I

(Usnesení, doporučení a stanoviska)

STANOVISKA

EVROPSKÝ INSPEKTOR OCHRANY ÚDAJŮ

Stanovisko Evropského inspektora ochrany osobních údajů ke sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů o identifikaci na základě rádiové frekvence (RFID) v Evropě: kroky k rámci politiky KOM(2007) 96

(2008/C 101/01)

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 směrnici Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací,

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 15. března 2007 Komise přijala sdělení „Identifikace na základě rádiové frekvence (RFID) v Evropě: kroky k rámci politiky“ ([1]) (dále jen „sdělení“). Podle článku 41 nařízení (ES) č. 45/2001 je EIOÚ pověřen poradenstvím pro orgány a instituce Společenství ve všech otázkách, které se týkají zpracování osobních údajů. V souladu s uvedeným článkem předkládá EIOÚ toto stanovisko.

2. Stanovisko musí být chápáno jako reakce EIOÚ na toto sdělení, jakož i na další provedená opatření v oblasti RFID po přijetí tohoto sdělení. Mezi tato další významná opatření, která byla v tomto stanovisku zohledněna, patří:

— rozhodnutí Komise ze dne 28. června 2007, kterým se zřizuje skupina odborníků pro identifikaci na základě rádiové frekvence ([2]), které přímo vyplývá ze sdělení. Tato skupina je rovněž označována jako skupina zainteresovaných stran RFID. V souladu s čl. 4 odst. 4 písm. b) rozhodnutí se EIOÚ účastní činnosti skupiny jako pozorovatel,

— usnesení Rady ze dne 22. března 2007 o strategii pro bezpečnou informační společnost v Evropě ([3]),

— projekt „RFID a správa identity“ iniciovaný Evropským parlamentem ([4]).

([1]) KOM(2007) 96 v konečném znění.
([2]) Rozhodnutí 467/2007/ES, (Úř. věst. L 176, 6.7.2007, s. 25).
([3]) Úř. věst. C 68, 24.3.2007, s. 1.
([4]) Projekt „RFID a správa identity – Případové studie z počátku vývoje směrem k inteligentnímu prostředí“, zadaný orgánem Evropského parlamentu pro posuzování vědeckých a technologických a možností (STOA) a provedený evropskou skupinou pro posuzování technologií (ETAG), http://www.europarl.europa.eu/stoa/default_en.htm

— přijetí stanoviska č. 4/2007 o koncepci osobních údajů ([1]) Pracovní skupinou pro ochranu údajů zřízenou podle článku 29 v červnu roku 2007,

— sdělení Komise Evropskému parlamentu a Radě o pokračování pracovního programu pro lepší provádění směrnice o ochraně osobních údajů ([2]) a stanovisko EIOÚ k tomuto sdělení ze dne 25. července 2007 ([3]),

— přijetí ze strany Komise návrhu směrnice, kterou se mění (mimo jiné) směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací ([4]).

3. EIOÚ vítá sdělení Komise o RFID, jelikož se zabývá hlavními otázkami v souvislosti se zaváděním RFID technologie, přičemž nezanedbává otázky týkající se ochrany soukromí a údajů. Toto sdělení těží z důsledných a pečlivých přípravných prací. Komise před vypracováním tohoto sdělení zorganizovala pět tematických pracovních setkání a jednu on-line veřejnou konzultaci ([5]).

4. EIOÚ souhlasí s tím, že RFID systémy by mohly hrát klíčovou roli při rozvoji informační společnosti, která se obvykle označuje jako „internet věcí“, a rovněž zcela sdílí obavy, které jsou vyjádřeny v bodě 3.2 sdělení a týkají se toho, že RFID systémy mohou ohrozit práva jednotlivce na ochranu soukromí a údajů. Ve výroční zprávě za rok 2005 EIOÚ označil RFID, jakož i biometrické prvky, prostředí vnější inteligence a systémy správy identity za technologie, které budou mít pravděpodobně velký vliv na ochranu údajů.

5. Ke zdomácnění a obecnému přijetí RFID technologií přispěje podle EIOÚ nejen pohodlí, které tyto technologie přinesou, či nové služby, které nabízejí, ale i výhody vyplývající z dobře uzpůsobených a konzistentních záruk v oblasti ochrany údajů.

6. Krátce řečeno: EIOÚ považuje RFID za zásadní novou technologii, jež byla plným právem ve sdělení Komise označena za odrazový můstek k nové etapě rozvoje informační společnosti.

7. Tento vývoj vede k závažným otázkám v různých oblastech, přičemž jednou z těchto oblastí je ochrana údajů a soukromí. Stanovisko EIOÚ se týká pouze této oblasti.

II. **ZAMĚŘENÍ STANOVISKA**

8. Toto stanovisko je zaměřeno především na možné důsledky tohoto vývoje pro oblast ochrany údajů a soukromí. Ty jsou v současné době nejisté, a to i vzhledem k tomu, že vývoj RFID systémů a jejich zdomácnění jsou v plném proudu a že vůbec není jasné, kde se tento vývoj zastaví.

9. V tomto ohledu přijal EIOÚ následující postup:

— Zaprvé je třeba objasnit faktické důsledky, které ze zavádění RFID systémů vyplývají pro ochranu údajů a soukromí.

— Zadruhé je nutné tyto důsledky upřesnit, a to v kontextu stávajícího právního rámce pro ochranu údajů a soukromí.

— Zatřetí se EIOÚ zabývá otázkou, zda je nezbytné, aby v souvislosti s těmito důsledky byla pro řešení otázek vyplývajících z používání RFID technologií přijata konkrétnější pravidla. Tento problém, na který EIOÚ již upozornil ve stanovisku ke sdělení o směrnici o ochraně údajů, bude podrobněji rozpracován níže.

10. Tímto přístupem usiluje EIOÚ o prosazení toho, aby byly při vývoji a zdomácnění RFID systémů brány v úvahu oprávněné obavy související s ochranou údajů a soukromím.

III. **OBJASNĚNÍ DŮSLEDKŮ**

RFID systémy a tagy

11. Přestože je vývoj, jak již bylo uvedeno, v plném proudu a výsledek je nejistý, je možné hlavní rysy tohoto vývoje velmi dobře popsat z hlediska důsledků pro oblast ochrany údajů.

([1]) Dokument WP 136, zveřejněný na webových stránkách pracovní skupiny.

([2]) Sdělení Komise Evropskému parlamentu a Radě ze dne 7. března 2007 o pokračování pracovního programu pro lepší provádění směrnice o ochraně osobních údajů, KOM(2007) 87 v konečném znění.

([3]) Úř. věst. C 255, 27.10.2007, s. 1. Dále jen „stanovisko ke sdělení o směrnici o ochraně osobních údajů“.

([4]) Návrh směrnice Evropského parlamentu a Rady ze dne 13. listopadu 2007, kterou se mění směrnice 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací, směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací a nařízení (ES) č. 2006/2004 o spolupráci v oblasti ochrany spotřebitele, KOM(2007) 698 v konečném znění. Směrnice 2002/58/ES bude dále označována jako „směrnice o ochraně soukromí v odvětví elektronických komunikací“.

([5]) http://www.rfidconsultation.eu/

12. Při posuzování těch aspektů RFID technologie, které souvisejí s ochranou údajů a soukromím, je velice důležité nezabývat se pouze RFID tagy, ale celkovou RFID infrastrukturou: tagem, čtečkou, sítí, referenční databází a databází, v níž jsou ukládána data generovaná komunikací mezi tagem a čtečkou. Jak již bylo stručně uvedeno v úvodu sdělení, v případě RFID technologie nejde pouze o „elektronické tagy", a proto nebudou otázky ochrany údajů omezeny výhradně na tagy, ale budou se týkat všech částí celkové RFID infrastruktury. Každý z těchto prvků infrastruktury může přispět vlastním dílem k provedení evropského právního rámce v oblasti ochrany údajů. Na tyto prvky budou mít stimulující účinek hlavní trendy vývoje informační společnosti, jako například téměř neomezená šířka pásma, všudypřítomnost připojení k síti a neomezená kapacita skladování dat.

Dopad RFID systémů a tagů

13. Přestože je zapotřebí širšího přístupu, jak bylo zdůrazněno v předchozím odstavci, existuje několik důvodů pro to, aby byla pozornost věnována především využívání RFID technologie při označování výrobků spotřebního zboží RFID tagy, jako například v odvětví maloobchodu. Zcela zřejmým důvodem je předpokládané větší využití, u něhož se zdá, že povede k obecně rozšířeným aplikacím. Ve srovnání s dalšími RFID aplikacemi, které jsou využívány méně nebo v omezené míře, se označování jednotlivých výrobků RFID tagy může stát masovou tržní aplikací. Již v současné době je mnoho spotřebních výrobků vybaveno RFID tagy. S tím souvisí skutečnost, že toto využití se bude týkat velkého množství osob, u nichž dojde ke zpracování osobních údajů pravděpodobně při každém nákupu výrobku se zabudovaných RFID tagem.

14. Zvláštní pozornost by měla být věnována důsledkům, které z označování RFID tagy vyplývají pro majitele jednotlivých výrobků. RFID systémy by mohly rozšířit vzájemné vazby mezi výrobkem a jeho majitelem. Jakmile dojde k rozšíření těchto vazeb, mohou být majitelé za účelem budoucích transakcí snímáni a zařazováni do kategorií jako „málo finančních prostředků" nebo „lákavý cíl", přičemž příliš konkrétní vazby ([1]) by mohly vést k automatickému „trestání" určitého chování (povinnosti související s recyklací, odpady atd.). Jednotlivci by neměli být podrobeni postupu automatizovaného rozhodnutí s nepříznivými právními důsledky. Riziko, že nastane situace, kdy v informační společnosti budou přijímána automatizovaná rozhodnutí a technologie budou zneužívány s cílem usměrňovat chování lidí, se vzhledem k možnostem RFID technologie zvyšuje.

15. U údajů uložených v RFID tagu nebo u jím generovaných údajů se může jednat o osobní údaje, jak jsou vymezeny v článku 2 směrnice o ochraně údajů. Například čipové karty používané v dopravě mohou obsahovat informace umožňující identifikaci, jakož i informace o cestách, které držitel karty v poslední době uskutečnil. Pokud by nějaká bezohledná osoba chtěla držitele karet sledovat, stačilo by strategicky umístit čtečky, které by poskytly informace o jejich pohybu, čímž by došlo k porušení jejich soukromí a ochrany osobních údajů.

16. K podobnému ohrožení soukromí by mohlo dojít, pokud by informace uložené v RFID tagu zahrnovaly jména osob. RFID tagy obsahují jednoznačný identifikátory, které přísluší spotřebním výrobkům: pokud má každý tag takový jednoznačný identifikátor, mohla by být identifikace prostřednictvím tohoto tagu využívána ke sledování. Pokud například někdo nosí hodinky s RFID tagem obsahujícím určité identifikační číslo, mohlo by toto číslo být považováno za jednoznačný identifikátor nositele hodinek, a to i když je totožnost nositele neznámá. Podle toho, jakým způsobem jsou informace využívány a propojeny s hodinkami nebo jejich nositelem, by se směrnice mohla či nemohla použít. Použila by se například, kdyby u informací o tom, kde se jednotlivci právě pohybují, existovala pravděpodobnost, že budou použity pro sledování jejich chování, nebo kdyby byly informace využívány pro účely cenového rozlišení, odepření přístupu nebo nevyžádané reklamy.

17. V této souvislosti je třeba zajistit, aby RFID aplikace byly zaváděny spolu s nezbytnými technologickými opatřeními, jejichž účelem bude minimalizovat riziko poskytování informací bez vědomí subjektu údajů. Mezi tato opatření může patřit požadavek, aby RFID infrastruktura, a především RFID tagy, byly navrženy tak, aby k ničemu takovému nedocházelo. RFID tagy by například mohly být zaváděny spolu s „likvidační funkcí", která by umožnila jejich deaktivaci. Tato možnost bude dále rozpracována v kapitole IV tohoto stanoviska.

18. V rámci diskuze o ochraně soukromí se objevují nové otázky související se skutečností, že RFID systémy umožňují sledovat výrobky i mimo místo prodeje. Při analýze dopadu těchto systémů budou tedy muset být zohledněny dva prvky: nakolik je výrobek považován za „spojený" s konkrétní osobou a mobilita výrobku ([2]).

19. Životní cyklus předmětu by rovněž mohl být součástí potřebné analýzy rizik a přispět ke kvantitativnímu posouzení možných hrozeb týkajících se soukromí. Vzhledem k tomu, že tag nemůže být deaktivován, u spotřebitelských výrobků s dlouhým životním cyklem bude možné shromáždit o majiteli výrobku značné množství údajů, které umožní vytvořit o majiteli velmi přesný profil. Naproti tomu u výrobků s krátkým životním cyklem, jako například u perlivé vody v plechovce, existuje v jednotlivých fázích od výroby až po recyklaci méně rizik, a mohla by být proto vyžadována méně přísná opatření než u výrobků s mnohem delším životním cyklem.

([1]) Dr. Sarah Spiekermannová, ředitelka berlínského Centra pro výzkum ekonomiky internetu (Berlin Research Centre on Internet Economics), odborný seminář o RFID a všudypřítomné výpočetní technice organizovaný fórem Transatlantický dialog spotřebitelů (TACD), 13. března 2007.

([2]) Dara J. Glasser, Kenneth W. Goodman a Norman G. Einspruch, Chips, tags and scanners: Ethical challenges for radio frequency identification (Čipy, tagy a skenery: etické problémy identifikace na základě rádiové frekvence), Ethics and Information Technology, ročník 9, č. 2/2007.

Otázky ochrany soukromí a údajů související se zaváděním RFID systému

20. Pro účely lepšího pochopení důsledků RFID systémů pro ochranu soukromí a údajů lze rozlišovat mezi pěti základními otázkami týkajícími se soukromí a bezpečnosti.

21. První otázkou je identifikace subjektu údajů. Před více než šedesáti lety bylo účelem RFID tagu identifikovat předmět jako vlastní nebo cizí. Dnes mohou RFID systémy nejen rozpoznat, o jaký předmět se jedná, ale mohou rovněž v konečném důsledku vést k identifikaci jednotlivce, a proto je nutné, aby tato identifikace probíhala v souladu s pravidly pro ochranu údajů.

22. Druhou otázkou je určení správce či správců. V případě RFID systémů může být určení správce uvedeného v článku 2 směrnice o ochraně údajů obtížnější, a vyžaduje proto důkladnější posouzení. I nadále však platí, že určení správce je velmi důležitý krok při stanovování odpovědnosti všech příslušných aktérů, kteří budou muset dodržovat právní rámec pro ochranu údajů. Během životního cyklu tagu by mohlo několikrát dojít ke změně správce údajů, a to na základě dodatečných služeb, které mohou být poskytovány v souvislosti s předmětem, který je označen tagem.

23. Třetí otázkou je oslabení významu tradičního rozlišování mezi osobní a veřejnou sférou. I když ani v minulosti nebylo rozlišování mezi osobní a veřejnou sférou vždy jednoznačné, většina lidí si byla vědoma hranic mezi nimi (a přechodných zón), a jejich rozhodnutí tak byla informovaná a intuitivní. Podle Halla ([1]) je osobní prostor obvykle vyjádřen fyzickou vzdáleností od ostatních. Správa osobních údajů může být rovněž považována za dynamický proces, při němž dochází k posouvání hranic ([2]). Vzhledem k tomu, že se v případě tagů jedná o bezdrátovou komunikaci, přičemž informace z tagu je možno přečíst na zařízení mimo tag, není překvapující, že dochází ke stírání těchto tradičních hranic a jejich posuzování a že se objevují obavy související s ochranou soukromí. Existují obavy, že by jednotlivci mohli přijít o část dosavadní kontroly nad tím, co se děje v určité fyzické vzdálenosti, nebo o veškerou tuto kontrolu. V důsledku toho se na čtecí rozsah prvních aplikací RFID systémů zaměřili ve stejné míře jak příznivci, tak odpůrci těchto systémů.

24. Čtvrtá otázka se týká velikosti a fyzických vlastností RFID tagů. Vzhledem k tomu, že tagy musí být v zásadě malé a levné, budou bezpečnostní opatření, která by se mohla pro tuto složku RFID systému použít, a priori omezená. Jelikož však bezdrátový aspekt komunikace ve srovnání s komunikací pomocí kabelu přináší další skupinu rizik, jsou dodatečná bezpečnostní opatření nezbytná.

25. Pátou otázkou je nedostatek transparentnosti při zpracování. RFID systémy mohou vést k tomu, že bez vědomí jednotlivců bude docházet ke shromažďování a zpracovávání informací, jež by mohly být využívány k vytváření profilu těchto jednotlivců. Tento důsledek lze velmi dobře doložit při poměrně častém srovnávání RFID systémů s mobilními telefony. Na jedné straně byla technologie mobilních telefonů velmi dobře přijímána, a to nezávisle na potenciálních rizicích narušení soukromí. Z toho by mohlo vyplývat, že RFID bude přijímána stejným způsobem. Na druhé straně je třeba zdůraznit, že mobilní telefon je viditelný předmět, který je stále pod kontrolou uživatele a který je možné vypnout, což není případ RFID.

26. I když výše uvedené shromažďování a zpracovávání informací bez vědomí subjektu údajů může být oprávněné, je rovněž možné a za různých okolností dokonce velmi pravděpodobné, že dochází ke shromažďování a zpracovávání neoprávněnému.

27. Vysvětlení uvedená v této kapitole vedou k následujícímu závěru. Plošné využívání RFID technologie je zcela nové a může mít zásadní dopad na naši společnost a na ochranu základních práv v naší společnosti, mezi něž patří soukromí a ochrana údajů. V důsledku RFID může dojít ke kvalitativní změně.

IV. SPECIFIKACE DŮSLEDKŮ

Úvod

28. Tato kapitola se zaměří především na dopad RFID na ochranu základních práv v naší společnosti, jako jsou soukromí a ochrana údajů. Tento dopad bude rozveden ve dvou krocích, přičemž prvním krokem bude stručný popis toho, jakou ochranu základních práv poskytuje stávající právní rámec. V druhé fázi se bude EIOÚ podrobně zabývat tím, jak plně využít stávající právní rámec. Tento cíl je uveden ve stanovisku ke sdělení o směrnici o ochraně osobních údajů jako „úplné provedení stávajících ustanovení směrnice“.

29. Východisko je tedy toto: nové technologie, jako například RFID systémy, mají jednoznačný dopad na požadavky v souvislosti s účinným právním rámcem v oblasti ochrany údajů. Potřeba účinné ochrany osobních údajů fyzických osob může rovněž vést k omezením v používání těchto nových technologií. Interakce je tedy dvoustranná: technologie ovlivňují právní předpisy a naopak ([3]).

([1]) Hall, E.T.1966. The Hidden Dimension (Skrytý rozměr). (1. vydání). Garden City, N.Y: Doubleday.

([2]) Altman, I. 1975. The Environment and Social Behaviour (Environmentální a sociální chování), Brooks/Cole Monterrey.

([3]) Viz poznámky EIOÚ z března roku 2006 ke sdělení Komise o interoperabilitě evropských databází, zveřejněné na webové stránce EIOÚ.

Ochrana základních práv

30. Ochrana základních práv na soukromí a ochranu údajů je v Evropské unii zaručena v první řadě legislativním rámcem, který je nezbytný, jelikož se zabýváme právy uznanými v článku 8 Evropské úmluvy o ochraně lidských práv a základních svobod a v článku 7 Listiny základních práv Unie. Do příslušného legislativního rámce v oblasti ochrany údajů a RFID patří v zásadě směrnice o ochraně údajů 95/46/ES a směrnice o ochraně soukromí v odvětví elektronických komunikací 2002/58/ES ([1]).

31. Obecný legislativní rámec pro ochranu údajů stanovený ve směrnici 95/46/ES se vztahuje na RFID v případech, kdy údaje zpracovávané RFID systémy spadají do definice osobních údajů. Zatímco v některých případech se u RFID aplikací jedná jednoznačně o zpracování osobních údajů spadající do oblasti působnosti směrnice o ochraně údajů, existují rovněž aplikace, u nichž nemusí být použitelnost směrnice o ochraně údajů tak zřejmá. Cílem stanoviska č. 4/2007 pracovní skupiny pro ochranu údajů zřízené podle článku 29, které se týká pojmu osobních údajů, je přispět k jasnějšímu a obecněji uznávanému chápání pojmu osobních údajů, a tím přispět k odstranění nejasností ([2]).

32. Pokud jde o směrnici o ochraně soukromí v odvětví elektronických komunikací, je situace následující: doposud není jasné, zda se tato směrnice použije v případě RFID aplikací. Z tohoto důvodu obsahuje návrh na změnu směrnice předložený Komisí dne 13. listopadu 2007 ustanovení, jehož cílem je jasně stanovit, že směrnice se použije u některých RFID aplikací. Na další RFID aplikace by se však směrnice vztahovat nemusela, jelikož se vztahuje pouze na zpracování osobních údajů v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací ve veřejných komunikačních sítích.

33. Ochrana osobních údajů může být doplněna řadou samoregulačních nástrojů (mimo legislativní rámec). Využívání těchto nástrojů je aktivně podporováno v obou směrnicích, zejména v článku 27 směrnice o ochraně údajů, který stanoví, že členské státy a Komise podporují vypracování kodexů chování, které mají přispět k řádnému provedení směrnice. Samoregulační nástroje by kromě toho mohly účinně přispět k provedení bezpečnostních opatření vyžadovaných podle článku 17 směrnice o ochraně údajů a článku 14 směrnice o ochraně soukromí v odvětví elektronických komunikací.

([1]) Bod 59 tohoto stanoviska se bude zabývat tím, zda do legislativního rámce patří i třetí směrnice, a sice směrnice Evropského parlamentu a Rady 1999/5/ES o rádiových zařízeních a telekomunikačních koncových zařízeních a vzájemném uznávání jejich shody,(Úř. věst. L 91, 7.4.1999, s. 10).

([2]) Viz mimo jiné s. 10 stanoviska uvedeného v poznámce pod čarou 5.

Úplné provedení stávajícího rámce

34. Ve stanovisku ke sdělení o směrnici o ochraně údajů je vyjmenována řada nástrojů, jež jsou pro lepší provádění směrnice k dispozici. Většina nezávazných nástrojů v uvedeném stanovisku se týká RFID, jako například výkladová nebo jiná sdělení, prosazování osvědčených postupů, používání osvědčení o dodržení zásad ochrany soukromí a auditů v oblasti ochrany soukromí prováděných třetími stranami Možností přijmout zvláštní pravidla pro RFID se bude zabývat kapitola V. Zlepšení lze však dosáhnout i ve stávajícím rámci.

Samoregulační nástroje

35. EIOÚ souhlasí s Komisí v tom, že v první fázi je třeba ponechat prostor pro samoregulaci, umožnit zainteresovaným stranám rychle vytvořit prostředí z právního hlediska vyhovující, a přispět tak k vytvoření celkově bezpečnějšího právního prostředí.

36. Očekává se, že Komise bude v konzultaci se skupinou zainteresovaných stran RFID tento proces samoregulace podporovat a vést. V této souvislosti EIOÚ vítá doporučení, které bylo oznámeno ve sdělení a u něhož se očekává, že bude obsahovat konkrétní pokyny stanovující „*zásady, kterými by se v souvislosti s používáním RFID měly řídit veřejné orgány a ostatní zúčastněné strany*“.

37. Sdělení předpokládá, že samoregulace bude mít podobu kodexu chování nebo kodexu osvědčených postupů. Podle EIOÚ by samoregulace bez ohledu na podobu měla:

— poskytovat konkrétní a praktické pokyny pro určité typy RFID aplikací, a přispět tak k souladu s právním rámcem v oblasti ochrany údajů,

— řešit konkrétní otázky a problémy, které se v oblasti ochrany údajů objevují v souvislosti s generickými RFID aplikacemi,

— přispět k jednotnému a harmonizovanému uplatňování směrnice o ochraně údajů v celé EU, a to právě v odvětví, kde se bude pravděpodobně na celoevropské úrovni využívat tentýž typ RFID aplikací,

— být uplatňována všemi příslušnými zainteresovanými stranami Nedodržování by mělo negativní (pravděpodobně finanční) důsledky.

38. EIOÚ upozorňuje na jednu otázku, kdy bude samoregulace obzvlášť užitečná. V případě RFID aplikací, u nichž probíhá zpracování osobních údajů, ukládá směrnice o ochraně osobních údajů správcům údajů řadu povinností, zejména podle článku 17 (bezpečnost zpracování) a podle článku 7 (právní důvod). Podle těchto ustanovení musí správci údajů zavést opatření, která zabrání neoprávněnému poskytování údajů. Dále pak musí zajistit, aby ke zpracování údajů, jako je například poskytování informací případně prostřednictvím čteček, docházelo pouze s případným informovaným souhlasem osoby, které se údaje týkají.

39. Tato ustanovení směrnice o ochraně osobních údajů mohou být vykládána tím způsobem, že zaváděné RFID aplikace musejí být z technického hlediska řešeny tak, aby se zabránilo rizikům nežádoucího poskytování informací nebo aby se tato rizika minimalizovala a aby se zajistilo, že ke zpracování nebo předávání údajů bude docházet pouze s případným informovaným souhlasem. Podle názoru EIOÚ bude skutečnost, že taková povinnost existuje (tj. povinnost použít nezbytné technické vybavení s cílem zabránit rizikům nežádoucího poskytování informací nebo tato rizika minimalizovat), a to i co se týče zavádění RFID aplikací, dokonce zřejmější a jasnější, pokud bude tento požadavek součástí výše uvedeného připravovaného kodexu chování nebo kodexu osvědčených postupů. Z těchto důvodů EIOÚ vřele doporučuje, aby v doporučení Komise byla směrnice o ochraně osobních údajů vykládána tak, že existuje povinnost zavádět RFID aplikace s nutnými technologickými opatřením, která zabrání nežádoucímu shromažďování nebo poskytování informací.

Nezbytnost pokynů

40. EIOÚ doporučuje, aby Komise v úzké spolupráci se skupinou odborníků pro RFID vypracovala jeden nebo několik dokumentů poskytujících jasné vodítko, jak použít stávající právní rámec v prostředí RFID. Součástí pokynů by mělo být, jak v praxi dodržet zásady stanovené ve směrnici o ochraně osobních údajů a směrnici o ochraně soukromí v odvětví elektronických komunikací. Pokud jde o celkový přístup a konkrétní obsah pokynů, předkládá EIOÚ následující návrhy.

41. V souvislosti s pokyny obsahujícími zásady pro používání RFID je zapotřebí dostatečného zaměření a individuálního odvětvového přístupu. Univerzální přístup by nevyhovoval požadovanému účelu, kterým je zajistit jasný a soudržný rámec. Rozsah pokynů by měl být spíše omezen na dobře vymezené RFID odvětvové aplikace.

42. Kromě toho by pokyny měly obsahovat praktické a účinné metody pro vypracování *technik a standardů*, které by mohly přispět k tomu, že RFID systémy budou v souladu s právním rámcem v oblasti ochrany údajů, a z nichž bude vyplývat používání technologií v souladu se zásadou „soukromí coby aspekt návrhu".

43. Při použití stávajícího právního rámce v prostředí RFID musí být zvláštní pozornost věnována uplatnění zásad a závazků, jež souvisejí s ochranou údajů a vztahují se na správce údajů u aplikací RFID. Zvláště důležité jsou tyto závazky a zásady:

— zásada práva na informace, včetně práva vědět, kdy dochází ke shromažďování údajů prostřednictvím čteček a ve vhodných případech rovněž, že výrobky jsou vybaveny tagem,

— zásada, že souhlas je jedním z právních předpokladů zpracování údajů. Tato zásada se uplatňuje prostřednictvím povinnosti deaktivovat RFID tagy v místě prodeje, pokud subjekt údajů nevyslovil souhlas ([1]). Právo, aby RFID tagy byly deaktivovány, má rovněž zajistit bezpečnost informací, tj. zajistit, aby nedocházelo k nežádoucímu poskytování údajů zpracovávaných prostřednictvím RFID tagů třetím stranám,

— právo, aby jednotlivci nebyli podrobováni rozhodnutím s nepříznivými právními důsledky výhradně na základě automatizovaného zpracování předem stanoveného osobního profilu.

44. Co se týče práva na informace, pokyny by měly stanovit, že jednotlivcům musí být poskytovány informace týkající se zpracování jejich osobních údajů. Mimo jiné by měli být upozorněni především na i) přítomnost čteček a přítomnost aktivovaných RFID tagů umístěných na výrobcích nebo jejich obalech; ii) důsledky přítomnosti čteček a tagů z hlediska shromažďování informací a iii) zamýšlené účely využití shromážděných informací.

45. Vhodným opatřením pro poskytování těchto informací by mohlo být používání log. Loga by mohla být používána s cílem upozornit na přítomnost čteček a RFID tagů, u nichž se předpokládá, že nebudou deaktivovány. Samotné používání log však nebude dostatečné z hlediska zajištění korektního zpracování údajů, které vyžaduje, aby informace byly subjektům údajů poskytovány jasným a srozumitelným způsobem. Používání log by mělo být považováno za doplňující opatření při poskytování podrobnějších informací.

([1]) Viz podrobněji body 46 až 50 tohoto stanoviska.

Základ: zásada „opt-in“ (zásada výslovného souhlasu)

46. U řešení týkajících se všech příslušných RFID aplikací by měla být jako nezbytný předpoklad dodržována a uplatňována zásada „opt-in“ v místě prodeje. Umožnit, aby k předávání informací prostřednictvím RFID tagů docházelo i poté, co výrobek opustí místo prodeje, by bylo nezákonné, pokud ovšem správce údajů nemá pro takové opatření vhodné právní důvody. O vhodných právních důvodech lze obvykle hovořit pouze v případě a) souhlasu subjektu údajů nebo b) v případě, že je předání informací nezbytné pro poskytnutí služby, a to na zvláštní a bezplatnou žádost dotyčné osoby ([1]). V obou případech by se jednalo o zásadu „opt-in“.

47. Podle zásady „opt-in“ by tagy měly být deaktivovány v místě prodeje, ledaže by osoba, která výrobek s tagem zakoupila, trvala na tom, aby byl ponechán aktivní. Právo ponechat tag aktivní by dotyčné osobě umožnilo vyjádřit souhlas s dalším zpracováním údajů, a to například s komunikací údajů čtečce při příštím kontaktu se správcem údajů.

48. EIOÚ zdůrazňuje, že je důležitý flexibilní přístup, aby bylo možné zvládnout narůstající různorodost RFID aplikací a usnadnit vývoj nových obchodních modelů. Flexibilita je nutná, pokud jde o uplatňování zásady „opt-in“.

49. Možností pro uplatnění zásady „opt-in“ je několik. Alternativou k odstranění tagu by například mohlo být blokování tagu, dočasné vyřazení tagu z provozu nebo zablokování pro používání pouze jedním konkrétním uživatelem podle modelu, který je uplatňován v oblasti zabezpečení a označován jako „resurrecting duckling model“ ([2]). U tagů s krátkým životním cyklem by se mohly z referenční databáze vymazávat adresy tagů umožňující přesně určit informace uložené v určité databázi, čímž by se zabránilo dalšímu zpracování doplňujících údajů shromážděných tagem.

50. EIOÚ tedy uvádí, že zásada „opt-in“ v místě prodeje je právní povinností, která je v souladu se směrnicí o ochraně údajů již dodržována ve většině situací, zároveň se však domnívá, že by bylo užitečné, aby samoregulační nástroje tuto povinnost výslovně uváděly, a to i s cílem zajistit, aby byla zásada „opt-in“ uplatňována nejvhodnějším způsobem. V každém případě je třeba výslovně uvádět povinnost dodržovat zásadu „opt-in“ u RFID aplikací, které nespadají do oblasti působnosti směrnice o ochraně údajů.

([1]) U některých RFID aplikací by bylo možné uplatnit jiné právní důvody, například článek 7f (oprávněné zájmy správce, s výhradou příslušných záruk).

([2]) Autory tohoto označení jsou Frank Stajano a Ross Anderson z University of Cambridge, kteří se inspirovali „tím, jak vylíhlé house předpokládá, že první pohyblivý objekt, který vidí, musí být jeho matka“.

Nezbytnost zásady „soukromí coby aspekt návrhu“

51. S cílem minimalizovat hrozby týkající se soukromí a ochrany údajů podpořilo sdělení Komise v bodě 3.2 na straně 6 myšlenku, aby byla co nejdříve stanovována a přijímána konstrukční kritéria. EIOÚ tento přístup vítá. Stanovení a přijetí konstrukčních kritérii, označovaných jako nejlepší dostupné technologie, bude totiž přínosné pro právní úpravu ochrany údajů a bezpečnostní požadavky. Pokud budou stanovena a často přezkoumávána technologická a organizační kritéria, dojde k posílení modelu, který je v Evropské unii v současné době rozvíjen za účelem skloubení požadavků v oblasti soukromí a bezpečnosti.

52. Správné vymezení nejlepších dostupných technologií z hlediska soukromí a bezpečnosti v souvislosti s RFID systémy bude rozhodující rovněž pro vytvoření důvěryhodného prostředí, v němuž budou RFID systémy uživateli obecně přijímány, jakož i pro konkurenceschopnost evropského průmyslu.

53. Je třeba dále pracovat na tom, aby za účelem podpory procesu výběru nejlepších dostupných technologií pro RFID systémy byla prováděna rovněž posouzení dopadu z hlediska soukromí a bezpečnosti. EIOÚ se domnívá, že Evropská agentura pro bezpečnost sítí a informací (ENISA) může spolu se společnými výzkumnými středisky Evropské komise a příslušnými zainteresovanými stranami v odvětví průmyslu přispět ke stanovení osvědčených postupů a vypracování vhodných metodik. Projekt, který byl nedávno zahájen německým Federálním úřadem pro bezpečnost informačních systémů a který se týká technických pokynů pro RFID, je názorným příkladem ([3]) nejlepší dostupné technologie, která by měla být nyní rozvíjena na evropské úrovni

54. Rozhodující roli při včasném přijetí zásady „soukromí coby aspekt návrhu“ mohou sehrát rovněž standardy. Komise by se tedy měla podílet na přijetí záruk v oblasti soukromí a ochrany údajů při vypracovávání mezinárodních standardů v souvislosti s RFID. Pracovní skupina pro ochranu údajů zřízená podle článku 29 ve svém pracovním dokumentu ([4]) o RFID uvedla řadu příkladů, kdy standardy mohou přispět k vývoji RFID systémů, které nebudou představovat ohrožení soukromí.

([3]) http://www.bsi.bund.de/veranst/rfid/index.htm

([4]) Pracovní dokument (WP 105) týkající se otázek ochrany údajů v souvislosti s RFID technologií, 19. ledna 2005.

55. EIOÚ rovněž vítá postoj Komise ohledně výzkumu a vývoje RFID technologií a nutnosti omezit rizika týkající se soukromí. Zásada „soukromí coby aspekt návrhu“ musí být totiž zavedena co nejdříve během vývoje technologií, což přispěje k tomu, že tyto technologie budou v souladu s právním rámcem pro ochranu údajů. EIOÚ ve své výroční zprávě za rok 2006 uvedl, že se do práce na této otázce zapojí a bude poskytovat stanoviska a poradenství k jednotlivým projektům sedmého rámcového programu (2007–2013).

V. **JSOU ZVLÁŠTNÍ LEGISLATIVNÍ OPATŘENÍ POTŘEBNÁ?**

56. Samoregulace nemusí být dostatečným prostředkem pro provedení stávajícího rámce v oblasti ochrany údajů a soukromí. Samoregulace sice splňuje požadavky uvedené výše, její použití je však dobrovolné a v případě nedodržení nemohou být vždy účinně uplatněny sankce. Za účelem zajištění ochrany práv jednotlivce v oblasti soukromí a ochrany údajů mohou tedy být potřebná další závazná legislativní opatření. To platí především v případech, kdy samoregulační přístup nebude dostatečně efektivní.

57. Klíčovou otázkou je stanovit nezbytné právní nástroje, aby se zajistilo, že zaváděné RFID aplikace budou z technického hlediska řešeny tak, aby se zabránilo rizikům nežádoucího poskytování informací nebo aby se tato rizika minimalizovala, a že odpovědní správci údajů budou přijímat vhodná opatření v souladu s povinnostmi stanovenými podle stávajících právních předpisů. To vede k některým dalším otázkám:

— Jsou zvláštní opatření nutná?

— Pokud ano, mohou být tato pravidla přijímána v rámci stávajícího právního rámce, například prostřednictvím stávajících postupů projednávání ve výborech?

— Nebo je pro zajištění účinného zavádění RFID aplikací na základě technologií zvyšujících ochranu soukromí nutný nový legislativní nástroj?

58. Tato kapitola se bude zabývat možnostmi přijímání závazných legislativní opatření v rámci stávajícího legislativního rámce, zatímco v kapitole VI bude zvlášť posouzena otázka nezbytnosti nového legislativního nástroje.

59. V první řadě je třeba věnovat zvláštní pozornost ustanovením článku 17 směrnice 95/46/ES, čl. 14 odst. 3 směrnice 2002/58/ES a čl. 3 odst. 3 písm. c) směrnice 1999/5/ES. Podle čl. 14 odst. 3 mohou členské státy přijímat opatření, aby bylo zajištěno, že koncové zařízení je sestrojeno tak, že odpovídá právu uživatelů na ochranu a kontrolu využití jejich osobních údajů v souladu se směrnicí 1999/5/ES ([1]). V čl. 3 odst. 3 písm. c) směrnice 1999/5/ES je stanoveno, že Komise může postupem projednávání ve výborech rozhodnout, aby přístroje v určitých třídách zařízení nebo přístroje určitých typů byly konstruovány takovým způsobem, aby byly vybaveny bezpečnostním zařízením zajišťujícím ochranu osobních údajů a soukromí uživatele a účastníka. Až dosud se čl. 3 odst. 3 písm. c) směrnice 1999/ES nepoužil.

60. Na základě těchto ustanovení mají legislativní orgány na vnitrostátní úrovni i na úrovni Společenství pravomoc stanovit, že RFID systémy budou konstruovány tak, aby obsahovaly bezpečnostní zařízení pro ochranu soukromí a údajů, což je označováno jako „soukromí coby aspekt návrhu“ ([2]). Tento přístup zahrnuje rovněž využívání nejlepších dostupných technologií.

61. Aby bylo „soukromí aspektem každého návrhu“, EIOÚ doporučuje, aby Komise využívala mechanismu podle čl. 3 odst. 3 písm. c) směrnice 1999/5/ES, v konzultaci se skupinou odborníků pro RFID.

62. Dále je pak změnou uvedených směrnic možné stanovit, že bude stávající legislativní rámec uplatňován v případě RFID. Jak již bylo uvedeno, Komise nedávno předložila návrh na změnu směrnice o ochraně soukromí v odvětví elektronických komunikací, který v tomto ohledu obsahuje nové ustanovení. EIOÚ vítá, že bylo poprvé potvrzeno, že směrnice se použije i v případě RFID aplikací. EIOÚ se konkrétními otázkami vyplývajícími ze vztahu mezi směrnicí o ochraně soukromí v odvětví elektronických komunikací a RFID bude zabývat ve stanovisku k návrhu na změnu směrnice, které bude vydáno na začátku roku 2008.

63. Vzhledem k tomu, že Komise nemá v úmyslu předložit v dohledné době návrh na změnu směrnice o ochraně údajů ([3]), jsou možnosti stanovit použití stávajícího legislativního rámce v případě RFID omezené.

VI. **JE PRO RFID POTŘEBNÝ ZVLÁŠTNÍ LEGISLATIVNÍ RÁMEC?**

Záměry Komise

64. Ve sdělení ([4]) je zdůrazněn význam bezpečnosti a zásady „soukromí coby aspekt návrhu“. Uvádí se rovněž, že je nutné zapojení všech zainteresovaných stran. Hlavním

([1]) A v souladu s rozhodnutím Rady 87/95/EHS ze dne 22. prosince 1986 o normalizaci v oblasti informačních technologií a telekomunikací (Úř. věst. L 36, 7.2.1987, s. 31).
([2]) Viz kapitola IV.
([3]) EIOÚ tento přístup podporuje, viz bod 64.
([4]) Viz bod 4.1 sdělení.

výsledkem činností Komise bude „*doporučení, v němž představí zásady, kterými by se v souvislosti s používáním RFID měly řídit veřejné orgány a ostatní zúčastněné strany*“. Doporučení bude přijato pravděpodobně na jaře roku 2008. Legislativní cíle obsažené ve sdělení zahrnují následující dva kroky.

— Komise posoudí příslušná ustanovení o RFID obsažená v připravovaném návrhu na změnu směrnice o ochraně soukromí v odvětví elektronických komunikací. Jak již bylo uvedeno, Komise v listopadu roku 2007 předložila návrh na změnu směrnice o ochraně soukromí v odvětví elektronických komunikací, v němž potvrdila použitelnost směrnice u RFID aplikací ([1]), ale nenavrhla rozšíření její působnosti na soukromé sítě,

— Komise vyhodnotí, zda jsou další legislativní kroky k zajištění ochrany údajů a soukromí nezbytné.

65. V souladu s tímto přístupem lze očekávat, že Komise přinejmenším v krátkodobém horizontu nemá v úmyslu předložit návrh zvláštních právních předpisů k zajištění ochrany údajů a soukromí v oblasti RFID.

Parametry pro legislativní orgán

66. Ve svém stanovisku ke sdělení o směrnici o ochraně údajů nastínil EIOÚ některé aspekty legislativní činnosti související se zpracováním osobních údajů, jež je možno shrnout následujícím způsobem:

— Zaprvé je třeba dodržovat hlavní zásady ochrany údajů: „*Nejsou zapotřebí nové zásady, jsou však nepochybně zapotřebí jiná správní ujednání, která by na jedné straně byla účinná a vhodná pro sítěmi propojenou společnost a na druhé straně minimalizovala správní náklady*“ ([2]).

— Zadruhé legislativní návrhy by měly být předkládány, jeli dostatečně prokázána nezbytnost a přiměřenost. Proto by se krátkodobě neměl měnit obecný legislativní rámec pro ochranu údajů.

— Zatřetí změny vyplývající z vývoje ve společnosti mohou mít za následek zvláštní právní předpisy, jejichž cílem bude upravit zásady směrnice o ochraně údajů podle problémů vzniklých u specifických technologií, jako je RFID. Je zřejmé, že i v této souvislosti je třeba splnit podmínky nezbytnosti a přiměřenosti.

67. Jako další krok je užitečné specifikovat očekávání, s nimiž se musí legislativní orgán v oblasti RFID vyrovnat:

— Právní předpisy musí být flexibilní a musí ponechat prostor pro inovace a technologický rozvoj. To by mělo vést k právním předpisům, jež jsou z hlediska technologií dostatečně neutrální.

— Zadruhé je třeba, aby právní předpisy poskytly právní jistotu. To by mělo vést k právním předpisům, jež jsou dostatečně specifické. Zainteresované strany musí přesně vědět, jak je jejich chování regulováno.

— Zatřetí, právní předpisy musí účinně chránit všechny oprávněné příslušné zájmy. To v každém případě vyžaduje prosazování právních předpisů a jasné vymezení odpovědnosti zúčastněných stran. ([3]). Nutnost respektovat tyto požadavky je zřejmá zejména s ohledem na ochranu soukromí a ochranu údajů, základní práva osob podle Evropské úmluvy lidských práv a základních svobod a Listiny základních práv Evropské unie.

Stanovisko EIOÚ

68. Pro EIOÚ je zřejmé, že by evropský legislativní orgán neměl reagovat na všechny nové technologie. Vývoj nových technologií může postupovat rychle, zatímco přijímání právních předpisů a jejich vstup v platnost postupuje a mělo by postupovat pomalu. Právní předpis by měl být výsledkem vyváženosti všech příslušných zájmů. Má-li být nástrojem směrnice, je třeba ještě více času, protože směrnice musí být plně provedeny v právních systémech členských států.

69. Avšak RFID není jen další nová technologie, jak bylo zdůrazněno v několika částech tohoto stanoviska. Sdělení odkazuje k RFID jakožto k bráně k nové fázi vývoje informační společnosti, o níž se často hovoří jako o „internetu věcí“ a v níž budou RFID tagy klíčovými prvky prostředí vnější inteligence. Tato prostředí hrají důležitou roli při rozvoji toho, co se často nazývá „společností dohledu“ ([4]). S ohledem na tyto skutečnosti je možno legislativní opatření v oblasti RFID odůvodnit. V důsledku RFID může dojít ke kvalitativní změně.

([1]) Viz navrhovaný nový článek 3 směrnice 2002/58/ES.
([2]) Bod 24 stanoviska ke sdělení o směrnici o ochraně údajů.
([3]) Převedeno do terminologie ochrany údajů to znamená identifikaci „správce údajů“.
([4]) Tato myšlenka byla zopakována v prohlášení evropských orgánů pro ochranu údajů, jež bylo přijato dne 2. listopadu 2006 v Londýně a jež je k dispozici na této webové stránce: http://www.edps.europa.eu/EDPSWEB/edps/lang/en/pid/51

70. V tomto ohledu EIOÚ doporučuje zvážit přijetí (návrhu) právního předpisu Společenství upravujícího hlavní otázky použití RFID v příslušných odvětvích, pokud by selhalo řádné provádění stávajícího právního rámce. Takové právní opatření musí být po vstupu v platnost považováno za *lex specialis* ve vztahu k obecnému rámci na ochranu údajů.

71. Přijetí takového právního nástroje by mělo tyto výhody:

— Tento nástroj by mohl stanovit základní parametry pro samoregulační mechanismy.

— Možnost přijetí právního nástroje by se mohla ukázat jako účinná pobídka pro zainteresované strany ke stanovení samoregulačních mechanismů nabízejících odpovídající ochranu.

72. Komise by mohla být požádána o přípravu konzultačního dokumentu týkajícího se všech výhod a nevýhod zvláštního právního předpisu a hlavních prvků takového předpisu. Zainteresované strany by mohly být požádány o poskytnutí informací pro tuto konzultaci. Pracovní skupina pro ochranu údajů zřízená podle článku 29 by se mohla pravděpodobně rovněž zúčastnit.

Možné způsoby

73. Zásahem legislativního orgánu by mohl být stanoven právní rámec „na míru“, který sestává z kombinace regulativních nástrojů, jež specifikují a doplňují stávající právní rámec. Tento právní rámec „na míru“ by měl vycházet ze známých zásad pro ochranu údajů a měl by se zaměřit na rozdělení povinností a na účinnost kontrolních mechanismů.

74. Zvláštní důvod, proč by takový právní předpis „na míru“ byl potřeba, souvisí se skutečností, že u všech RFID aplikací neprobíhá zpracování osobních údajů. Jinak řečeno, pokud RFID aplikace nevyžadují zpracování osobních údajů, strany podílející se na výrobě a prodeji výrobků vybavených RFID tagy nejsou právně vázány provádět technologická opatření, jež by zabránila odposlechu nebo zavedení čteček bez řádného informování osob. Nicméně jak se ukázalo, riziko narušení soukromí vyplývající z možného dohledu nad osobami existuje rovněž u těchto RFID aplikací, takže je třeba stejného druhu ochrany soukromí. To může být právě případ označování spotřebního zboží tagy *dříve*, než je doručeno do místa prodeje. Souhrnně řečeno, RFID aplikace, jež nezpracovávají osobní údaje, mohou stále ještě ohrožovat soukromí osob tím, že umožňují nepovolené sledování a využití informací pro nepřijatelné účely.

75. EIOÚ se domnívá, že je třeba tomuto neblahému důsledku zabránit. Vzhledem k tomu, že stávající právní předpisy částečně – alespoň pro RFID aplikace, jež nezpracovávají osobní údaje – neupravují toto ohrožení soukromí a s ohledem na nedostatky řešení prostřednictvím právně nevynutitelných předpisů se zdá být nezbytným využít povinných legislativních opatření k zajištění uspokojivého výsledku.

76. Tato opatření by měla v každém případě:

— stanovit zásadu „opt-in“ v místě prodeje jako přesnou a nezadatelnou právní povinnost, a to rovněž pro RFID aplikace, jež nespadají do oblasti působnosti směrnice o ochraně údajů ([1]);

— zajistit povinné zavádění RFID aplikací s vhodnými technickými vlastnostmi nebo konstruovanými podle zásady „soukromí coby aspektu návrhu“.

VII. **OTÁZKA SPRÁVY**

77. Ačkoliv rozměr „inherentní přeshraničnosti“ systémů RFID je uváděn ve sdělení pouze v rámci vnitřního trhu, EIOÚ se domnívá, že tímto rozměrem je třeba se zabývat na mezinárodní úrovni. Již v obchodě jsou systémy RFID „přeshraniční“, protože tagy jsou aktivní i mimo místo prodeje. Na úrovni systému RFID jako celku se tyto technologie rovněž stanou „přeshraničními“, pokud by se přenos osobních údajů do třetí země mohl uskutečnit, protože výrobce výrobku s tagem, jenž je součástí systému RFID, je usazen mimo Evropskou unii. ([2])

78. S ohledem na budoucnost představuje správa referenční databáze totožnosti RFID kritický rozměr pro vhodné prosazování evropského právního rámce na ochranu údajů. Evropský inspektor ochrany údajů naléhavě vyzývá, aby bylo nalezeno řešení, protože další narušení tohoto právního rámce by již nebylo přijatelné.

79. EIOÚ považuje otázku správy RFID za hlavní úkol, jenž bude vyžadovat značné investice. Musí být nalezeno správné fórum pro jednání, jakož i nejvhodnější správa infrastruktury s cílem zajistit, aby byla práva na ochranu údajů v těchto mezinárodních prostředích odpovídajícím způsobem dodržována.

([1]) V kapitole IV je uvedeno, že zásada „opt-in“ v místě prodeje je právní závazek, který již existuje na základě směrnice o ochraně údajů.

([2]) Povinnosti týkající se předávání osobních údajů jsou upraveny v článcích 25 a 26 směrnice o ochraně údajů.

80. V této souvislosti EIOÚ vyzývá Komisi, aby předložila stanovisko týkající se správy, případně za konzultace skupiny zainteresovaných stran RFID.

VIII. **ZÁVĚRY**

81. EIOÚ vítá sdělení Komise o RFID, jelikož se zabývá hlavními otázkami v souvislosti se zaváděním RFID technologie, přičemž nezanedbává otázky týkající se ochrany soukromí a údajů. Souhlasí se stanoviskem, že systémy RFID by mohly hrát klíčovou úlohu při rozvoji informační společnosti, o níž se obvykle hovoří jako o „internetu věcí".

Objasnění důsledků

82. Plošné využívání RFID technologie je zcela nové a může mít zásadní dopad na naši společnost a na ochranu základních práv v naší společnosti, mezi něž patří soukromí a ochrana údajů. V důsledku RFID může dojít ke kvalitativní změně.

83. Je možno rozlišit pět základních otázek týkajících se soukromí a bezpečnosti:

— identifikace subjektu údajů,

— identifikace správce údajů či správců údajů,

— oslabení významu tradičního rozlišování mezi osobní a veřejnou sférou,

— důsledky velikosti a fyzických vlastností RFID tagů,

— nedostatek transparentnosti při zpracování.

Specifikace důsledků

84. Obecný legislativní rámec pro ochranu údajů stanovený ve směrnici 95/46/ES se vztahuje na RFID v případech, kdy údaje zpracovávané RFID systémy spadají do definice osobních údajů.

85. Pokud jde o směrnici o ochraně soukromí v odvětví elektronických komunikací: návrh na změnu směrnice předložený Komisí dne 13. listopadu 2007 obsahuje ustanovení, jehož cílem je jasně stanovit, že se tato směrnice použije u některých RFID aplikací. Na některé další RFID aplikace by se však směrnice vztahovat nemusela, jelikož se týká pouze zpracování osobních údajů v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací ve veřejných komunikačních sítích.

86. Ochrana osobních údajů může být doplněna řadou samoregulačních nástrojů. Je vhodné ponechat prostor pro takovou samoregulaci, pokud:

— poskytuje konkrétní a praktické pokyny pro určité typy RFID aplikací,

— řeší konkrétní otázky a problémy, které se v oblasti ochrany údajů objevují v souvislosti s generickými RFID aplikacemi,

— přispívá k jednotnému a harmonizovanému uplatňování směrnice o ochraně údajů v celé EU,

— je uplatňována všemi příslušnými zainteresovanými stranami.

87. EIOÚ doporučuje, aby Komise v úzké spolupráci se skupinou odborníků pro RFID vypracovala jeden nebo několik dokumentů poskytujících jasné vodítko, jak použít stávající právní rámec v prostředí RFID.

88. V souvislosti s pokyny obsahujícími zásady pro používání RFID je zapotřebí dostatečného zaměření a individuálního odvětvového přístupu. Pokyny by měly obsahovat praktické a účinné metody pro vypracování *technik a standardů*, které by mohly přispět k tomu, že RFID systémy budou v souladu s právním rámcem v oblasti ochrany údajů, a z nichž bude vyplývat používání technologií v souladu se zásadou „soukromí coby aspekt návrhu".

89. EIOÚ vítá přístup obsažený ve sdělení Komise s cílem potvrdit myšlenku stanovení a přijetí včasných konstrukčních kritérií.

90. Ačkoliv se EIOÚ domnívá, že zásada „opt-in" v místě prodeje je právní povinností, jež v souladu se směrnicí o ochraně údajů platí již ve většině situací, měly by samoregulační nástroje tuto povinnost výslovně uvádět.

Je třeba zvláštních opatření?

91. Aby bylo „soukromí aspektem každého návrhu", EIOÚ doporučuje, aby Komise využívala mechanismu podle čl. 3 odst. 3 písm. c) směrnice 99/5/ES, v konzultaci se skupinou odborníků pro RFID.

92. V tomto ohledu EIOÚ doporučuje zvážit přijetí (návrhu) právního předpisu Společenství upravujícího hlavní otázky použití RFID v příslušných odvětvích, pokud by selhalo řádné provádění stávajícího právního rámce. Takové právní opatření musí být po vstupu v platnost považováno za *lex specialis* ve vztahu k obecnému rámci na ochranu údajů. Toto právní opatření by se mělo rovněž zabývat obavami, jež vznikají v souvislosti se soukromím a ochranou údajů u některých RFID aplikací, jako je označování jednotlivých výrobků tagy dříve, než jsou doručeny do místa prodeje, což nemusí nutně zahrnovat zpracování osobních údajů.

93. Komise by měla připravit konzultační dokument týkající se všech výhod a nevýhod zvláštního právního předpisu a hlavních prvků takového předpisu.

94. Zásahem legislativního orgánu by mohl být stanoven právní rámec „na míru“, který by sestával z kombinace regulativních nástrojů, jež specifikují a doplňují stávající právní rámec. Opatření by měla v každém případě:

— stanovit zásadu „opt-in“ v místě prodeje jako přesnou a nezadatelnou právní povinnost, a to rovněž pro RFID aplikace, jež nespadají do oblasti působnosti směrnice o ochraně údajů ([1]);

— zajistit povinné zavádění RFID aplikací s vhodnými technickými vlastnostmi nebo konstruovanými podle zásady „soukromí coby aspektu návrhu“.

Otázka správy

95. V této souvislosti EIOÚ vyzývá Komisi, aby předložila stanovisko týkající se správy, případně za konzultace skupiny zainteresovaných stran RFID.

V Bruselu dne 20. prosince 2007.

Peter HUSTINX

Evropský inspektor ochrany údajů

([1]) V kapitole IV je uvedeno, že zásada „opt-in“ v místě prodeje je právní závazek, který již existuje na základě směrnice o ochraně údajů.