Stanovisko evropského inspektora ochrany údajů ke sdělení Komise Evropskému parlamentu a Radě – „Strategie vnitřní bezpečnosti Evropské unie: pět kroků směrem k bezpečnější Evropě“

(2011/C 101/02)

EVROPSKÝ INSPEKTOR OCHRANY ÚDAJŮ,

s ohledem na Smlouvu o fungování Evropské unie, a zejména na článek 16 této smlouvy,

s ohledem na Listinu základních práv Evropské unie, a zejména na články 7 a 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 ([1]),

s ohledem na žádost o stanovisko v souladu s nařízením (ES) č. 45/2001 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů ([2]), a zejména na článek 41,

PŘIJAL TOTO STANOVISKO

I. ÚVOD

1. Dne 22. listopadu 2010 přijala Komise sdělení s názvem „Strategie vnitřní bezpečnosti Evropské unie: pět kroků směrem k bezpečnější Evropě“ (dále jen „sdělení“) ([3]). Sdělení bylo zasláno evropskému inspektorovi ochrany údajů (EIOÚ) ke konzultaci.

2. EIOÚ vítá, že byl Komisí konzultován. EIOÚ poskytl již před přijetím sdělení neformální připomínky k návrhu znění, z nichž některé byly zohledněny v konečné verzi sdělení.

Souvislosti sdělení

3. Strategie vnitřní bezpečnosti Evropské unie (dále jen „ISS“), kterou se sdělení zabývá, byla přijata dne 23. února 2010 za španělského předsednictví ([4]). Tato strategie stanoví evropský model bezpečnosti, který zahrnuje mimo jiné opatření v oblasti prosazování práva a soudní spolupráce, správy hranic a civilní ochrany, při náležitém respektování společných evropských hodnot, jako jsou základní práva. Mezi její hlavní cíle patří:

— představit veřejnosti stávající nástroje EU, které již pomáhají zajistit bezpečnost a svobodu občanů EU, a přidané hodnoty opatření EU v této oblasti,

— dále rozvíjet společné nástroje a politiky využívající integrovanějšího přístupu, jenž řeší příčiny nejistoty, a nikoli pouze důsledky,

— posílit prosazování práva a soudní spolupráci, správu hranic, civilní ochranu a řešení katastrof.

4. ISS se zaměřuje na řešení nejnaléhavějších hrozeb a výzev týkajících se bezpečnosti EU, jako je závažná trestná činnost a organizovaný zločin, terorismus a kyberkriminalita, řízení vnějších hranic EU a zvyšování odolnosti vůči přírodním nebo lidmi způsobeným katastrofám. Strategie stanoví obecné pokyny, zásady a směry, kterými by se EU měla řídit při řešení těchto otázek, a vyzývá Komisi, aby navrhla opatření včetně harmonogramu k přijetí této strategie.

5. Dále je důležité poukázat v této souvislosti na nedávné závěry Rady pro spravedlnost a vnitřní věci o vytvoření a provádění politického cyklu EU pro boj proti organizované a závažné mezinárodní trestné činnosti přijaté ve dnech 8.–9. listopadu 2010 ([5]) (dále jen „závěry z listopadu 2010“). Tento dokument sleduje závěry Rady o architektuře vnitřní bezpečnosti z roku 2006 ([6]) a vyzývá Radu a Komisi, aby definovaly komplexní ISS založenou na společných hodnotách a zásadách EU, jež byly potvrzeny v Listině základních práv Evropské unie ([7]).

([1]) Úř. věst. L 281, 23.11.1995, s. 31.
([2]) Úř. věst. L 8, 12.1.2001, s. 1.
([3]) KOM(2010) 673 v konečném znění.
([4]) Dok. 5842/2/10.
([5]) 3043. zasedání Rady pro spravedlnost a vnitřní věci, 8.–10. listopadu 2010, Brusel.
([6]) Dok. 7039/2/06 SVV 86 CATS 34.
([7]) Politický cyklus EU pro boj proti organizované a závažné mezinárodní trestné činnosti, kterým se zabývaly závěry Rady z listopadu 2010, sestává ze čtyř kroků: 1) Rozvoj politiky na základě posouzení hrozeb závažné trestné činnosti a organizovaného zločinu Evropské unie (EU SOCTA) 2) Stanovení politik a rozhodování na základě vymezení omezeného počtu priorit Radou 3) Provádění a monitorování ročního operačního plánu (OAP) a 4) Na konci politického cyklu důkladné zhodnocení, které bude rovněž sloužit jako vstup pro další politický cyklus.

6. Pokud jde o směry a cíle, které by měly vést k provedení ISS, závěry z listopadu 2010 odkazují na úvahy o proaktivním přístupu založeném na zpravodajské činnosti, úzké spolupráci mezi agenturami EU, včetně dalšího zlepšování jejich výměny informací, a cíl informování občanů o důležitosti činnosti Unie vyvíjené za účelem zajištění jejich ochrany. Ve svých závěrech Rada dále vyzývá Komisi, aby společně s odborníky příslušných agentur a členských států vypracovala víceletý strategický plán (dále jen „MASP“) pro každou prioritu, který stanoví nejvhodnější strategii pro řešení problému. Vyzývá rovněž Komisi, aby na základě konzultací s odborníky členských států a agentur EU vypracovala nezávislý mechanismus pro provádění MASP. EIOÚ se v tomto stanovisku bude těmito otázkami zabývat, jelikož úzce souvisí s ochranou osobních údajů, soukromí a dalšími základními právy a svobodami nebo mají na tyto oblasti významný dopad.

Obsah a cíl sdělení

7. Sdělení navrhuje pět strategických cílů, přičemž všechny tyto cíle souvisí s ochranou soukromí a údajů.

— zničit mezinárodní zločineckou síť,

— předcházet terorismu a řešit radikalizaci a nábor,

— zvýšit pro občany a podniky úroveň bezpečnosti v kyberprostoru,

— posílit bezpečnost prostřednictvím řízení hranic a

— zlepšit odolnost Evropy vůči krizím a katastrofám.

8. Strategie vnitřní bezpečnosti Evropské unie navrhovaná ve sdělení předkládá sdílený program pro členské státy, Evropský parlament, Komisi, Radu, agentury a jiné subjekty, včetně občanské společnosti a místních orgánů, a navrhuje, jak by mohly na základě spolupráce v následujících čtyřech letech dosáhnout cílů ISS.

9. Sdělení vychází z Lisabonské smlouvy a uznává pokyny zavedené Stockholmským programem (a jeho akčním plánem), které v kapitole 4.1 zdůrazňují nezbytnost přijetí komplexní ISS založené na dodržování základních práv, mezinárodní ochraně a právním státu. Kromě toho by se podle Stockholmského programu mělo rozvíjení, monitorování a provádění strategie vnitřní bezpečnosti stát jedním z prvořadých úkolů Stálého výboru pro operativní spolupráci v oblasti vnitřní bezpečnosti (COSI) zřízeného podle článku 71 Smlouvy o fungování Evropské unie. Strategie vnitřní bezpečnosti by se v zájmu zajištění jejího účinného provádění měla vztahovat i na bezpečnostní aspekty integrované správy hranic a popřípadě i na justiční spolupráci v trestních věcech, pokud se týkají operativní spolupráce v oblasti vnitřní bezpečnosti. V této souvislosti je rovněž důležité zdůraznit, že Stockholmský program požaduje integrovaný přístup k ISS, která by měla zohlednit strategii vnější bezpečnosti vypracovanou v rámci Unie, jakož i další politiky Unie, zejména ty, které se týkají vnitřního trhu.

Cíl stanoviska

10. Sdělení poukazuje na různé oblasti politiky, které jsou součástí široce chápaného konceptu „vnitřní bezpečnosti“ v Evropské unii nebo na něj mají dopad.

11. Cílem tohoto stanoviska není analyzovat všechny oblasti politiky a jednotlivá témata, kterými se sdělení zabývá, ale:

— přezkoumat samotné cíle ISS navržené ve sdělení z konkrétního hlediska ochrany soukromí a údajů a – z tohoto úhlu – zdůraznit nutné vazby na další strategie, které jsou v současnosti projednávány a přijímány na úrovni EU,

— uvést řadu poznámek a konceptů týkajících se ochrany údajů, které by měly být zohledněny při navrhování, rozvíjení a provádění ISS na úrovni EU,

— předložit – tam, kde je to užitečné a vhodné – návrhy týkající se toho, jak nejlépe zohlednit otázky týkající se ochrany údajů při provádění opatření navrhovaných ve sdělení.

12. EIOÚ v této souvislosti zejména zdůrazní vazbu mezi ISS a strategií pro správu informací a přípravu souhrnného rámce pro ochranu údajů. Evropský inspektor ochrany údajů kromě toho zmíní koncepty jako: nejlepší dostupné techniky a ochrana soukromí již ve fázi návrhu („Privacy by design“), hodnocení dopadů na soukromí a ochranu údajů a práva subjektů údajů, které mají přímý dopad na navrhování a provádění ISS. Stanovisko se rovněž vyjádří k řadě vybraných oblastí politiky, jako je integrovaná správa hranic, včetně systému EUROSUR, a zpracování osobních údajů agenturou FRONTEX, jakož i k dalším oblastem, jako je program TFTP.

II. OBECNÉ PŘIPOMÍNKY

Potřeba komplexnějšího a „strategičtějšího“ přístupu ke strategiím EU souvisejícím s ISS

13. V současné době jsou na úrovni EU projednávány a navrhovány různé strategie založené na Lisabonské smlouvě a Stockholmském programu, které mají přímý či nepřímý dopad na ochranu údajů. Jednou z nich je i ISS, která je úzce propojena s dalšími strategiemi (o nichž se zmiňují nedávná sdělení Komise nebo u nichž se předpokládá, že se tak stane v blízké budoucnosti), jako je strategie EU pro správu informací a evropský model pro výměnu informací, strategie pro uplatňování Listiny základních práv EU, komplexní strategie pro ochranu údajů a politika EU pro boj proti terorismu. EIOÚ v tomto stanovisku věnuje zvláštní pozornost propojení se strategií pro správu informací a souhrnným rámcem pro ochranu údajů založeném na článku 16 Smlouvy o fungování Evropské unie, které mají na ISS z hlediska ochrany údajů nejpatrnější vazby.

14. Všechny tyto strategie představují pestrou směsici navzájem propojených směrů politik, programů a akčních plánů, které vyžadují komplexní a integrovaný přístup na úrovni EU.

15. Obecněji lze říci, že tento přístup „propojování strategií“ – pokud bude zohledněn v rámci budoucích opatření – by ukázal, že na úrovni EU existuje vize, pokud jde o *strategie EU*, a že tyto strategie a nedávno přijatá sdělení, která se jimi zabývají, jsou navzájem úzce propojeny, což je fakt, přičemž společným bodem pro všechny z nich je Stockholmský program. Tento přístup by rovněž vedl k vytvoření pozitivních synergií mezi různými politikami spadajícími do prostoru svobody, bezpečnosti a práva a zabránil by možnému zdvojení činnosti a úsilí v této oblasti. Stejně významné je také to, že by tento přístup vedl k účinnějšímu a soudržnějšímu uplatňování pravidel o ochraně údajů v kontextu všech navzájem propojených strategií.

16. EIOÚ zdůrazňuje, že jedním z pilířů ISS je účinná správa informací v Evropské unii, která by v zájmu odůvodnění nutnosti výměny informací měla být založena na zásadách nezbytnosti a proporcionality.

17. Kromě toho, jak je uvedeno ve stanovisku EIOÚ ke sdělení o správě informací ([8]), EIOÚ zdůrazňuje, že každé nové legislativní opatření, jež má usnadnit uchovávání osobních dat a jejich výměnu, by mělo být navrženo jen v případě, že bude konkrétně doložena jeho potřeba ([9]). Tento právní požadavek by měl být při provádění ISS přeměněn na proaktivní přístup k politice. Potřeba komplexního přístupu k ISS je rovněž nevyhnutelně spjata s potřebou posouzení všech nástrojů, které v oblasti vnitřní bezpečnosti již existují, dříve než budou navrženy nástroje nové.

18. V této souvislosti EIOÚ rovněž navrhuje, aby byly častěji používány doložky, jež stanoví pravidelné hodnocení stávajících nástrojů, jako jsou nástroje obsažené ve směrnici o uchovávání údajů, která je v současné době předmětem hodnocení ([10]).

Ochrana údajů jako cíl ISS

19. Sdělení odkazuje na ochranu osobních údajů v odstavci „Politiky v oblasti bezpečnosti založené na společných hodnotách“, kde uvádí, že nástroje a opatření týkající se provádění ISS musí být založeny na společných hodnotách včetně právního státu a dodržování základních práv stanovených v Listině základních práv Evropské unie. V této souvislosti stanoví, že „Zatímco výměna informací usnadňuje účinné prosazování práva v EU, musíme také chránit soukromí fyzických osob a jejich základní právo na ochranu osobních údajů.“

20. Je to vítané prohlášení. Nicméně takové prohlášení nemůže být považováno za dostatečné řešení problematiky ochrany údajů v ISS. Sdělení se podrobněji nezabývá ochranou údajů ([11]) ani nevysvětluje, jak by mělo dodržování ochrany soukromí a osobních údajů být zajištěno v praxi v rámci opatření, kterými se provádí ISS.

([8]) Stanovisko ze dne 30. září 2010 ke sdělení Komise Evropskému parlamentu a Radě – „Přehled o správě informací v prostoru svobody, bezpečnosti a práva“.

([9]) Toto je právní požadavek; viz zejména rozsudek ESD ve spojených věcech C-92/09 a C-93/09 ze dne 2. listopadu 2010. V konkrétnějších souvislostech EIOÚ podpořil tento přístup rovněž v dalších stanoviscích k legislativním návrhům souvisejícím s prostorem svobody, bezpečnosti a práva: např. ze dne 19. října 2005 o třech návrzích týkajících se Schengenského informačního systému druhé generace (SIS II); stanovisko ze dne 20. prosince 2007 k návrhu rámcového rozhodnutí Rady o používání jmenné evidence cestujících pro účely vynucování práva; stanovisko ze dne 18. února 2009 k návrhu nařízení o zřízení systému „Eurodac“ pro porovnávání otisků prstů za účelem účinného uplatňování nařízení (ES) č. [.../...] (kterým se stanoví kritéria a postupy pro určení členského státu příslušného k posuzování žádosti o poskytnutí mezinárodní ochrany podané státním příslušníkem třetí země nebo osobou bez státní příslušnosti v některém z členských států); stanovisko ze dne 18. února 2009 k návrhu nařízení, kterým se stanoví kritéria a postupy pro určení členského státu příslušného k posuzování žádosti o poskytnutí mezinárodní ochrany podané státním příslušníkem třetí země nebo osobou bez státní příslušnosti v některém z členských států; a stanovisko ze dne 7. října 2009 k návrhům v oblasti přístupu donucovacích orgánů do systému EURODAC.

([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).

([11]) Ochrana údajů je konkrétněji zmiňována pouze v souvislosti se záležitostí zpracovávání osobních údajů agenturou FRONTEX.

21. Podle EIOÚ by měla jedním z cílů *Strategie vnitřní bezpečnosti Evropské unie* být *ochrana* v širším smyslu, která by zajistila *náležitou* rovnováhu mezi ochranou občanů před existujícími hrozbami na jedné straně a ochranou jejich soukromí a práva na ochranu osobních údajů na straně druhé. Jinými slovy otázka bezpečnosti a soukromí musí být v rámci rozvoje ISS rovněž náležitě zohledněna, což je v souladu se Stockholmským programem a závěry Rady.

22. Krátce řečeno, zajišťování bezpečnosti při plném dodržování ochrany soukromí a údajů by mělo být uvedeno jako zvláštní cíl Strategie vnitřní bezpečnosti Evropské unie. Tento cíl by měl být zohledněn v rámci všech opatření k provedení strategie přijatých členskými státy a orgány EU.

23. Evropský inspektor ochrany údajů v této souvislosti odkazuje na sdělení (2010) 609 o komplexním přístupu k ochraně osobních údajů v Evropské unii ([12]). EIOÚ k tomuto sdělení brzy vydá stanovisko, na tomto místě však zdůrazňuje, že ISS nemůže účinně fungovat bez podpory spolehlivého programu ochrany údajů, který ji doplňuje a nastoluje vzájemnou důvěru a zajišťuje lepší účinnost.

III. POZNÁMKY A KONCEPTY TÝKAJÍCÍ SE NAVRHOVÁNÍ A UPLATŇOVÁNÍ ISS

24. Je zřejmé, že některá z opatření přijatých v zájmu plnění cílů ISS mohou zvýšit rizika pro ochranu soukromí a osobních údajů jednotlivců. EIOÚ by rád konkrétně upozornil na koncepty, jež mohou tato rizika vyvážit, jako je ochrana soukromí již ve fázi návrhu („Privacy by design"), hodnocení dopadů na soukromí a ochranu údajů, práva subjektů údajů a nejlepší dostupné techniky. Všechny tyto koncepty by měly být při uplatňování ISS zohledněny a mohou užitečným způsobem přispět k tomu, aby politiky uplatňované v této oblasti ve větší míře respektovaly soukromí a ochranu údajů.

Ochrana soukromí již ve fázi návrhu („privacy by design")

25. Evropský inspektor ochrany údajů při různých příležitostech a v různých stanoviscích podpořil koncept „zabudovaného" soukromí (ochrana soukromí již ve fázi návrhu „Privacy by design" nebo standardní nastavení ochrany soukromí „Privacy by default"). Tento koncept je nyní vypracováván pro veřejný i soukromý sektor, a musí se tedy významně projevit rovněž v rámci vnitřní bezpečnosti EU a v oblasti policie a justice ([13]).

26. Sdělení se o tomto konceptu nezmiňuje. EIOÚ navrhuje, aby byl tento koncept zmíněn v cílených opatřeních, která budou navržena a přijata v rámci provádění ISS, zejména v souvislosti s cílem 4 „posílení bezpečnosti prostřednictvím správy hranic", kde je jasná zmínka o posíleném využívání nových technologií pro hraničních kontrolách a ostraze hranic.

Posouzení dopadů na soukromí a ochranu údajů

27. EIOÚ vyzývá Komisi, aby se – v rámci budoucího navrhování a provádění ISS založené na sdělení – zabývala tím, co přesně by mělo být chápáno pod skutečným „hodnocením dopadů na soukromí a ochranu údajů" v prostoru svobody, bezpečnosti a práva, a zejména v ISS.

28. Sdělení se zmiňuje o posouzení hrozby a rizik. EIOÚ tuto skutečnost vítá. Toto sdělení se nicméně v žádném bodě nezabývá posuzováním dopadů na soukromí a ochranu údajů. EIOÚ se domnívá, že práce na provádění sdělení o ISS je dobrou příležitostí k vypracování takového posouzení v kontextu vnitřní bezpečnosti. Evropský inspektor ochrany údajů konstatuje, že ani sdělení, ani pokyny Komise pro posuzování dopadů ([14]) tento aspekt nespecifikují a nerozvíjejí natolik, aby se stal jedním z požadavků politik.

29. Proto evropský inspektor ochrany údajů doporučuje, aby u budoucích nástrojů bylo prováděno konkrétnější a přísnější posouzení dopadů na soukromí a ochranu údajů, buď jako samostatné posouzení, nebo v rámci celkového posouzení dopadů na základní práva vypracovaného Komisí. Toto posouzení dopadů by nemělo pouze stanovit obecné zásady nebo analyzovat možnosti politik, jako je tomu v současné době, ale mělo by rovněž doporučovat specifické a konkrétní záruky.

30. Měly by být proto vypracovány specifické ukazatele a charakteristiky, aby se zajistilo, že každý návrh s dopadem na soukromí a ochranu údajů v oblasti vnitřní bezpečnosti EU bude podroben důkladnému posouzení, včetně takových aspektů, jako je zásada proporcionality, nezbytnosti a omezení účelu.

31. Kromě toho by v této souvislosti mohlo být užitečné odvolat se na článek 4 doporučení o RFID ([15]), ve kterém Komise vyzvala členské státy, aby zajistily spolupráci subjektů odvětví s příslušnými zúčastněnými stranami

([12]) Sdělení Komise Evropskému parlamentu, Radě a Evropskému hospodářskému a sociálnímu výboru a Výboru regionů o komplexním přístupu k ochraně údajů v Evropské unii, KOM (2010) 609.

([13]) EIOÚ ve svém stanovisku ke sdělení Komise o Stockholmském programu doporučil, aby pro tvůrce a uživatele informačních systémů bylo právní povinností vyvíjet a používat systémy, které jsou v souladu se zásadou ochrany soukromí již ve fázi návrhu („privacy by design").

([14]) SEK(2009) 92, 15.1.2009.

([15]) K(2009) 3200 v konečném znění, 12.5.2009.

z občanské společnosti při vypracování rámce pro posuzování dopadů na soukromí a ochranu údajů. Také madridské usnesení přijaté mezinárodní konferencí komisařů pro ochranu soukromí a údajů v listopadu 2009 vyzvalo k provádění posouzení dopadů na soukromí a ochranu údajů před zaváděním nových informačních systémů a technologií pro zpracování osobních údajů nebo významnými změnami stávajícího způsobu zpracování.

Práva subjektů údajů

32. Evropský inspektor ochrany údajů konstatuje, že sdělení se konkrétně nezabývá otázkou práv subjektů údajů, která má v rámci ochrany údajů rozhodující roli a měla by mít dopad na koncepci ISS. Je nezbytné zajistit, aby v rámci všech různých systémů a nástrojů zabývajících se vnitřní bezpečností EU měly osoby, na něž se tyto systémy a nástroje vztahují, podobná práva, pokud jde o to, jak jsou zpracovávány jejich osobní údaje.

33. Mnohé ze systémů, o kterých se sdělení zmiňuje, ovšem zavádějí specifická pravidla v oblasti práv občanů (která se rovněž vztahují na takové kategorie osob, jako jsou oběti, osoby podezřelé z trestných činů nebo přistěhovalci), ale mezi těmito systémy a nástroji existuje mnoho rozdílů, aniž pro to je pádný důvod.

34. Evropský inspektor ochrany údajů proto vyzývá Komisi, aby se v brzké budoucnosti důkladněji zabývala otázkou sjednocení práv subjektů údajů v EU v rámci ISS a strategie EU pro správu informací.

35. Zvláštní pozornost je třeba věnovat nápravným mechanismům. Strategie vnitřní bezpečnosti Evropské unie by měla zaručit, že vždy, když nebyla práva jednotlivců plně respektována, správci údajů zahájí postupy pro vyřizování stížností, které jsou snadno dostupné, účinné a finančně přístupné.

Nejlepší dostupné techniky

36. Provádění ISS bude nevyhnutelně založeno na využívání infrastruktury IT, která podpoří opatření stanovená ve sdělení. Nejlepší dostupné techniky lze považovat za nástroje umožňující dosažení řádné rovnováhy mezi plněním cílů ISS a dodržováním práv jednotlivců. V této souvislosti by EIOÚ rád znovu připomněl doporučení učiněná v předchozích stanoviscích ([16]), která se týkají potřeby stanovení a podpory konkrétních opatření pro provádění nejlepších dostupných technik Komisí ve spolupráci se zúčastněnými subjekty v odvětví. Takové uplatňování znamená nejúčinnější a nejpokročilejší fázi rozvoje činností a jejich metod fungování, jež naznačí praktickou vhodnost jednotlivých technik pro dosahování předpokládaných výsledků efektivním způsobem a v souladu s rámcem EU pro ochranu soukromí a údajů. Tento přístup je plně v souladu s přístupem „privacy by design" zmíněným výše.

37. V případě, že je to vhodné a proveditelné, by měly být vypracovány referenční dokumenty o nejlepších dostupných technikách s cílem poskytnout pokyny a větší právní jistotu pro skutečné provádění opatření v rámci ISS. Tím by se rovněž podpořila harmonizace takových opatření v různých členských státech. A v neposlední řadě stanovení nejlepších dostupných technik respektujících soukromí a bezpečnost zjednoduší dohled orgánů na ochranu údajů tím, že jim poskytne technické reference přijaté správci údajů, které jsou v souladu s ochranou soukromí a údajů.

38. EIOÚ rovněž zdůrazňuje význam náležitého sladění ISS s činnostmi, které již byly vykonány v rámci sedmého rámcového programu pro výzkum a technologický rozvoj a rámcový program „Bezpečnost a ochrana svobod". Společná vize poskytnutí nejlepších dostupných technik umožní inovaci znalostí a schopností vyžadovaných pro ochranu občanů při současné ochraně základních práv.

39. Evropský inspektor ochrany údajů nakonec zdůrazňuje úlohu, kterou může hrát Evropská agentura pro bezpečnost sítí a informací (ENISA) při vypracovávání pokynů a hodnocení schopností v oblasti bezpečnosti vyžadovaných pro zajištění integrity a dostupnosti informačních systémů a rovněž při prosazování těchto nejlepších dostupných technik. S ohledem na tuto skutečnost EIOÚ vítá, že se agentura jako klíčový subjekt podílí na zlepšování schopnosti řešení kybernetických útoků a boji proti kyberkriminalitě ([17]).

Seznámení se subjekty a jejich úkoly

40. V této souvislosti je rovněž třeba uvést podrobnější informace týkající se činitelů, které jsou součástí architektury ISS nebo k ní přispívají. Sdělení uvádí různé činitele a subjekty,

([16]) Stanovisko EIOÚ k inteligentním dopravním systémům, červenec 2009 a stanovisko EIOÚ ke sdělení o RFID z prosince 2007; viz rovněž výroční zpráva EIOÚ z roku 2006 s. 48.

([17]) EIOÚ předpokládá přijetí stanoviska k právnímu rámci agentury ENISA ještě v prosinci 2010.

jako jsou občané, soudní orgány, agentury EU, vnitrostátní orgány, policie a podniky. Konkrétní úlohy a pravomoci těchto činitelů by měly být v navrhovaných opatřeních v rámci provádění ISS lépe vymezeny.

IV. ZVLÁŠTNÍ PŘIPOMÍNKY K OBLASTEM POLITIK SOUVISEJÍCÍM S ISS

Integrovaná správa hranic

41. Sdělení zmiňuje skutečnost, že díky vstupu Lisabonské smlouvy v platnost má EU lepší pozici pro využití synergií v politikách správy hranic ohledně pohybu osob a zboží. V souvislosti s pohybem osob uvádí, že: „EU může řešit řízení migrace a boj proti trestné činnosti jako dva cíle strategie integrované správy hranic." Dokument správu hranic považuje rovněž za potenciálně účinný prostředek pro boj proti závažné trestné činnost a organizovanému zločinu ([18]).

42. EIOÚ rovněž konstatuje, že sdělení stanoví tři strategické prvky: 1) posílené používání nových technologií při hraničních kontrolách (SIS II, VIS II, systém vstupu/výstupu a program registrovaných cestujících); 2) posílené používání nových technologií při ostraze hranic (evropský systém ostrahy hranic, EUROSUR) a 3) posílená koordinace mezi členskými státy prostřednictvím agentury FRONTEX.

43. EIOÚ by rád využil příležitosti, která se mu naskýtá v podobě tohoto stanoviska, a opakuje žádosti, které učinil v řadě předchozích stanovisek a jejichž předmětem bylo zavedení jasné politiky v oblasti správy hranic na úrovni EU, která plně respektuje pravidla ochrany údajů. Evropský inspektor ochrany údajů věří, že současná činnost týkající se ISS a správy informací představuje velmi dobrou příležitost k přijetí konkrétnějších opatření k zajištění soudržného přístupu k politikám v těchto oblastech.

44. EIOÚ bere na vědomí, že sdělení neodkazuje pouze na stávající rozsáhlé systémy a systémy, které mohou začít fungovat v blízké budoucnosti (např. SIS, SIS II a VIS), ale rovněž na systémy, které mohou být navrženy Komisí v budoucnosti, ohledně nichž však dosud nebylo přijato rozhodnutí (tj. program pro registrované cestující (RTP) a systém vstupu/výstupu (Entry/Exit System)). V této souvislosti je třeba připomenout, že cíle a legitimitu zavedení těchto systémů je ještě třeba vyjasnit a prokázat, rovněž ve světle výsledků konkrétních posouzení dopadů provedených Komisí. Pokud se tak nestane, sdělení může být vnímáno jako dokument, který předjímá rozhodovací postup, a v důsledku toho nebere v úvahu skutečnost, že konečné rozhodnutí o tom, zda RTP a systém vstupu/výstupu budou zavedeny v Evropské unii, ještě nebylo přijato.

45. EIOÚ proto navrhuje, aby se v rámci budoucí činnosti na provádění ISS takovému předjímání zabránilo. Jak je uvedeno výše, veškerá rozhodnutí o zavedení rozsáhlých systémů, které zasahují do soukromí, by měla být přijata na základě náležitého posouzení všech stávajících systémů, s řádným ohledem na zásadu nezbytnosti a proporcionality.

EUROSUR

46. Sdělení uvádí, že Komise předloží legislativní návrh na zřízení systému EUROSUR do roku 2011, a přispěje tak k vnitřní bezpečnosti a boji proti zločinu. Uvádí se zde rovněž, že EUROSUR bude využívat nové technologie vyvinuté prostřednictvím výzkumných činností a projektů financovaných EU, jako jsou satelitní snímky na zjištění a sledování cílů na námořních hranicích, například rychlých plavidel dovážejících do EU drogy.

47. V této souvislosti EIOÚ konstatuje, že není jasné, zda a případně do jaké míry legislativní návrh na zřízení systému EUROSUR, který má Komise předložit do roku 2011, předpokládá zpracovávání osobních údajů v rámci EUROSUR. Komise v tomto sdělení k této otázce nezaujala jasné stanovisko. Tato záležitost je o to relevantnější, že sdělení stanoví jasné vazby mezi systémem EUROSUR a agenturou FRONTEX na taktické, operační a strategické úrovni (viz poznámky týkající se agentury FRONTEX) a požaduje, aby oba subjekty úzce spolupracovaly.

Zpracovávání osobních údajů agenturou FRONTEX

48. EIOÚ vydal dne 17. května 2010 stanovisko k přezkumu nařízení o agentuře FRONTEX ([19]), ve kterém požadoval zahájení skutečné diskuse a důkladný rozbor problematiky ochrany údajů v souvislosti s posilováním stávajících úkolů agentury FRONTEX a přidělováním téže agentuře úkolů nových.

49. Ve sdělení je zmiňována nutnost posílit přispění agentury FRONTEX na vnějších hranicích v rámci cíle 4 *Posílení bezpečnosti prostřednictvím správy hranic*. V této souvislosti se ve sdělení uvádí, že na základě zkušenosti a v souvislosti s obecným přístupem EU ke správě informací se Komise domnívá, že zmocnění agentury FRONTEX, aby zpracovávala a používala tyto informace v omezeném rozsahu a v

([18]) Tisková zpráva ke Strategii vnitřní bezpečnosti Evropské unie: pět kroků směrem k bezpečnější Evropě Memo 10/598.

([19]) Stanovisko EIOÚ ze dne 17. května 2010 k návrhu nařízení Evropského parlamentu a Rady, kterým se mění nařízení Rady (ES) č. 2007/2004 o zřízení Evropské agentury pro řízení operativní spolupráce na vnějších hranicích členských států Evropské unie (FRONTEX).

souladu s jasně stanovenými pravidly správy osobních údajů, významně přispěje k odstranění zločinných spolčení. Tento přístup je nový ve srovnání s přístupem zastávaným v návrhu Komise o přezkumu nařízení o agentuře FRONTEX, který je v současnosti předmětem diskuse v Evropském parlamentu a Radě a který se o zpracovávání osobních údajů nezmiňuje.

50. V této souvislosti Evropský inspektor ochrany údajů vítá skutečnost, že sdělení obsahuje některé informace týkající se okolností, za nichž se takové zpracování může ukázat jako nezbytné (např. analýza rizik, lepší provádění společných operací nebo výměna informací s Europolem). Sdělení konkrétně vysvětluje, že v současnosti informace o zločincích zapojených do nezákonných obchodních sítí – s nimiž agentura FRONTEX přichází do styku – nemohou být dále použity pro analýzu rizik nebo pro lepší zacílení budoucích společných operací. Příslušné údaje o podezřelých zločincích se navíc nedostanou k odpovědným vnitrostátním orgánům nebo k Europolu pro další vyšetřování.

51. Evropský inspektor ochrany údajů nicméně konstatuje, že se sdělení nezmiňuje o probíhající diskusi o revizi právního rámce agentury FRONTEX, která, jak je uvedeno výše, se na tento problém zaměřuje s cílem nalézt legislativní řešení. Kromě toho může znění sdělení zdůrazňující úlohu agentury FRONTEX v souvislosti s cílem rozbití zločinných spolčení vykládáno tak, že rozšiřuje pravomoci agentury. EIOÚ navrhuje, aby byl tento bod zohledněn jak v rámci přezkumu nařízení o agentuře FRONTEX, tak při provádění ISS.

52. Evropský inspektor ochrany údajů rovněž upozorňuje na nutnost zajištění toho, aby nedošlo duplicitě úkolů mezi agenturami Europol a Frontex. EIOÚ v této souvislosti vítá, že se ve sdělení uvádí, že je třeba zabránit duplicitě úkolů mezi těmito agenturami. Nicméně tato otázka by měla být jasněji rozpracována jak v revidovaném nařízení o agentuře FRONTEX, tak v opatřeních, kterými se provádí ISS a které stanoví úzkou spolupráci mezi agenturami FRONTEX a EUROPOL. To je zvláště důležité z hlediska zásad omezení účelu a kvality údajů. Toto konstatování se rovněž vztahuje na budoucí spolupráci s takovými agenturami, jako je Evropská agentura pro bezpečnost sítí a informací (ENISA) nebo Evropský podpůrný úřad pro otázky azylu (EASO).

Využití biometrických údajů

53. Sdělení se konkrétně nezabývá současným jevem širšího využití biometrických údajů v prostoru svobody, bezpečnosti a práva, včetně rozsáhlých informačních systémů EU a dalších nástrojů správy hranic.

54. EIOÚ proto využívá této příležitosti a připomíná svůj návrh ([20]), aby tato vysoce citlivá záležitost z hlediska ochrany údajů byla náležitě zohledněna při provádění ISS, zejména v kontextu správy hranic.

55. Evropský inspektor ochrany údajů rovněž doporučuje, aby byla vypracována jasná a jednoznačná politika pro využití biometrických údajů v prostoru svobody, bezpečnosti a práva, která bude vycházet z důkladného zhodnocení a posouzení potřeby využití biometrických údajů v jednotlivých případech v kontextu ISS, za plného respektování takových základních zásad ochrany údajů, jako je proporcionalita, nezbytnost a omezení účelu.

Program sledování financování terorismu (TFTP)

56. Ve sdělení se uvádí, že Komise v roce 2011 vypracuje politiku EU pro získávání a analýzu údajů, které se týkají finančních transakcí a jsou uloženy na území EU. EIOÚ v této souvislosti odkazuje na své stanovisko ze dne 22. června 2010 o zpracovávání a předávání údajů o finančních transakcích z Evropské unie do Spojených států pro účely Programu sledování financování terorismu (TFTP II) ([21]). Všechny kritické poznámky vyjádřené v tomto stanovisku jsou rovněž platné a použitelné v kontextu plánované práce na rámci EU pro údaje o finančních transakcích. Měly by být proto zohledněny v diskusích o této otázce. Zvláštní pozornost by měla být věnována přiměřenosti získávání a zpracovávání velkého objemu údajů o osobách, které nejsou podezřelé z trestných činů, a otázce účinného dohledu nezávislými a soudními orgány.

Bezpečnost v kyberprostoru pro občany a podniky

57. Evropský inspektor ochrany údajů vítá, že je ve sdělení přikládán velký význam preventivním opatřením na úrovni EU a zastává názor, že posilování bezpečnosti informačních sítí je stěžejním faktorem přispívajícím k dobře fungující informační společnosti. EIOÚ také podporuje konkrétní činnosti, které zlepšují schopnost řešení kybernetických útoků, budují kapacity donucovacích a soudních orgánů a utvářejí partnerství s průmyslem s cílem posílit občany a podniky. Role agentury ENISA jako subjektu usnadňujícího provádění řady opatření stanovených v tomto cíli je rovněž vítána.

([20]) Viz zejména stanovisko EIOÚ ke sdělení o přehledu o správě informací v prostoru svobody, bezpečnosti a práva uvedené v poznámce pod čarou 8.

([21]) Stanovisko EIOÚ ze dne 22. června 2010 k návrhu rozhodnutí Rady o uzavření Dohody mezi Evropskou unií a Spojenými státy americkými o zpracovávání a předávání údajů o finančních transakcích z Evropské unie do Spojených států pro účely Programu sledování financování terorismu (TFTP II).

58. Nicméně *Strategie vnitřní bezpečnosti Evropské unie* se blíže nezabývá plánovanými opatřeními k vynucování práva v kyberprostoru, tím, jak by tyto činnosti mohly ohrozit práva jednotlivců a jaké by měly být vyžadovány záruky. Evropský inspektor ochrany údajů vyzývá k ambiciózněji šímu přístupu k přiměřeným zárukám; tento přístup by měl sloužit k ochraně základních práv všech jednotlivců včetně těch, kteří mohou být dotčeni opatřeními pro boj s možnou trestnou činností v této oblasti.

V. **ZÁVĚRY A DOPORUČENÍ**

59. Evropský inspektor ochrany údajů požaduje, aby v rámci provádění ISS byly propojovány různé strategie a sdělení EU. Tento přístup by měl být uplatňován na základě konkrétního akčního plánu vycházejícího z důkladného posouzení potřeb, který by měl vyústit v souhrnnou, integrovanou a dobře strukturovanou politiku EU v oblasti ISS.

60. EIOÚ rovněž využívá této příležitosti ke zdůraznění významu právního požadavku na důkladné posouzení všech stávajících nástrojů, které budou využity v rámci ISS a výměny informací předtím, než budou navrženy nástroje nové. V této souvislosti se důrazně doporučuje zahrnout ustanovení, jež stanoví pravidelné hodnocení účinnosti relevantních nástrojů.

61. EIOÚ navrhuje, aby v rámci přípravy víceletého strategického plánu požadovaného v závěrech Rady z listopadu 2010 byla zohledněna probíhající příprava souhrnného rámce pro ochranu údajů na základě článku 16 Smlouvy o fungování Evropské unie, zejména sdělení (2009) 609.

62. EIOÚ předkládá řadu návrhů týkajících se poznámek a konceptů relevantních z hlediska ochrany údajů, které by měly být zohledněny v oblasti ISS, jako je zásada ochrany soukromí již ve fázi návrhu, hodnocení dopadů na soukromí a ochranu údajů a nejlepší dostupné techniky.

63. Evropský inspektor ochrany údajů doporučuje, aby u budoucích nástrojů bylo prováděno posouzení dopadů na soukromí a ochranu údajů, buď jako samostatné posouzení, nebo v rámci celkového posouzení dopadů na základní práva vypracovaného Komisí.

64. Vyzývá také Komisi, aby vypracovala soudržnější a jednotnější politiku stanovení předběžných podmínek pro využití biometrických údajů v oblasti ISS a lepšího sladění práv subjektů údajů na úrovni EU.

65. EIOÚ nakonec uvedl řadu poznámek ke zpracování osobních údajů v souvislosti se správou hranic, a to zejména agenturou FRONTEX nebo případně v rámci systému EUROSUR.

V Bruselu dne 17. prosince 2010.

Peter HUSTINX

evropský inspektor ochrany údajů