különleges szabályok, valamint az Európa Tanács 108. sz. egyezménye és annak 181. sz. kiegészítő jegyzőkönyve, valamint az R (87) 15. sz. rendőrségi ajánlás. Magánszemélyek a nemzeti adatvédelmi biztoshoz fordulhatnak a személyes adatok feldolgozásához fűződő jogaik érvényesítése érdekében. | A személyes adatokat törölni kell, ha azokra az átadás céljából már nincs szükség. Az átvadó államban irányadó leghosszabb adatmegőrzési időszak kötelező a fogadó államra. | A prümi határozat végrehajtás alatt áll. Tíz tagállam kapott engedélyt a DNS, öt az ujjlenyomatok, hét pedig a gépjármű-nyilvántartási adatok cseréjére. Norvégia és Izland ezen eszközökhöz való csatlakozása folyamatban van. | A Bizottságnak 2012-ben kell benyújtania értékelő jelentését a Tanácsnak. |

A működő, és a végrehajtási vagy mérlegelési szakaszban eszközök áttekintése táblázatos formában

| Eszköz | Előzmények | Cél(ok) | Szerkezet | Az érintett személyes adatok köre | Az adatokhoz való hozzáférés | Adatvédelem | Adatmegőrzés | A végrehajtás állapota | Felülvizsgálat |
|--------------------------------------------------------------------|--------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Az adatmegőrzési irányelv | A tagállamok kezdeményezték. | A súlyos bűncselekmények kivizsgálásának, felderítésének és üldözésének javítása a kommunikációs forgalmi és helymeghatározó adatok megőrzése útján. | Decentralizált, az eszköz a távközlési szolgáltatók számára állapít meg adatmegőrzési kötelezettséget. | Telefonszám, IP-cím és mobilberendezési azonosító. | A hatóságok hozzáférési jogait nemzeti szinten szabályozzák. | A 95/46/EK irányelv és a 2002/58/EK irányelv. | 6-tól 24 hónapig. | Hat tagállam még nem ültette át ezt az irányelvet, továbbá a német és a román alkotmánybíróság alkotmányellenesnek nyilvánította a végrehajtó jogszabályokat. | A Bizottságnak 2010-ben kell benyújtania értékelő jelentését az EP-nek és a Tanácsnak. |
| Európai Bűnügyi Nyilvántartási Információs Rendszer (ECRIS) | Belgium kezdeményezte és a Bizottság terjesztette be a javaslatot. | Az uniós polgárokra vonatkozóan a bűnügyi nyilvántartásokban szereplő adatok határokon átnyúló megosztásának javítása. | Decentralizált, az összekapcsolás központi hatóságokon keresztül valósul meg, amelyek az s-TESTA hálózatot fogják használni a bűnügyi nyilvántartásokból származó információk cseréjére. | Születési adatok; büntető ítélet, a büntetés és a bűncselekmény; kiegészítő információk, beleértve az ujjlenyomatokat (amennyiben rendelkezésre állnak). | Bíróságok és illetékes közigazgatási hatóságok. | A 2005/876/IB tanácsi határozat szabályait tartalmazó 2009/315/IB tanácsi kerethatározat által megállapított különös szabályok, valamint a 2008/977/IB tanácsi kerethatározat, az Európa Tanács 108. sz. egyezménye és az R (87) 15. sz. rendőrségi ajánlás. | A belföldi adatmegőrzési szabályok alkalmazandók, mivel az eszköz csak az adatcserét szabályozza. | Az ECRIS végrehajtás alatt áll. Kilenc tagállam megkezdte az információk elektronikus úton történő cseréjét. | A Bizottságnak két értékelő jelentést kell benyújtania a Tanácsnak és az EP-nek: a 2008/675/IB kerethatározatról 2011-ben; a 2009/315/IB kerethatározatról 2015-ben; 2016-tól a Bizottságnak a 2009/316/IB tanácsi határozat (ECRIS) működéséről rendszeresen beszámolót kell közzétennie. |

A működő, és a végrehajtási vagy mérlegelési szakaszban eszközök áttekintése táblázatos formában

| Eszköz | Előzmények | Cél(ok) | Szerkezet | Az érintett személyes adatok köre | Az adatokhoz való hozzáférés | Adatvédelem | Adatmegőrzés | A végrehajtás állapota | Felülvizsgálat |
|----------------------------------------------------------------------|------------------------------|-----------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| A pénzügyi hírszerző egységek közötti együttműködés (FIU-net) | Hollandia kezdeményezte. | A pénzmosás és a terrorizmus finanszírozásának elemzéséhez és nyomozásához szükséges információk cseréje. | Decentralizált, a FIU-k a FIU-neten keresztül cserélnék információkat, amely az s-TESTA hálózaton üzemel. Hamarosan sor kerülhet az Europol SIENA alkalmazásának igénybevételére a FIU-net céljaira. | A pénzmosás és a terrorizmus finanszírozásának elemzése vagy nyomozása szempontjából releváns bármely adat. | Pénzügyi hírszerző egységek (a rendőrségen, a bíróságokon vagy a pénzügyi hatóságoknak beszámoló közigazgatási testületeken belül). | A 2008/977/IB tanácsi kerethatározat, az Európa Tanács 108. sz. egyezménye és R (87) 15. sz. rendőrségi ajánlása. | A belföldi adatmegőrzési szabályok alkalmazandók, mivel az eszköz csak az adatcserét szabályozza. | Húsz tagállam vesz részt a FIU-netben, amely az s-TESTA hálózaton üzemelő online adatmegosztási alkalmazás. | Pénzügyi szolgáltatásokról szóló cselekvési tervének részeként a Bizottság 2009 óta folytatja a 2005/60/EK irányelv végrehajtásának felülvizsgálatát. |
| A vagyoni visszaszerzési hivatalok közötti együttműködés | A tagállamok kezdeményezték. | A bűncselekményből származó jövedelmek felkutatásához és azonosításához szükséges információk cseréje. | Decentralizált, a vagyoni visszaszerzési hivataloknak az információcserét a svéd kezdeményezésen keresztül kell bonyolítaniuk. Hamarosan sor kerülhet az Europol SIENA alkalmazásának igénybevételére a vagyoni visszaszerzési hivatalok együttműködésének céljaira. | A célzott tulajdon, pl.: bankszámlák, ingatlan és személygépkocsik adatai, valamint a keresett személyek adatai, így a név, cím, részvényesekre vonatkozó vagy céges adatok. | A vagyoni visszaszerzési hivatalok. | Az Európa Tanács 108. sz. egyezménye és annak 181. sz. kiegészítő jegyzőkönyve, valamint az R (87) 15. sz. rendőrségi ajánlása. | A belföldi adatmegőrzési szabályok alkalmazandók, mivel az eszköz csak az adatcserét szabályozza. | Több mint húsz tagállam hozott létre vagyoni visszaszerzési hivalt; tizenkét tagállam vesz részt egy kísérleti projektben, amely az Europol SIENA alkalmazását veszi igénybe a vagyoni felkutatása szempontjából releváns adatok cseréjéhez. | A Bizottságnak 2010-ben kell benyújtania értékelő jelentését a Tanácsnak. |

A működő, és a végrehajtási vagy mérlegelési szakaszban eszközök áttekintése táblázatos formában

| Eszköz | Előzmények | Cél(ok) | Szerkezet | Az érintett személyes adatok köre | Az adatokhoz való hozzáférés | Adatvédelem | Adatmegőrzés | A végrehajtás állapota | Felülvizsgálat |
|-----------------------------------------------------------------------|------------------------------|-------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A számítástechnikai bűnözés elleni nemzeti és uniós platformok | Franciaország kezdeményezte. | Az interneten elkövetett bűncselekményekre vonatkozó információk gyűjtése, cseréje és elemzése. | Decentralizált, a nemzeti figyelmeztető platformokból és a számítástechnikai bűnözés elleni küzdelem Europol által kezelt platformjából áll. Hamarosan sor kerülhet az Europol SIENA alkalmazásának igénybevételére a platformok közötti adatsere céljaira. | Az interneten észlelt jogellenes tartalom vagy magatartás. | A nemzeti platformok kapják az állampolgárok bejelentéseit; a számítástechnikai bűnözés elleni küzdelem Europol által kezelt platformja pedig a bűnüldöző hatóságok bejelentéseit a számítástechnikai bűnözés súlyos, határokon átnyúló eseteiről. | Az Europol határozat és a 2008/977/IB tanácsi kerethatározat által megállapított különös szabályok, az Európa Tanács 108. sz. egyezménye és annak 181. sz. kiegészítő jegyzőkönyve, az R (87) 15. sz. rendőrségi ajánlás, és a 45/2001/EK rendelet. | A belföldi adatmegőrzési szabályok alkalmazandók, mivel az intézkedés csak az információcserét szabályozza. | Majdnem mindegyik tagállam hozott létre nemzeti figyelmeztető platformot; az Europol dolgozik a számítástechnikai bűnözés elleni küzdelem európai platformján. | Az Europol tevékenysége kiterjed a számítástechnikai bűnözésre, a jövőben pedig be fog számolni az uniós platform tevékenységéről a jóváhagyás céljából a Tanács, és tájékoztatás céljából az Európai Parlament elé terjesztett éves jelentéseiben. |

A működő, és a végrehajtási vagy mérlegelési szakaszban eszközök áttekintése táblázatos formában

| Eszköz | Előzmények | Cél(ok) | Szerkezet | Az érintett személyes adatok köre | Az adatokhoz való hozzáférés | Adatvédelem | Adatmegőrzés | A végrehajtás állapota | Felülvizsgálat |
|----------------|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Europol | A tagállamok kezdeményezték. | A szervezett bűnözés, a terrorizmus és a két vagy több tagállamot érintő súlyos bűncselekmények egyéb formáinak megelőzése és az ellenük folytatott küzdelem támogatása. | Az Europol hágai székhelyű uniós ügynökség. Az Europol fejleszti a SIENA-t, saját biztonságos információcsere-hálózati alkalmazását. | Az Europol Információs Rendszer (EIS) személyes adatokat tartalmaz, így az alábbiakat: biometrikus azonosítók, az Europol megbízatásának hatálya alá tartozó bűncselekményekkel gyanúsított személyek büntető ítéletei és a szervezett bűnözéshez fűződő kapcsolataik. Az elemzési célú munkafájlok (AWF) bármely releváns személyes adatot tartalmazhatnak. | Az EIS-hez az Europol nemzeti egységek, az összekötő tisztviselők, az Europol személyzete és az igazgató férhet hozzá. Az AWF-ekhez az összekötő tisztviselők hozzáférhetnek. Az Europolal megállapodást kötött harmadik országokkal sor kerülhet a személyes adatok cseréjére. | Az Europol határozat és a 2008/977/IB tanácsi kerethatározat által megállapított különös szabályok, az Európa Tanács 108. sz. egyezménye és annak 181. sz. kiegészítő jegyzőkönyve, az R (87) 15. sz. rendőrségi ajánlás, és a 45/2001/EK rendelet. | Az AWF-ek legfeljebb három évig tárolhatók, és további hároméves meghosszabbítás lehetséges. | Az Europol aktívan használják a tagállamok, valamint az Europolal operatív megállapodást kötött harmadik országok. Az Europol új jogalapját az összes tagállam végrehajtotta. | A közös ellenőrző szerv ellenőrzi a személyes adatok Europol általi feldolgozását, valamint az ilyen adatok Europol általi átadását egyéb felek részére. A testület rendszeresen jelentést terjeszt az EP és a Tanács elé. Az Europol a tevékenységéről szóló éves jelentést nyújt be jóváhagyás céljából a Tanács, és tájékoztatás céljából az EP elé. |

A működő, és a végrehajtási vagy mérlegelési szakaszban eszközök áttekintése táblázatos formában

| Eszköz | Előzmények | Cél(ok) | Szerkezet | Az érintett személyes adatok köre | Az adatokhoz való hozzáférés | Adatvédelem | Adatmegőrzés | A végrehajtás állapota | Felülvizsgálat |
|-----------------|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|--------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Eurojust | A tagállamok kezdeményezték. | A tagállamokban a nyomozások és a büntetőeljárások összehangolásának javítása, valamint az illetékes hatóságok közötti együttműködés fokozása. | Az Eurojust hágai székhelyű uniós szerv, amely az s-TESTA hálózatot használja adatcsere céljára. | A két vagy több tagállamot érintő súlyos bűncselekmények gyanúsítottjainak és elkövetőinek személyes adatai, így a születési adatok, elérhetőség, DNS-profil, ujjlenyomatok, fényképek, valamint távközlési forgalmi és helymeghatározó adatok. | Az Europol 27 nemzeti tagja, akik megoszthatják az adatokat nemzeti hatóságokkal és harmadik országokkal, ha az információ forrása ehhez hozzájárul. | Az Eurojust határozattal megállapított különleges szabályok, a 2008/977/IB tanácsi kerethatározat, valamint az Európa Tanács 108. sz. egyezménye és annak 181. sz. kiegészítő jegyzőkönyve, valamint az R (87) 15. sz. rendőrségi ajánlás. | Az adatokat törölni kell, ha átadásuk célja teljesült, és ha egy ügyet lezárnak. | Az Eurojust módosított jogalapját a tagállamok most hajtják végre. | 2014 júniusig a Bizottságnak felül kell vizsgálnia az Eurojust nemzeti tagjai közötti információcserét. 2013 júniusáig az Eurojustnak jelentést kell tennie a Tanácsnak és a Bizottságnak az ügyviteli rendszeréhez való nemzeti hozzáférés biztosításáról. A közös ellenőrző szerv ellenőrzi a személyes adatok Europol általi feldolgozását, és évente jelentést tesz a Tanácsnak. Az Eurojust testületének elnöke az Eurojust tevékenységéről szóló éves jelentést nyújt be a Tanácsnak, amelyet az továbbít az EP számára. |

A működő, és a végrehajtási vagy mérlegelési szakaszban eszközök áttekintése táblázatos formában

| Eszköz | Előzmények | Cél(ok) | Szerkezet | Az érintett személyes adatok köre | Az adatokhoz való hozzáférés | Adatvédelem | Adatmegőrzés | A végrehajtás állapota | Felülvizsgálat |
|---------------------------------------------------------------------------------------------------|----------------------------|-----------------------------------------------------------------------------------------------|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| PNR-megállapodások az Egyesült Államokkal és Ausztráliával; API/PNR megállapodás Kanadával | A Bizottság kezdeményezte. | A terrorizmus és a súlyos transznacionális bűnözés egyéb formáinak megelőzésére és leküzdése. | Nemzetközi megállapodások. | Az Egyesült Államokkal és Ausztráliával kötött megállapodások 19 PNR-adatkategóriára, köztük születési, foglalási, fizetési és kiegészítő információkra terjednek ki; a Kanadával kötött megállapodás pedig 25 hasonló adatelemet tartalmaz. | Az Egyesült Államok Belbiztonsági Minisztériuma, a Kanadai Határügynökség és az Ausztrál Vám- és Államvédelmi Szolgálat, amelyek megosztják az adatokat belföldi bűnüldöző és terrorelhárító szolgálatokkal. | Az adatvédelmi szabályokat az adott nemzetközi megállapodások tartalmazzák. | Egyesült Államok: hét év aktív, nyolc év passzív használat; Ausztrália: 3,5 év aktív, két év passzív használat; Kanada: 72 óra aktív, 3,5 év passzív használat. | Az Egyesült Államokkal és az Ausztráliával kötött megállapodás átmenetileg alkalmazandó; a kanadai hatályos. A Bizottság újra fogja tárgyalni e megállapodásokat. Hat uniós tagállam a PNR-adatok bűnüldözési célú felhasználását lehetővé tevő jogszabályokat fogadott el. | Mindegyik megállapodás rendszeres felülvizsgálatot ír elő, a Kanadával és Ausztráliával kötött megállapodások pedig felmondási záradékot is tartalmaznak. |

A működő, és a végrehajtott vagy mérlegelési szakaszban eszközök áttekintése táblázatos formában

| Eszköz | Előzmények | Cél(ok) | Szerkezet | Az érintett személyes adatok köre | Az adatokhoz való hozzáférés | Adatvédelem | Adatmegőrzés | A végrehajtás állapota | Felülvizsgálat |
|---------------------------------|----------------------------|-------------------------------------------------------------------------------------------------------|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| EU-USA TFTP-megállapodás | A Bizottság kezdeményezte. | A terrorizmus és az azt finanszírozó tevékenység megelőzése, felderítése, kivizsgálása vagy üldözése. | Nemzetközi megállapodás. | Pénzügyi üzenetadatok, amelyek többek között tartalmazzák a pénzügyi tranzakciók megbízójának és jogosultjainak nevét, számlaszámát, címét és azonosító számát. | Az Egyesült Államok Pénzügyminisztériuma megoszthatja a pénzügyi üzenetekből lehívott személyes adatokat az egyesült államokbeli bűnüldöző, közbiztonsági vagy terrorelhárító hatóságokkal, az EU tagállamokkal, az Eurojusttal. A harmadik országokba történő továbbítás az EU tagállamok hozzájárulásával lehetséges. | A megállapodás a cél korlátozására és az arányosságra vonatkozó szigorú rendelkezéseket tartalmaz. | A pénzügyi üzenetekből lehívott személyes adatok nem őrizhetők meg tovább, mint ami a konkrét nyomozás vagy büntetőeljárás lefolytatásához szükséges; a le nem hívott adatok legfeljebb 5 évig őrizhetők meg. | Az Európai Parlament 2010. július 8-án megadta az egyetértését e megállapodás megkötéséhez. A Tanács most várhatóan elfogadja az e megállapodás megkötéséről szóló tanácsi határozatot, ezt követően pedig a megállapodás a két fél közötti levélváltás útján lép hatályba. | A Bizottságnak hat hónappal a hatályba lépést követően felül kell vizsgálnia a megállapodást. Értékelő jelentését meg kell küldenie a Tanácsnak és az EP-nek. |