Stanovisko evropského inspektora ochrany údajů ke sdělení Komise Evropskému parlamentu a Radě o prostoru svobody, bezpečnosti a práva ve službách občanům

(2009/C 276/02)

EVROPSKÝ INSPEKTOR OCHRANY ÚDAJŮ,

s ohledem na Smlouvu o založení Evropského společenství, a zejména na článek 286 této smlouvy,

s ohledem na Listinu základních práv Evropské unie, a zejména na článek 8 této listiny,

s ohledem na směrnici Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů,

s ohledem na nařízení Evropského parlamentu a Rady (ES) č. 45/2001 ze dne 18. prosince 2000 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů, a zejména na článek 41 tohoto nařízení,

PŘIJAL TOTO STANOVISKO:

I. ÚVOD

1. Dne 10. června 2009 přijala Komise sdělení Evropskému parlamentu a Radě o prostoru svobody, bezpečnosti a práva ve službách občanům ([1]). V souladu s článkem 41 nařízení (ES) č. 45/2001 předkládá evropský inspektor ochrany údajů (EIOÚ) své stanovisko.

2. Komise před přijetím sdělení neformálně konzultovala EIOÚ dopisem ze dne 19. května 2009. EIOÚ na tuto konzultaci odpověděl dne 20. května 2009 zasláním neformálních připomínek, jejichž cílem bylo dále zlepšit znění sdělení. Navíc EIOÚ aktivně přispěl k dopisu Pracovní skupiny pro policii a spravedlnost ze dne 14. ledna 2009 o víceletém programu pro oblast svobody, bezpečnosti a práva ([2]).

3. Sdělení (bod 1) zdůrazňuje, že Unie „potřebuje nový víceletý program, který staví na dosud dosaženém pokroku a čerpá poučení ze současných slabých stránek, aby mohl kladně ovlivnit budoucnost. Tento nový program by měl stanovit priority na příštích pět let“. Tento víceletý program (již známý jako „Stockholmský program“) bude navazovat na Tamperský program a Haagský program, které daly silný politický impuls prostoru svobody, bezpečnosti a práva.

4. Sdělení má být základem k tomuto novému víceletému programu. EIOÚ bere v této souvislosti na vědomí, že přestože víceleté programy nejsou samy o sobě závaznými nástroji, mají výrazný dopad na politiku, kterou orgány budou v dotčené oblasti rozvíjet, jelikož mnoho konkrétních legislativních a nelegislativních opatření bude z daného programu vyplývat.

5. Sdělení je tedy třeba vnímat v této souvislosti. Představuje další krok v debatě, která víceméně započala dvěma zprávami předloženými v červnu roku 2008 tzv. „skupinami pro budoucnost“ zřízenými předsednictvím Rady s cílem poskytnout myšlenky týkající se témat: Svoboda, bezpečnost, soukromí – evropské vnitřní věci v otevřeném světě ([3]) a „Navrhovaná řešení pro budoucí program EU v oblasti justice“ ([4]).

II. HLAVNÍ OBSAH STANOVISKA

6. Stávající stanovisko neposkytuje pouze reakci na sdělení, ale je též příspěvkem EIOÚ k obecnější debatě o budoucnosti prostoru svobody, bezpečnosti a práva, která musí vyústit v nový strategický pracovní program (Stockholmský program), jak oznámilo švédské předsednictví EU ([5]). Toto stanovisko se bude též zabývat určitými důsledky možného vstupu Lisabonské smlouvy v platnost.

7. Po popisu hlavních hledisek stanoviska v části III se budeme zabývat obecným posouzením sdělení v části IV.

8. Část V se zabývá otázkou, jak reagovat na potřebu trvalého respektu ochrany soukromí a osobních údajů v souvislosti s rostoucí výměnou osobních údajů. Zaměříme se na bod 2.3 sdělení o ochraně osobních údajů a soukromí a obecněji na potřeby další legislativních a nelegislativních opatření za účelem zlepšení rámce pro ochranu údajů.

([1]) KOM(2009) 262 v konečném znění (dále jen „sdělení“).

([2]) Nezveřejněn. Pracovní skupina pro policii a spravedlnost byla zřízena evropskou konferencí komisařů pro ochranu údajů, aby připravovala její postoje v oblasti vynucování práva a jednala jejím jménem v naléhavých záležitostech.

([3]) Dokument Rady č. 11657/08. Dále jen „zpráva o vnitřních věcech“.

([4]) Dokument Rady č. 11549/08 („zpráva o justici“).

([5]) Pracovní program vlády pro předsednictví v EU, http://www.regeringen.se

9. Část VI se zabývá potřebami a možnostmi uchovávání informací, přístupu k informacím a jejich výměny jakožto nástrojů pro vynucování práva, či jak je řečeno ve sdělení, pro „Evropu jako ochránce“. Bod 4 sdělení obsahuje několik cílů týkajících se toku informací a technologických nástrojů, zejména v bodech 4.1.2 (Umění zacházet s informacemi), 4.1.3 (Mobilizovat potřebné technologické nástroje) a 4.2.3.2 (Informační systémy). Vytvoření evropského informačního modelu (v bodu 4.1.2) je možné vnímat jako nejambicióznější návrh v této souvislosti. Stanovisko EIOÚ tento návrh podrobně analyzuje.

10. Část VII se krátce dotýká zvláštního tématu v rámci prostoru svobody, bezpečnosti a práva, který souvisí s ochranou údajů, a to konkrétně přístupu ke spravedlnosti a e-justici.

III. **HLEDISKA V TOMTO STANOVISKU**

11. Toto stanovisko pojímá potřebu ochrany základních práv jako hlavní hledisko pro analýzu sdělení a obecněji pro budoucnost prostoru svobody, bezpečnosti a práva v podobě dané novým víceletým programem. Dále bude stavět na příspěvcích EIOÚ k rozvoji politiky EU v této oblasti, zejména na jeho konzultativní roli. Doposud EIOÚ přijal více než třicet stanovisek a připomínek k iniciativám vyplývajícím z Haagského programu, které lze všechny nalézt na webových stránkách EIOÚ.

12. Ve svém hodnocení sdělení se EIOÚ bude zabývat zejména následujícími čtyřmi hledisky, která jsou důležitá pro budoucnost prostoru svobody, bezpečnosti a práva. Všechna tato hlediska hrají klíčovou roli i ve sdělení.

13. První hledisko je exponenciální nárůst počtu digitálních informací o občanech jako důsledek rozvíjejících se informačních a komunikačních technologií ([6]). Společnost se posouvá směrem k modelu, často nazývanému „společností dohledu“, kde je nanejvýš pravděpodobné, že každá transakce a téměř každý pohyb občanů zanechá digitální záznam. Tzv. „internet věcí“ a „inteligentní prostředí“ se již rychle rozvíjejí prostřednictvím používání štítků RFID. Stále častěji jsou používány digitalizované vlastnosti lidského těla (biometrie). Toto vede k stále propojenějšímu světu, ve kterém mají organizace zajišťující veřejnou bezpečnost přístup k rozsáhlému množství potenciálně užitečných informací, které mohou přímo ovlivnit život dotčených osob.

14. Druhé hledisko je internacionalizace. Na jedné straně v době digitálního věku není výměna údajů vázána vnějšími hranicemi Evropské unie, ale na druhé straně existuje zvýšená potřeba mezinárodní spolupráce v celé řadě činností EU, pokud jde o prostor svobody, bezpečnosti a práva: boj proti terorismu, policejní a soudní spolupráce, občanské soudnictví a hraniční kontroly jsou jen některými z příkladů.

15. Třetí hledisko je použití údajů pro účely vynucování práva: hrozby pro společnost z poslední doby, v souvislosti s terorismem nebo jiné, vedly pro donucovací orgány k více možnostem (k potřebě více možností) ke shromažďování, uchovávání a výměně osobních údajů. V mnoha případech se zapojily soukromé strany, jak mimo jiné ukazuje směrnice o uchovávání údajů ([7]) a různé nástroje týkající se údajů jmenné evidence cestujících (PNR) ([8]).

16. Čtvrtým hlediskem je volný pohyb. Postupný rozvoj prostoru svobody, bezpečnosti a práva vyžaduje další odstranění vnitřních hranic a možných překážek volného pohybu v rámci prostoru. Nové nástroje v této oblasti by v žádném případě neměly hranice obnovovat. Volný pohyb zahrnuje v tomto kontextu na jedné straně volný pohyb osob a na druhé straně volný pohyb (osobních) údajů.

17. Tato čtyři hlediska ukazují, že kontext, ve kterém jsou informace používány, se rychle mění. V tomto kontextu není pochyb o významu silného mechanismu na ochranu základních práv občanů a zejména na ochranu soukromí a údajů. Z těchto důvodů proto EIOÚ volí potřebu ochrany jako hlavní hledisko pro tuto analýzu, jak je zmíněno v bodě 11.

([6]) Zpráva o vnitřních věcech hovoří v této souvislosti dokonce o „digitálním cunami“.

([7]) Směrnice Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES, Úř. věst. L 105, 13.4.2006, s. 54.

([8]) Viz např. Dohoda mezi Evropskou unií a Spojenými státy americkými o zpracovávání údajů jmenné evidence cestujících (PNR) leteckými dopravci a o jejich předávání Ministerstvu vnitřní bezpečnosti Spojených států amerických (dohoda PNR 2007), Úř. věst. L 204, 4.8.2007, s. 18 a návrh rámcového rozhodnutí Rady o používání jmenné evidence cestujících pro účely vynucování práva, KOM (2007) 654 v konečném znění.

IV. **OBECNÉ POSOUZENÍ**

18. Sdělení a Stockholmský program mají za cíl stanovit záměry EU pro příštích pět let s účinky, jež se mohou projevit i později. EIOÚ bere na vědomí, že sdělení je napsáno tzv. „neutrálním způsobem ve vztahu k Lisabonu". EIOÚ plně chápe, proč Komise zaujala tento přístup, ale lituje též, že sdělení nemohlo plně těžit z dalších možností, které nabízí Lisabonská smlouva. Hledisku Lisabonské smlouvy bude v tomto sdělení věnována větší pozornost.

19. Sdělení staví na výsledcích činností EU v prostoru svobody, bezpečnosti a práva v posledních letech. Tyto výsledky je možné charakterizovat jako podmíněné událostmi, s důrazem na opatření rozšiřující pravomoci donucovacích orgánů a narušující soukromí občanů. Toto jistě platí v oblastech, kde jsou osobní údaje intenzivně využívány a vyměňovány, a které jsou tedy zásadní, pokud jde o ochranu údajů. Výsledky jsou podmíněny událostmi, neboť vnější události jako 11. září a bombové útoky v Madridu a Londýně daly silný impuls k legislativní činnosti. Například předávání údajů o cestujících Spojeným státům americkým lze chápat jako důsledek 11. září ([9]), zatímco bombové útoky v Londýně vedly ke směrnici o uchovávání údajů ([10]). Byla zdůrazněna opatření více narušující soukromí, neboť se zákonodárce EU zaměřil na opatření, která umožňují použití údajů a jejich výměnu, zatímco opatření, která mají za cíl zaručit ochranu osobních údajů, byla projednávána s menší naléhavostí. Hlavním ochranným opatřením, které bylo přijato po tříletých jednáních v Radě, bylo rámcové rozhodnutí Rady 2008/977/SVV o ochraně osobních údajů zpracovávaných v rámci policejní a justiční spolupráce v trestních věcech ([11]). Výsledkem bylo rámcové rozhodnutí Rady, které není plně uspokojivé (viz. body 29 až 30).

20. Zkušenosti z posledních let ukazují, že je třeba posuzovat důsledky pro donucovací orgány a evropské občany před přijetím nových nástrojů. Takové posouzení by mělo řádně vzít v úvahu dopady na soukromí a účinnost v případě vynucování práva – v první řadě, když jsou nové nástroje navrhovány a projednávány, ale také poté, co jsou tyto nástroje zavedeny – prostřednictvím pravidelného přezkumu. Takové posouzení je též nezbytné před tím, než nový víceletý program stanoví hlavní iniciativy pro blízkou budoucnost.

21. EIOÚ těší, že sdělení uznává ochranu základních práv a zejména ochranu osobních údajů za jednu z klíčových otázek v budoucnosti prostoru svobody, bezpečnosti a práva. Bod 2 sdělení popisuje EU jako jedinečný prostor, pokud jde o ochranu základních práv, založený na společných hodnotách. Je též pozitivní, že přistoupení k Evropské úmluvě o ochraně lidských práv je zmíněno jako prioritní otázka – dokonce první prioritní otázka sdělení. Přistoupení je důležitým krokem vpřed při zajišťování harmonického a soudržného systému pro ochranu lidských práv. Kromě toho zaujímá ve sdělení přední místo ochrana údajů.

22. Toto zaměření sdělení ukazuje na pevný úmysl zajistit ochranu práv občanů, a zaujmout tak vyváženější přístup. Vlády potřebují vhodné nástroje k zajištění bezpečnosti občanů, ale v evropské společnosti musejí plně respektovat základní práva občanů. Služba občanům ([12]) vyžaduje po Evropské unii, aby tuto rovnováhu chránila.

23. Z hlediska EIOÚ bere sdělení potřebu této rovnováhy velice dobře v úvahu, včetně potřeby ochrany osobních údajů. Uznává potřebu změny toho, na co je kladen důraz. To je velice důležité, neboť politiky v oblasti prostoru svobody, bezpečnosti a práva by neměly podporovat postupný přesun ke společnosti dohledu. EIOÚ očekává, že Rada zaujme stejný přístup ve Stockholmském programu, a to rovněž uznáním pokynů v bodě 25 níže.

24. Je to o to víc důležité, jelikož prostor svobody, bezpečnosti a práva je oblastí, která „utváří životní podmínky občanů, zejména osobní prostor jejich vlastní odpovědnosti a osobního a společenského bezpečí, který je chráněn základními právy", jak nedávno zdůraznil německý ústavní soud ve svém rozhodnutí ze dne 30. června 2009 týkajícím se Lisabonské smlouvy ([13]).

([9]) Dohoda PNR z roku 2007 zmíněná v předešlé poznámce pod čarou a předcházející dohody.

([10]) Směrnice Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES, Úř. věst. L 105, 13.4.2006, s. 54. Ačkoli je právním základem článek 95 Smlouvy o ES, jednalo se o okamžitou reakci na bombové útoky v Londýně.

([11]) Rámcové rozhodnutí Rady 2008/977/SVV ze dne 27. listopadu 2008 o ochraně osobních údajů zpracovávaných v rámci policejní a justiční spolupráce v trestních věcech, Úř. věst. L 350, 30.12.2008, s. 60.

([12]) Viz název sdělení.

([13]) Tisková zpráva č. 72/2009 ze dne 30. června 2009 německého federálního ústavního soudu, odstavec 2 c).

25. EIOÚ zdůrazňuje, že v tomto prostoru:

— By údaje měly být vyměňovány mezi úřady členských států včetně příslušných evropských subjektů či databází na základě odpovídajícího a účinného mechanismu, který plně respektuje základní práva občanů a zajišťuje vzájemnou důvěru.

— To vyžaduje nejen dostupnost informací spojenou se vzájemným uznáváním právních systémů členských států (a EU), ale též harmonizaci norem na ochranu informací, například prostřednictvím společného rámce ochrany údajů, avšak nejen jeho prostřednictvím.

— Tyto společné normy by neměly být použitelné pouze v situacích s přeshraničním rozměrem. Vzájemná důvěra může existovat pouze, pokud jsou normy pevné a pokud jsou vždy respektovány bez rizika, že nebudou použity, jakmile není či přestane být patrný přeshraniční rozměr. Kromě toho rozdíly mezi „vnitřními" a „přeshraničními" údaji nemohou fungovat v praxi, zejména pokud jde o využití údajů ([14]).

V. NÁSTROJE PRO OCHRANU ÚDAJŮ

V.1 Na cestě k úplnému režimu ochrany údajů

26. EIOÚ schvaluje strategický přístup, kdy je ve sdělení ochraně údajů přiděleno přední místo. Mnoho iniciativ v prostoru svobody, bezpečnosti a práva vskutku závisí na použití osobních údajů, a kvalitní ochrana údajů je proto zásadní pro jejich úspěch. Respektování soukromí a ochrana údajů nejsou jen právními povinnostmi, jež jsou stále více uznávány na úrovni EU, ale představují též zásadní otázku pro evropské občany, jak ukazují výsledky Eurobarometru ([15]). Navíc je omezení přístupu k osobním údajům zásadní též pro zajištění důvěry donucovacích orgánů.

27. Bod 2.3 sdělení stanoví, že je nutný úplný režim ochrany údajů, který zahrne všechny oblasti pravomocí Unie ([16]). EIOÚ plně podporuje tento cíl, nezávisle na vstupu Lisabonské smlouvy v platnost. Bere též na vědomí, že takový režim nutně neznamená jeden právní rámec použitelný na veškerá zpracování. Podle současných smluv jsou možnosti přijetí jednoho, soudržného právního rámce, který by se uplatnil na všechna zpracování, omezené kvůli struktuře pilířů a kvůli skutečnosti, že – alespoň pokud jde o první pilíř, má ochrana údajů zpracovávaných evropskými orgány oddělený právní základ (článek 286 Smlouvy o ES). Avšak EIOÚ poukazuje na skutečnost, že některá zlepšení mohou být provedena tím, že se plně využijí možnosti nabízené stávajícími smlouvami, jak již bylo zdůrazněno Komisí ve sdělení „Provádění Haagského programu: cesta vpřed" ([17]). Po vstupu Lisabonské smlouvy v platnost poskytne článek 16 Smlouvy o fungování EU nezbytný právní základ pro soudržný právní rámec, který bude použitelný pro všechna zpracování.

28. EIOÚ konstatuje, že to je v každém případě zásadní pro zajištění soudržnosti právního rámce ochrany údajů tam, kde je to nutné, prostřednictvím harmonizace a konsolidace různých právních nástrojů použitelných v prostoru svobody, bezpečnosti a práva.

Podle stávajících smluv

29. V nedávné době byl učiněn první krok prostřednictvím přijetí rámcového rozhodnutí Rady 2008/977/SVV ([18]). Avšak tento právní nástroj nelze charakterizovat jako soudržný rámec v zásadě proto, že jeho ustanovení nejsou obecně účinná. Neuplatňují se na vnitřní situace, kdy osobní údaje pocházejí z členského státu, který je používá. Takové omezení nutně sníží přidanou hodnotu rámcového rozhodnutí Rady, ledaže by všechny členské státy rozhodly zahrnout vnitřní situace do vnitrostátních prováděcích předpisů, což není pravděpodobné.

30. Druhý důvod, proč EIOÚ je toho názoru, že z dlouhodobého hlediska neobsahuje rámcové rozhodnutí Rady 2008/977/SVV uspokojivý rámec pro ochranu údajů v prostoru svobody, bezpečnosti a práva, spočívá v tom, že několik zásadních ustanovení není v souladu se směrnicí 95/46/ES. Na základě stávajících smluv by mohlo být druhým krokem rozšíření oblasti působnosti rámcového rozhodnutí Rady a jeho přizpůsobení směrnici 95/46/ES.

31. Další impuls k vytvoření úplného režimu ochrany údajů by mohl být dán stanovením jasné a dlouhodobé vize. Tato vize by mohla zahrnovat globální a soudržný přístup

([14]) EIOÚ vysvětlil tento poslední bod ve stanovisku ze dne 19. prosince 2005 k návrhu rámcového rozhodnutí Rady o ochraně osobních údajů zpracovávaných v rámci policejní a soudní spolupráce v trestních věcech (KOM(2005) 475 v konečném znění), Úř. věst. C 47, 25.2.2006, s. 27, odstavce 30 až 32.

([15]) Ochrana údajů v Evropské unii – průzkum názorů občanů – analytická zpráva, Flash Eurobarometer Series 225, leden 2008, http://www.ec.europa.eu/public_opinion/flash/fl_225_en.pdf

([16]) Viz též prioritní otázky sdělení.

([17]) KOM(2006) 331 v konečném znění ze dne 28. června 2006.

([18]) Viz poznámka pod čarou 11.

k definici sběru a výměny údajů, jakož i využívání stávajících databází, a také záruky ochrany údajů. Tato vize by měla zabránit zbytečnému překrývání a duplikaci nástrojů (a tedy i zpracování osobních údajů). Měla by též posílit soulad politik EU v této oblasti, jakož i důvěru v to, jak veřejné orgány nakládají s údaji občanů. EIOÚ doporučuje Radě, aby vyjádřila potřebu jasné a dlouhodobé vize ve Stockholmském programu.

32. EIOÚ dále doporučuje zhodnotit a zohlednit opatření, která již byla v této oblasti přijata, jejich konkrétní provádění a jejich účinnost. Toto hodnocení by mělo řádně zohlednit dopady na soukromí a účinnost, pokud jde o vynucování práva; pokud by tato hodnocení ukázala, že určitá opatření nepřinášejí plánované výsledky, nebo že nejsou přiměřená sledovaným cílům, měly by být zváženy následující kroky:

— jako první krok – změna či zrušení opatření, pokud se zdá, že je nelze dostatečně odůvodnit jako mající konkrétní přínos pro donucovací orgány a evropské občany,

— jako druhý krok posouzení možností zlepšení uplatňování stávajících opatření,

— teprve jako třetí krok navržení nových legislativních opatření, pokud je pravděpodobné, že nová opatření jsou nutná k dosažení zamýšlených cílů. Nové nástroje by měly být přijaty pouze, pokud mají jasný a konkrétní přínos pro donucovací orgány a evropské občany.

EIOÚ doporučuje uvést systém hodnocení stávajících opatření ve Stockholmském programu.

33. V neposlední řadě je nutné klást zvláštní důraz na lepší provádění stávajících záruk, v souladu se sdělením Komise o pokračování pracovního programu pro lepší provádění směrnice o ochraně osobních údajů ([19]) a doporučeními, která učinil EIOÚ ve stanovisku k tomuto sdělení ([20]). Komise ve třetím pilíři bohužel nemá možnost zahájit řízení o porušení Smlouvy.

Podle Lisabonské smlouvy

34. Lisabonská smlouva otevírá možnost pro skutečně soudržný rámec ochrany údajů. Článek 16 odst. 2 Smlouvy o fungování Evropské unie vyžaduje, aby Rada a Evropský parlament přijaly pravidla pro ochranu údajů orgány, institucemi a jinými subjekty Unie a členskými státy, pokud vykonávají činnosti spadající do oblasti působnosti práva Unie, a soukromými stranami.

35. EIOÚ chápe důraz, který sdělení klade na úplný režim ochrany údajů, jakožto snahu Komise navrhnout právní rámec, který se použije na všechny činnosti zpracování. Tuto snahu, která zlepší soulad systému, zajistí právní jistotu, a tak zlepší ochranu, plně schvaluje. Zejména by se tak zabránilo budoucím obtížím při hledání dělící čáry mezi pilíři, když jsou data shromážděná v soukromém sektoru pro obchodní účely později používána pro účely vynucování práva. Tato dělící čára mezi pilíři neodráží dostatečně skutečnost, jak potvrdila významná rozhodnutí Evropského soudního dvora o PNR ([21]) a o uchovávání údajů ([22]).

36. EIOÚ navrhuje zdůraznit toto odůvodnění úplného režimu ochrany údajů ve Stockholmském programu. Ukazuje, že takový režim není pouze prostou preferenční volbou, ale vzhledem k měnícím se postupům při používání údajů nezbytností. Doporučuje zařadit do Stockholmského programu jako prioritu potřebu nového legislativního rámce, který by mj. nahradil rámcové rozhodnutí Rady 2008/977/SVV.

37. EIOÚ zdůrazňuje, že pojem úplného režimu ochrany údajů je založený na obecném právním rámci, který nevylučuje přijetí dodatečných pravidel pro ochranu údajů v oblasti policie a justice. Taková dodatečná pravidla by mohla zohlednit specifické potřeby v oblasti vynucování práva, jak předpokládá prohlášení 21 připojené k Lisabonské smlouvě ([23]).

V.2 **Nová formulace zásad ochrany údajů**

38. Sdělení zmiňuje, že technologické změny mění způsoby komunikace mezi lidmi a veřejnými a soukromými organizacemi. Podle Komise to vyžaduje přeformulování některých základních zásad ochrany údajů.

([19]) KOM(2007) 87 v konečném znění ze dne 7. března 2007.

([20]) Stanovisko ze dne 25. července 2007, Úř. věst. C 255, 27.10.2007, s. 1, zejména bod 30.

([21]) Rozsudek Soudního dvora ze dne 30. května 2006, Evropský parlament v. Rada Evropské unie (C-317/04) a Komise Evropských společenství (C-318/04), spojené věci C-317/04 a C-318/04, Sb. rozh. [2006], s. I-4721.

([22]) Rozhodnutí Soudu ze dne 10. února 2009, Irsko v. Evropský parlament a Rada, věc C-301/06, dosud nepublikováno.

([23]) Viz. prohlášení 21 o ochraně osobních údajů v oblasti justiční spolupráce v trestních věcech a policejní spolupráce, připojené k závěrečnému aktu mezivládní konference, která přijala Lisabonskou smlouvu, Úř. věst. C 115, 9.5.2008, s. 345.

39. EIOÚ tento záměr Komise vítá. Hodnocení účinnosti těchto zásad v kontextu technologických změn je nesmírně užitečné. V první řadě je důležité si uvědomit, že přeformulování a opětovné potvrzení zásad ochrany údajů nemusí být vždy přímo spojeno s technologickým rozvojem. Může to být také nutné s ohledem na ostatní hlediska zmíněná v části III výše, internacionalizaci, častějšímu používání údajů pro účely vynucování práva a volný pohyb.

40. Navíc může být z pohledu EIOÚ toto hodnocení zahrnuto do veřejné konzultace, jejíž uspořádání Komise oznámila na konferenci „Osobní údaje – širší použití, větší ochrana?“ konané ve dnech 19. a 20. května 2009. Tato veřejná konzultace by mohla poskytnout hodnotný vstup ([24]). EIOÚ navrhuje, aby Rada ve znění Stockholmského programu a Komise ve svých veřejných prohlášeních o konzultaci zdůraznily spojitost mezi záměry sdělení v bodě 2.3 a veřejnou konzultací o budoucnosti ochrany údajů.

41. Jako příklad toho, co takové hodnocení může zahrnovat, lze uvést následující body:

— Osobní údaje v rámci prostoru svobody, bezpečnosti a práva mohou být obzvláště citlivé povahy, jako např. údaje týkající se odsouzení ze trestný čin, policejní údaje a biometrické údaje, jako např. otisky prstů a profily DNA.

— Jejich zpracování může znamenat negativní důsledky pro subjekty údajů, zejména pokud vezmeme v úvahu donucovací pravomoci donucovacích orgánů. Navíc jsou sledování údajů a jejich analýza stále více automatické, poměrně často bez lidského zásahu. Technologie umožňuje použití databází s osobními údaji pro obecné vyhledávání (vytěžování dat – data mining, profilování atd.). Právní povinnosti, na kterých je zpracování údajů založeno, by měly být jasně stanoveny.

— Základem práva na ochranu údajů je, že osobní údaje jsou shromažďovány pro stanovené účely a nejsou používány způsobem neslučitelným s těmito účely. Použití pro neslučitelné účely by mělo být povoleno pouze tehdy, pokud je stanoveno právními předpisy a je nezbytné k dosažení konkrétního veřejného zájmu, jako např. účely uvedené v čl. 8 odst. 2 Evropské úmluvy o lidských právech.

— Potřeba respektovat zásadu omezení účelu by mohla mít důsledky pro současné trendy v použití údajů. Při vynucování práva se využívá údajů, které byly shromážděny soukromými společnostmi pro obchodní účely, v oblasti telekomunikací, dopravy a ve finančním sektoru. Navíc jsou vytvářeny informační systémy velkého rozsahu, např. v oblastech přistěhovalectví a hraničních kontrol. Kromě toho je možné propojení a přístup do databází, což rozšiřuje účely, pro které byly osobní údaje původně shromážděny. Je potřeba zamyslet se nad těmito současnými trendy, včetně případných možných úprav anebo dodatečných záruk.

— Vedle zásad ochrany údajů uvedených ve sdělení by hodnocení mělo věnovat pozornost potřebě transparentnosti zpracování, která by subjektům údajů umožnila výkon jejich práv. Transparentnost je zvláště obtížnou otázkou v oblasti vynucování práva, zejména proto, že by transparentnost měla být posuzována s ohledem na riziko pro vyšetřování.

— Měla by být nalezena řešení pro výměny se třetími zeměmi.

42. Toto hodnocení by se mělo dále zaměřit na možnosti zlepšení účinnosti použití zásad ochrany údajů. V této souvislosti by mohlo být užitečné soustředit se na nástroje, které mohou posílit odpovědnost správců údajů. Tyto nástroje musí umožnit plnou odpovědnost správců údajů za zacházení s údaji. „Řádná správa údajů“ je v této souvislosti užitečným pojmem. Zahrnuje právní, technické a organizační prostředky, kterými organizace zajišťují plnou odpovědnost za způsob, jakým se s údaji zachází, jako např. plánování a kontrolu, použití náležité technologie, odpovídající školení personálu, audity ověřující dodržování předpisů, atd.

V.3 **Technologie respektující soukromí**

43. EIOÚ oceňuje, že bod 2.3 sdělení zmiňuje certifikaci technologií respektujících soukromí. Navíc by bylo možné odkázat na „soukromí coby aspekt návrhu“ a potřebu stanovit „nejlepší dostupné techniky“, které jsou v souladu s rámcem ochrany údajů v EU.

44. Z pohledu EIOÚ by „soukromí coby aspekt návrhu“ a technologie respektující soukromí mohly být užitečnými nástroji pro lepší ochranu, jakož i pro účinnější použití informací. EIOÚ navrhuje dva – vzájemně se nevylučující – postupy:

— Režim pro certifikaci ochrany soukromí a údajů ([25]) jako možnost pro tvůrce a uživatele informačních systémů, ať jsou podporovány z fondů EU nebo právními předpisy EU či nikoliv.

([24]) Pracovní skupina pro ochranu údajů zřízená podle článku 29, jejíž je EIOÚ součástí, se rozhodla intenzivně pracovat na příspěvku k této veřejné konzultaci.

([25]) Příkladem takového režimu je evropský systém osvědčení o ochraně soukromí (EuroPriSe).

— Právní povinnost pro tvůrce a uživatele informačních systémů používat systémy, které jsou v souladu se zásadou „soukromí coby aspekt návrhu“. To by mohlo vyžadovat rozšíření stávající oblasti působnosti práva na ochranu údajů, aby se tvůrci stali odpovědnými za informační systémy, které vytvářejí ([26]).

EIOÚ navrhuje zmínit tyto možné postupy ve Stockholmském programu.

V.4 **Vnější aspekty**

45. Dalším tématem, které sdělení zmiňuje je vytvoření a prosazování mezinárodních norem v oblasti ochrany údajů. V současnosti probíhá mnoho činností za účelem vytvoření rozumných norem pro globální uplatnění, např. mezinárodní konferencí komisařů pro ochranu soukromí a údajů. V blízké budoucnosti by na tomto základě mohla být uzavřena mezinárodní dohoda. EIOÚ navrhuje, aby Stockholmský program tyto činnosti podpořil.

46. Sdělení také zmiňuje uzavření dvoustranných dohod založených na pokroku, kterého již bylo dosaženo se Spojenými státy. EIOÚ sdílí potřebu jasného právního rámce týkajícího se předávání údajů do třetích zemí, a vítá tedy společnou práci orgánů EU a USA v kontaktní skupině na vysoké úrovni týkající se možného transatlantického nástroje ochrany údajů, přičemž vyzývá k větší jasnosti a k pozornosti věnované určitým otázkám ([27]). Z tohoto pohledu je též zajímavé vzít na vědomí záměry uvedené ve zprávě o vnitřních věcech ohledně evropsko-atlantské oblasti spolupráce, pokud jde o prostor svobody, bezpečnosti a práva, o kterém by podle této zprávy měla EU rozhodnout do roku 2014. Takový prostor by nebyl možný bez řádných záruk ohledně ochrany údajů.

47. Podle EIOÚ by evropské normy na ochranu údajů, založené na Úmluvě Rady Evropy č. 108 o ochraně osob se zřetelem na automatizované zpracovávání osobních údajů ([28]) a na judikatuře Evropského soudního dvora a Evropského soudu pro lidská práva, měly určovat úroveň ochrany v obecné dohodě se Spojenými státy o ochraně údajů a jejich výměně. Taková obecná dohoda by mohla být základem pro konkrétní ujednání o výměně osobních údajů. To je ještě důležitější s ohledem na záměr vyjádřený v bodě 4.2.1. sdělení, a to že Evropská unie musí uzavřít, pokud to bude nezbytné, dohody o policejní spolupráci.

48. EIOÚ plně rozumí potřebě rozšíření mezinárodní spolupráce, v některých případech též se zeměmi, které nechrání základní práva. Je však zásadní vzít v úvahu, že tato mezinárodní spolupráce pravděpodobně způsobí velký nárůst shromažďování a předávání údajů ([29]). Proto je nezbytně nutné, aby zásady spravedlivého a zákonného zpracování – jakož i zásady náležitého postupu obecně – platily pro shromažďování a předávání osobních údajů za hranicemi Unie a aby byly osobní údaje předávány třetím zemím nebo mezinárodním organizacím pouze, pokud tyto zúčastněné třetí strany zajistí odpovídající úroveň ochrany nebo jiné příslušné záruky.

49. Závěrem EIOÚ doporučuje ve Stockholmském programu zdůraznit důležitost obecných dohod se Spojenými státy a jinými třetími zeměmi o ochraně údajů a výměně údajů, vycházející z úrovně ochrany zaručené na území EU. V širší souvislosti EIOÚ poukazuje na význam aktivní podpory dodržování základních práv, zejména ochrany údajů, ve vztahu k třetím zemím a mezinárodním organizacím ([30]). Navíc by Stockholmský program mohl uvádět obecný názor, že výměna osobních údajů se třetími zeměmi vyžaduje odpovídající úroveň ochrany či jiné vhodné záruky v těchto třetích zemích.

VI. **POUŽITÍ INFORMACÍ**

VI.1 **Na cestě k evropskému informačnímu modelu**

50. Lepší výměna informací je v rámci prostoru svobody, bezpečnosti a práva pro Evropskou unii nezbytným politickým cílem. Bod 4.1.2 sdělení zdůrazňuje, že bezpečnost

([26]) Uživatelé informací jsou zahrnuti v právu na ochranu údajů, stejně jako správci či zpracovatelé.

([27]) Stanovisko EIOÚ ze dne 11. listopadu 2008 k závěrečné zprávě Kontaktní skupiny EU-USA na vysoké úrovni pro sdílení informací a ochranu soukromí a osobních údajů, Úř. věst. C 128, 6.6.2009, s. 1.

([28]) ETS č. 108, 28.1.1981.

([29]) Viz dopis EIOÚ ze dne 28. listopadu 2005 o sdělení Komise o vnějším rozměru oblasti svobody, bezpečnosti a práva dostupný na webových stránkách EIOÚ.

([30]) Nedávná judikatura týkající se seznamů teroristů potvrzuje, že záruky jsou potřebné – i ve vztahu k Organizaci spojených národů – s cílem zajistit, aby protiteroristická opatření byla v souladu s normami EU o základních právech (spojené věci C-402/05 P a C-415/05 P, Kadi a Al Barakaat Foundation v. Rada, rozhodnutí ze dne 3. září 2008, dosud nepublikováno).

v Evropské unii spočívá ve účinných mechanismech výměny informací mezi vnitrostátními orgány a evropskými subjekty. Tento důraz na výměnu informací je logický v situaci, kdy neexistuje evropská policie, evropské trestní soudnictví ani evropská hraniční kontrola. Opatření související s informacemi proto představují nezbytný příspěvek Evropské unie, který orgánům členských států umožňuje řešit přeshraniční trestnou činnost účinným způsobem a účinně chránit vnější hranice. Nepřispívají však pouze k bezpečnosti občanů, ale též k jejich svobodě – volný pohyb osob jakožto hledisko tohoto stanoviska byl uveden výše, a ke spravedlnosti.

51. Právě z těchto důvodů byla do Haagského programu zahrnuta zásada dostupnosti. Podle této zásady by informace potřebné pro boj proti trestné činnosti měly proudit přes vnitřní hranice EU bez překážek. Nedávné zkušenosti ukazují, že bylo obtížné provést tuto zásadu do legislativních opatření. Návrh rámcového rozhodnutí Rady o výměně informací podle zásady dostupnosti ze dne 12. října 2005 ([31]), vypracovaný Komisí, nebyl v Radě přijat. Členské státy nebyly připraveny přijmout důsledky zásady dostupnosti v plném rozsahu. Namísto toho byly přijaty omezenější nástroje ([32]), jako např. rozhodnutí Rady 2008/615/SVV ze dne 23. června 2008 o posílení přeshraniční spolupráce, zejména v boji proti terorismu a přeshraniční trestné činnosti („Prümské rozhodnutí“) ([33]).

52. Zatímco zásada dostupnosti byla ústředním tématem Haagského programu, zdá se, že Komise nyní zvolila skromnější přístup. Má v plánu dále povzbudit výměnu informací mezi orgány členských států zavedením evropského informačního modelu. Švédské předsednictví EU smýšlí stejným způsobem ([34]). Předloží návrh strategie pro výměnu informací. Rada již započala práci na ambiciózním projektu strategie Evropské unie pro správu informací, která úzce souvisí s evropským informačním modelem. EIOÚ bere tento vývoj na vědomí s velkým zájmem a zdůrazňuje, že by v těchto projektech měla být věnována pozornost prvkům týkajícím se ochrany údajů.

Evropský informační model a ochrana údajů

53. Jako výchozí bod by mělo být zdůrazněno, že budoucnost prostoru svobody, bezpečnosti a práva by neměla být řízena technologiemi v tom smyslu, že téměř neomezené možnosti, které nové technologie nabízejí, by měly být vždy prověřeny z hlediska příslušných zásad ochrany údajů a měly by být využívány jen potud, pokud jsou s těmito zásadami v souladu.

54. EIOÚ bere na vědomí, že sdělení představuje informační model, který není jen technickým modelem: schopnost výkonné strategické analýzy a lepší shromažďování a zpracovávání operačních informací. Uznává též, že by měly být zohledněny prvky spojené s politikou, jako např. kritéria shromažďování, sdílení a zpracování informací,a přitom by měly být dodrženy zásady ochrany údajů.

55. Informační technologie a právní podmínky jsou, a nadále budou, nezbytné. EIOÚ vítá, že sdělení vychází z předpokladu, že evropský informační model nelze chápat na základě technických aspektů. Je nezbytné, aby informace byly shromažďovány, sdíleny a zpracovávány pouze na základě konkrétních potřeb bezpečnosti, přičemž je třeba zohlednit zásady ochrany údajů. EIOÚ také plně souhlasí s potřebou stanovit mechanismus kontroly umožňující hodnotit fungování výměny informací. Navrhuje, aby Rada tyto prvky ve Stockholmském programu dále rozpracovala.

56. V této souvislosti EIOÚ zdůrazňuje, že ochrana údajů, jejímž cílem je ochrana občanů, by neměla být vnímána jako překážka účinné správy údajů. Poskytuje důležitý nástroj pro zlepšení uchovávání informací, přístupu k nim a jejich výměny. Práva subjektů údajů být informováni o tom, jaké informace o nich jsou zpracovávány, a právo na opravu nesprávných informací mohou též posílit přesnost údajů v systémech správy údajů.

57. Právo na ochranu údajů má v podstatě následující důsledky: pokud jsou údaje potřebné pro určitý legitimní účel, mohou být použity; pokud nejsou potřebné pro dobře definovaný účel, osobní údaje nemohou být použity. V prvním případě je možné, že budou potřebná další opatření, aby byly poskytnuty přiměřené záruky.

58. EIOÚ je však kritický k rozsahu, v jakém sdělení zmiňuje „identifikaci budoucích potřeb“ jakožto součásti informačního modelu. Zdůrazňuje, že i v budoucnu by se vytváření informačních systémů mělo řídit zásadou omezení účelu ([35]). Je jednou ze základních záruk, které systém ochrany údajů dává občanům: tito musí vědět předem, za jakým účelem jsou údaje, které se jich týkají, shromažďovány a že budou skutečně použity jen za tímto účelem, zejména v budoucnu. Tato záruka je zakotvena i v článku 8 Listiny základních práv Evropské unie. Zásada omezení účelu umožňuje výjimky, které jsou zvláště významné pro prostor svobody, bezpečnosti a práva, ale tyto výjimky by neměly určovat strukturu systému.

([31]) KOM(2005) 490 v konečném znění.

([32]) Z pohledu zásady dostupnosti obsahuje Prümské rozhodnutí rozsáhlá ustanovení o použití biometrických údajů (DNA a otisků prstů).

([33]) Úř. věst. L 210, 6.8.2008, s. 1.

([34]) Viz pracovní program vlády pro předsednictví v EU, zmíněn v poznámce pod čarou 5, s. 23.

([35]) Viz též bod 41 výše.

Volba správné architektury

59. Volba správné architektury pro výměnu informací je základem pro vše následující. Význam náležité informační architektury sdělení uznává (bod 4.1.3), ale bohužel pouze ve vztahu k interoperabilitě.

60. EIOÚ zdůrazňuje další prvek: v rámci evropského informačního modelu by požadavky na ochranu údajů měly být nedílnou součástí vytváření systému a neměly by být vnímány jen jako nezbytná podmínka zákonnosti systému ([36]). Měly by být využity koncepty „soukromí coby aspekt návrhu" a potřeba stanovit „nejlepší dostupné techniky" ([37]), jak je popsáno v bodě 43 výše. Evropský informační model by měl být založen na těchto konceptech. Konkrétněji to znamená, že by informační systémy, které jsou navrhovány za účelem veřejné bezpečnosti, měly být vždy vytvářeny v souladu se zásadou „soukromí coby aspekt návrhu." EIOÚ doporučuje Radě, aby tyto prvky zahrnula do Stockholmského programu.

Interoperabilita systémů

61. EIOÚ zdůrazňuje, že interoperabilita není pouze technickou otázkou, ale má též důsledky pro ochranu občanů, zejména ochranu údajů. Z hlediska ochrany údajů má interoperabilita systémů, pokud dobře funguje, výhody týkající se zamezení dvojího uchovávání. Je však zároveň jasné, že technická možnost přístupu k údajům nebo jejich výměny se v mnoha případech stává silným impulsem k faktickému přístupu k těmto údajům a jejich výměně. Jinými slovy interoperabilita představuje určitá rizika propojení databází mající odlišné účely ([38]). Může ovlivnit přísná omezení ohledně účelu databází.

62. Stručně řečeno pouhá skutečnost, že je technicky možné vyměňovat digitální informace mezi interoperabilními databázemi či tyto databáze sloučit, neodůvodňuje výjimku ze zásady omezení účelu. Interoperabilita by měla být v konkrétních případech založena na jasném a pečlivém politickém rozhodnutí. EIOÚ navrhuje, aby byl tento pojem upřesněn ve Stockholmském programu.

([36]) Viz „Pokyny a kritéria pro vytváření, zavádění a použití bezpečnostních technologií zlepšujících ochranu soukromí" vypracované v rámci projektu PRISE (http://www.prise.oeaw.ac.at).

([37]) Nejlepší dostupné techniky chápeme jako neúčinnější a nejpokročilejší fázi vývoje činností a jejich způsobů fungování, což znamená praktickou vhodnost určitých technik být v zásadě základem aplikací a systémů ITS, které musí být v souladu s požadavky právního rámce EU v oblasti soukromí, ochrany údajů a bezpečnosti.

([38]) Viz připomínky EIOÚ ke sdělení Komise o interoperabilitě evropských databází, 10. března 2006, dostupné na: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2006/06-03-10_Interoperability_EN.pdf

VI.2 **Použití informací shromážděných pro jiné účely**

63. Sdělení se výslovně nezabývá jednou z nejvýznamnějších tendencí nedávných let, a to použitím údajů shromážděných v soukromém sektoru pro obchodní účely k účelům vynucování práva. Tato tendence se netýká pouze provozních údajů o elektronických komunikací a údajů o cestujících, kteří se letecky dopravují do (určitých) třetích zemí ([39]), ale zaměřuje se též na finanční sektor. Příkladem je směrnice Evropského parlamentu a Rady 2005/60/ES ze dne 26. října 2005 o předcházení zneužití finančního systému k praní peněz a financování terorismu ([40]). Další dobře známý a velice diskutovaný příklad se týká zpracování osobních údajů Společností pro celosvětovou mezibankovní telekomunikaci (SWIFT) ([41]), a to údajů, které jsou nezbytné pro účely programu ministerstva financí USA pro sledování financování terorismu.

64. EIOÚ je toho názoru, že tyto tendence si ve Stockholmském programu vyžadují zvláštní pozornost. Lze je vnímat jako odchylky od zásady omezení účelu a často velice narušují soukromí, jelikož tyto údaje mohou vypovídat hodně o chování jednotlivců. V každém případě, kdy jsou taková opatření navržena, musí existovat velice přesvědčivé důkazy o tom, že jsou tato opatření narušující soukromí nutná. Pokud jsou takové důkazy poskytnuty, musí být zajištěno, že práva jednotlivců budou plně respektována.

65. Podle EIOÚ by použití osobních údajů shromážděných pro obchodní účely k účelům vynucování práva mělo být povoleno pouze za přísných podmínek, a to:

— Údaje jsou používány pouze pro konkrétně stanovené účely jako např. boj proti terorismu či závažná trestná činnost, což je třeba stanovit případ od případu.

— Údaje jsou předávány spíše na základě systému „tlaku" než „vytažení" ([42]).

([39]) Viz např. bod 15 výše.

([40]) Úř. věst. L 309, 25.11.2005, s. 15.

([41]) Viz stanovisko 10/2006 ke zpracovávání osobních údajů Společností pro celosvětovou mezibankovní komunikaci (SWIFT) vypracované Pracovní skupinou článku 29.

([42]) V rámci systému „tlaku" zašle správce údajů („tlačí") na žádost údaje donucovacímu orgánu. Na základě systému „vytažení" mají donucovací orgány přístup do databází správce a získávají („vytahují") údaje z této databáze. V rámci systému „tahu" je těžší, aby se správce přijal svou odpovědnost.

— Žádosti o údaje by měly být přiměřené, úzce zaměřené a v zásadě založené na podezřeních týkajících se konkrétních osob.

— Běžné vyhledávání, vytěžování dat a profilování by mělo být vyloučeno.

— Veškeré použití údajů pro účely vynucování práva by mělo být zaznamenáno s cílem umožnit účinnou kontrolu použití subjektem údajů, který vykonává svá práva, orgány pro ochranu údajů, a soudy.

VI.3 **Informační systémy a subjekty EU**

Informační systémy s centralizovaným uchováváním či bez něj ([43])

66. V rámci prostoru svobody, bezpečnosti a práva během posledních let výrazně vzrostl počet informačních systémů založených na právních předpisech EU. Někdy jsou přijata rozhodnutí zřídit systém, který zahrnuje centralizované uchovávání údajů na evropské úrovni, v jiných případech právo pouze předpokládá výměnu informací mezi vnitrostátními databázemi. Schengenský informační systém je pravděpodobně nejlepším příkladem systému s centralizovaným uchováváním. Rozhodnutí Rady 2008/615/SVV (Prümské rozhodnutí) ([44]) je z hlediska ochrany údajů nejdůležitějším příkladem systému bez centralizovaného uchovávání, neboť předpokládá masovou výměnu biometrických údajů mezi orgány v členských státech.

67. Sdělení ilustruje, že tato tendence vytváření nových systémů bude pokračovat. Prvním příkladem, převzatým z bodu 4.2.2, je informační systém rozšiřující Evropský informační systému rejstříků trestů (ECRIS) tak, aby zahrnoval státní příslušníky zemí EU, jež nejsou členy EU. Komise již objednala studii o evropském rejstříku odsouzených státních příslušníků třetích zemí (European Index for Convicted Third Country Nationals, EICTCN), s možným vznikem ústřední databáze. Druhým příkladem je výměna informací o jednotlivcích uvedených v insolvenčních rejstřících jiných členských států v rámci e-justice (bod 3.4.1 sdělení) bez centralizovaného uchovávání.

68. Decentralizovaný systém by mohl mít určité výhody z hlediska ochrany údajů. Zabraňuje dvojímu uchovávání údajů orgánem členského státu a v centralizovaném systému, odpovědnost za údaje je jasná, neboť orgán členského státu je správcem, a kontrolu soudy a orgány pro ochranu údajů lze vykonávat na úrovni členského státu. Ale tento systém má též slabiny, pokud jsou údaje vyměňovány s jinými jurisdikcemi, např. co se týče zajištění toho, aby informace byly aktualizovány jak v zemi původu, tak v zemi určení, a toho, jak zajistit účinnou kontrolu na obou stranách. Ještě složitější je zajistit odpovědnost za technický systém pro výměnu. Tyto slabiny mohou být překonány tím, že se zvolí ústřední systém s odpovědností evropských orgánů, alespoň za část systému (jako např. za technickou infrastrukturu).

69. V této souvislosti by bylo užitečné vytvořit věcná kritéria pro volbu mezi centralizovaným a decentralizovaným systémem, která by zajišťovala jasná a náležitá politická rozhodnutí v konkrétních případech. Tato kritéria mohou přispět k fungování systémů samých, jakož i k ochraně údajů občanů. EIOÚ navrhuje zařadit záměr vypracování takových kritérií do Stockholmského programu.

Rozsáhlé informační systémy

70. Bod 4.2.3.2 sdělení se stručně zabývá budoucností velkých informačních systémů s důrazem na Schengenský informační systém (SIS) a vízový informační systém (VIS.)

71. Bod 4.2.3.2. také zmiňuje vytvoření elektronického systému registrace vstupů na území členských států a opuštění těchto území v rámci programu registrovaných cestujících. Komise zřízení tohoto systému oznámila již dříve jako součást „hraničního balíčku“ na základě podnětu místopředsedy Franca Frattiniho ([45]). EIOÚ byl poměrně kritický ve svých předběžných komentářích ([46]) ohledně tohoto návrhu, neboť nebyla dostatečně prokázána potřeba dalšího takového systému narušujícího soukromí vedle existujících rozsáhlých systémů. EIOÚ si nepovšimnul žádných dodatečných důkazů ohledně potřeby takového systému, a navrhuje proto, aby Rada tuto myšlenku ve Stockholmském programu neuváděla.

72. V této souvislosti si EIOÚ přeje odkázat na stanoviska o různých iniciativách v oblasti výměny informací v EU ([47]), ve kterých uvedl několik podnětů a připomínek týkajících se důsledků použití velkých databází na úrovni EU pro ochranu údajů. Mimo jiné věnoval zvláštní pozornost potřebě silných a vhodných záruk, které by měly existovat, jakož i proporcionalitě a nezbytnosti posouzení dopadů před tím, než budou v této oblasti navržena nebo přijata jakákoli opatření. EIOÚ se vždy zasazoval za

([43]) Centralizovaným uchováváním se v tomto kontextu rozumí uchovávání na ústřední evropské úrovni, zatímco decentralizovaným uchováváním se rozumí uchovávání na úrovni členských států.

([44]) Viz poznámka pod čarou 33.

([45]) Sdělení Komise „Příprava dalších kroků v oblasti správy hranic v Evropské unii“, 13.2.2008, KOM(2008) 69 v konečném znění.

([46]) Předběžné komentáře EIOÚ o třech sděleních Komise v oblasti správy hranic(KOM(2008) 69, KOM(2008) 68 a KOM(2008) 67), 3. března 2008: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2008/08-03-03_Comments_border_package_EN.pdf

([47]) Zejména: Stanovisko ze dne 23. března 2005 k návrhu nařízení Evropského parlamentu a Rady o Vízovém informačním systému (VIS) a výměně údajů o krátkodobých vízech mezi členskými státy, Úř. věst. C 181, 23.7.2005, s. 13, a stanovisko ze dne 19. října 2005 o třech návrzích týkajících se Schengenského informačního systému druhé generace (SIS II), Úř. věst. C 91, 19.4.2006, s. 38.

správnou a s ochranou údajů slučitelnou rovnováhu mezi bezpečnostními požadavky a soukromím jednotlivců, které jsou subjekty systémů. V pozici vykonavatele dohledu nad ústředními částmi systémů zaujal stejný postoj.

73. Navíc EIOÚ využívá této příležitosti k tomu, aby zdůraznil potřebu jednotného přístupu k výměně informací v EU jako celku, z hlediska jednoty systémů, které již existují a těmi, které jsou v procesu vývoje, po právní a technické stránce a stránce dohledu. Dnes je skutečně více než kdykoli před tím nutná odvážná a soudržná vize toho, jak by měla vypadat výměna informací v EU a budoucí rozsáhlé informační systémy. Jen na základě takové vize lze znovu uvažovat o elektronickém systému pro registraci vstupu na území členských států a opuštění těchto území.

74. EIOÚ navrhuje, aby Stockholmský program zmínil záměr vypracovat takovou vizi, která by měla zahrnovat zvážení možného vstupu Lisabonské smlouvy v platnost a jejích důsledků pro systémy, které jsou postaveny na právních základech prvního a třetího pilíře.

75. Nakonec sdělení zmiňuje založení nové agentury, do jejíž působnosti by měl podle sdělení rovněž spadat daný elektronický systém registrace vstupů na území a opouštění území. Mezitím Komise přijala návrh na zřízení této agentury ([48]). EIOÚ tento návrh v zásadě podporuje, neboť může zajistit účinnější fungování těchto systémů včetně ochrany údajů Včas k tomuto návrhu předloží stanovisko.

Europol a Eurojust

76. Role Europolu je zmíněna na několika místech ve sdělení, které zdůrazňuje jako zásadní věc, že Europol musí sehrávat klíčovou úlohu v koordinaci, výměně informací a v přípravě odborníků. Podobně bod 4.2.2 uvádí nedávné změny v právním rámci spolupráce mezi Eurojustem a Europolem a oznamuje, že bude pokračovat posilování Eurojustu, a to zejména v oblasti vyšetřování přeshraniční organizované trestné činnosti. EIOÚ tyto cíle plně podporuje za podmínky, že jsou náležitým způsobem respektovány záruky ochrany údajů.

([48]) Návrh Komise ze dne 24. června 2009 pro nařízení Evropského parlamentu a Rady o zřízení agentury pro provozní řízení Schengenského informačního systému (SIS II), vízového informačního systému (VIS), EURODAC a jiných rozsáhlých informačních systémů v rámci prostoru svobody, bezpečnosti a práva (KOM(2009) 293/2).

77. V této souvislosti EIOÚ vítá nově navrhovanou dohodu, na níž se nedávno dohodl Europol a Eurojust ([49]), která má za cíl zlepšení a rozšíření vzájemné spolupráce mezi oběma subjekty a zajištění účinné výměny informací mezi nimi. Jedná se o činnost, při které účinná a účelná ochrana údajů hraje zásadní roli.

VI.4 **Použití biometrických údajů**

78. EIOÚ konstatuje, že se sdělení nezabývá otázkou zvýšeného využívání biometrických údajů v různých právních nástrojích Evropské unie týkajících se použití výměny informací, včetně nástrojů, jež jsou základem rozsáhlých informačních systémů. To je politováníhodné vzhledem k tomu, že se jedná z hlediska ochrany údajů a soukromí o zvláště důležitou a citlivou záležitost.

79. EIOÚ uznává obecné výhody používání biometrie, avšak pravidelně zdůrazňuje významný dopad používání takových údajů na práva jednotlivců a doporučuje zařadit do každého konkrétního systému při využití biometrie přísná ochranná opatření. Nedávné rozhodnutí Evropského soudu pro lidská práva ve věci *S. a Marper v. Spojené království* ([50]) poskytuje v tomto ohledu užitečné údaje, zejména pokud jde o odůvodnění a omezení použití biometrických údajů. Zejména použití informací o DNA může o jednotlivcích prozradit citlivé údaje, též vezmeme-li v úvahu, že technické možnosti získávání informací z DNA neustále rostou. V případě rozsáhlého použití biometrických údajů v informačních systémech se též objevuje problém způsobený inherentními nepřesnostmi sběru a srovnávání biometrických údajů. Z těchto důvodů by měl zákonodárce EU projevovat zdrženlivost při použití těchto údajů.

80. Další opakovanou otázkou bylo v posledních letech použití otisků prstů dětí a starších osob kvůli inherentní nedokonalosti biometrických systémů v případě těchto věkových skupin. EIOÚ požádal o důkladnou studii za účelem náležitého určení přesnosti systémů ([51]). Navrhnul věkový limit 14 let pro děti, ledaže tato studie prokáže něco jiného. EIOÚ doporučuje, aby byla tato otázka zmíněna ve Stockholmském programu.

([49]) Návrh dohody schválený Radou, který má být podepsán oběma stranami. Viz rejstřík Rady:
http://register.consilium.europa.eu/pdf/en/09/st10/st10019.en09.pdf
http://register.consilium.europa.eu/pdf/cs/09/st10/st10107.cs09.pdf

([50]) Spojená žádost 30562/04 a 30566/04, S. a Marper v. Spojené království, rozhodnutí ze dne 4. prosince 2008, ECHR, dosud nepublikováno.

([51]) Stanovisko ze dne 26. března 2008 k návrhu nařízení, kterým se mění nařízení Rady (ES) č. 2252/2004 o normách pro bezpečnostní a biometrické prvky v cestovních pasech a cestovních dokladech vydávaných členskými státy, Úř. věst. C 200, 6.8.2008, s. 1.

81. S ohledem na uvedené skutečnosti EIOÚ navrhuje, že by bylo užitečné vypracovat věcná kritéria pro použití biometrických údajů. Tato kritéria by měla zajistit, aby údaje byly použity pouze tehdy, pokud to je nezbytné, vhodné a přiměřené a pokud byl zákonodárcem prokázán jasný, konkrétní a legitimní účel. Konkrétněji řečeno by biometrické údaje a zejména údaje o DNA neměly být použity, pokud lze stejného účinku dosáhnout použitím jiných, méně citlivých informací.

VII. **PŘÍSTUP KE SPRAVEDLNOSTI A K E-JUSTICI**

82. Technologie bude též používána jako nástroj pro lepší justiční spolupráci. V bodě 3.4.1 sdělení je e-justice prezentována jako nástroj poskytující občanům snadnější přístup ke spravedlnosti. Představuje portál s informacemi a videokonferencemi jako součástmi právních řízení. Dále se otevírá možnostem právních řízení on-line a předpokládá propojení mezi vnitrostátními rejstříky, jako např. insolvenčními rejstříky. EIOÚ konstatuje, že sdělení nezmiňuje nové iniciativy týkající se e-justice, ale konsoliduje činnosti, které již byly zahájeny. EIOÚ se některých z těchto činností účastní, v návaznosti na stanovisko, které vydal dne 19. prosince 2008 ke sdělení Komise – Směrem k evropské strategii pro elektronické soudnictví (e-justice) ([52]).

83. E-justice je ambiciózní projekt, který potřebuje plnou podporu. Může efektivně zlepšit justiční systém v Evropě a soudní ochranu občanů. Znamená podstatný krok vpřed směrem k evropskému prostoru práva. Vzhledem k tomuto pozitivnímu hodnocení lze učinit několik poznámek:

— Technologické systémy pro e-justici by měly být vytvořeny v souladu se zásadou „soukromí coby aspekt návrhu“. Jak bylo řečeno dříve, ve vztahu k evropskému informačnímu modelu, základem všeho je zvolit správnou architekturu.

— Propojení a interoperabilita systémů by měly respektovat zásadu omezení účelu.

— Odpovědnost jednotlivých aktérů by měla být přesně stanovena.

— Důsledky propojení vnitrostátních rejstříků s citlivými osobními údaji, jako jsou insolvenční rejstříky, pro jednotlivce by měly být analyzovány v předstihu.

VIII. **ZÁVĚRY**

84. EIOÚ schvaluje důraz, který sdělení klade na ochranu základní práv a zejména ochranu osobních údajů, jako na jednu z klíčových otázek budoucnosti prostoru svobody, bezpečnosti a práva. Podle EIOÚ sdělení správně podporuje rovnováhu mezi potřebami náležitých nástrojů v zájmu zaručení bezpečnosti občanů a ochranou jejich základních práv. Uznává, že by se měl klást větší důraz na ochranu osobních údajů.

85. EIOÚ plně podporuje bod 2.3 sdělení, který volá po úplném režimu ochrany údajů, který by zahrnoval všechny oblasti pravomocí EU nezávisle na vstupu Lisabonské smlouvy v platnost. V této souvislosti doporučuje:

— oznámit potřebu jasné a dlouhodobé vize takového úplného režimu ve Stockholmském programu,

— zhodnotit opatření, která byla v této oblasti přijata, jejich konkrétní provádění a účinnost, a vzít při tom v úvahu dopady na soukromí a účinnost, pokud jde o vynucování práva,

— zařadit do Stockholmského programu jako prioritu potřebu nového legislativního rámce, který by mj. nahradil rámcové rozhodnutí Rady 2008/977/SVV.

86. EIOÚ vítá záměry Komise znovu potvrdit zásady ochrany údajů, které musí být spojeny s veřejnou konzultací ohlášenou Komisí na konferenci s názvem „Osobní údaje – širší použití, větší ochrana?“ konané ve dnech 19. a 20. května 2009. Pokud jde o podstatu, EIOÚ zdůrazňuje význam zásady omezení účelu jako základního kamene práva na ochranu údajů a význam soustředění se na možnosti zlepšení účinnosti uplatňování zásad ochrany údajů prostřednictvím nástrojů, které posilují odpovědnost správců údajů.

87. „Soukromí coby aspekt návrhu“ a technologie respektující soukromí lze podpořit:

— režimem pro certifikaci ochrany soukromí a údajů jakožto možností pro tvůrce a uživatele informačních systémů,

— právní povinností pro tvůrce a uživatele informačních systémů používat systémy, které jsou v souladu se zásadou „soukromí coby aspekt návrhu“.

88. Pokud jde o vnější aspekty ochrany údajů, EIOÚ doporučuje:

— zdůraznit ve Stockholmském programu důležitost obecných dohod se Spojenými státy a ostatními třetími zeměmi o ochraně údajů a jejich výměně,

([52]) Stanovisko EIOÚ ze dne 19. prosince 2008 ke sdělení Komise – Směrem k evropské strategii pro elektronické soudnictví (e-justice), Úř. věst. C 128, 6.6.2009, s. 13.

— aktivně podporovat dodržování základních práv a zejména ochrany údajů ve vztazích se třetími zeměmi a s mezinárodními organizacemi,

— zmínit ve Stockholmském programu, že výměna údajů se třetími zeměmi vyžaduje odpovídající úroveň ochrany či jiné vhodné záruky v těchto třetích zemích.

89. EIOÚ bere s velkým zájmem na vědomí pokrok na cestě ke strategii Evropské unie pro správu informací a evropskému informačnímu modelu a zdůrazňuje, že by v těchto projektech měla být věnována pozornost prvkům týkajícím se ochrany údajů, které mají být dále rozpracovány ve Stockholmském programu. Architektura výměny informací by měla být založena na zásadě „soukromí coby aspekt návrhu“ a na „nejlepších dostupných technikách“.

90. Pouhá skutečnost, že je technicky možné vyměňovat digitální informace mezi interoperabilními databázemi či tyto databáze sloučit, neodůvodňuje výjimku ze zásady omezení účelu. Interoperabilita by měla být v konkrétních případech založena na jasném a pečlivém politickém rozhodnutí. EIOÚ navrhuje, aby byl tento koncept ve Stockholmském programu upřesněn.

91. Použití osobních údajů shromážděných pro obchodní účely k účelům vynucování práva by mělo podle EIOÚ být povoleno pouze za přísných podmínek stanovených v bodě 65 tohoto stanoviska.

92. Další podněty ohledně použití osobních informací zahrnují:

— Vypracovat podstatná kritéria pro volbu mezi centralizovanými a decentralizovanými systémy a zahrnout záměr tato kritéria vypracovat do Stockholmského programu.

— Vytvoření systému elektronické registrace vstupů na území členských států a opuštění těchto území v rámci programů registrovaných cestujících by ve Stockholmském programu být zmíněno nemělo.

— Podpořit posílení Europolu a Eurojustu a novou dohodu nedávno vypracovanou Europolem a Eurojustem.

— Vytvořit věcná kritéria pro použití biometrických údajů zajišťující, aby údaje byly použity pouze tehdy, pokud to je nezbytné, vhodné a přiměřené a pokud byl zákonodárcem prokázán jasný, konkrétní a legitimní účel. Údaje o DNA by neměly být používány, pokud lze stejného výsledku dosáhnout použitím jiných, méně citlivých informací.

93. EIOÚ podporuje e-justici a uvedl několik poznámek k tomu, jak projekt zlepšit (viz. bod 83).

V Bruselu dne 10. července 2009.

Peter HUSTINX

Evropský inspektor ochrany údajů