I

(Uznesenia, odporúčania a stanoviská)

STANOVISKÁ

EURÓPSKY DOZORNÝ ÚRADNÍK PRE OCHRANU ÚDAJOV

Stanovisko európskeho dozorného úradníka pre ochranu údajov k oznámeniu Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov o rádiofrekvenčnej identifikácii (RFID) v Európe: kroky k politickému rámcu KOM(2007) 96

(2008/C 101/01)

EURÓPSKY DOZORNÝ ÚRADNÍK PRE OCHRANU ÚDAJOV,

so zreteľom na Zmluvu o založení Európskeho spoločenstva, a najmä na jej článok 286,

so zreteľom na Chartu základných práv Európskej únie, a najmä na jej článok 8,

so zreteľom na smernicu Európskeho parlamentu a Rady 95/46/ES z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a o voľnom pohybe týchto údajov,

so zreteľom na smernicu Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002 týkajúcu sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií,

so zreteľom na nariadenie Európskeho parlamentu a Rady (ES) č. 45/2001 z 18. decembra 2000 o ochrane jednotlivcov so zreteľom na spracovanie osobných údajov inštitúciami a orgánmi Spoločenstva a o voľnom pohybe takýchto údajov, a najmä na jeho článok 41,

PRIJAL TOTO STANOVISKO:

I. ÚVOD

1. Komisia 15. marca 2007 prijala oznámenie o rádiofrekvenčnej identifikácii (RFID) v Európe: kroky k politickému rámcu ([1]) (ďalej len „oznámenie“). EDPS je podľa článku 41 nariadenia (ES) č. 45/2001 zodpovedný za poskytovanie poradenstva inštitúciám a orgánom Spoločenstva o všetkých záležitostiach, ktoré sa týkajú spracúvania osobných údajov. EDPS v súlade s uvedeným článkom predkladá toto stanovisko.

2. Toto stanovisko sa musí vnímať ako reakcia EDPS na oznámenie, ako aj iné opatrenia v oblasti RFID, ktoré sa uskutočnili od prijatia tohto oznámenia. Tieto iné relevantné opatrenia, zohľadnené v tomto stanovisku, zahŕňajú:

— rozhodnutie Komisie z 28. júna 2007, ktorým sa zriaďuje expertná skupina pre rádiofrekvenčnú identifikáciu ([2]) – priamy dôsledok oznámenia. Táto skupina je známa aj ako skupina strán zainteresovaných na RFID. EDPS sa v súlade s článkom 4 ods. 4 písm. b) rozhodnutia zúčastňuje na činnosti skupiny ako pozorovateľ,

— uznesenie Rady z 22. marca 2007 o Stratégii pre bezpečnú informačnú spoločnosť v Európe ([3]),

— projekt „RFID a riadenie identity“ iniciovaný Európskym parlamentom ([4]),

([1]) KOM(2007) 96 v konečnom znení.
([2]) Rozhodnutie 467/2007/ES (Ú. v. EÚ L 176, 6.7.2007, s. 25).
([3]) Ú. v. EÚ C 68, 24.3.2007, s. 1.
([4]) Projekt „RFID a riadenie identity – prípadové štúdie z prvej línie vývoja smerom k inteligentnému prostrediu“, ktorý zadal útvar posudzovania vedeckotechnických možností (STOA – Scientific Technology Option Assessment) Európskeho parlamentu a ktorý vykonáva ETAG (European Technology Assessment Group) http://www.europarl.europa.eu/stoa/default_en.htm

— prijatie stanoviska č. 4/2007 o koncepcii osobných údajov ([1]) pracovnou skupinou na ochranu údajov podľa článku 29 v júni 2007,

— oznámenie Komisie Európskemu parlamentu a Rade o pokračovaní pracovného programu pre lepšiu implementáciu smernice o ochrane údajov ([2]) a stanovisko EDPS k tomuto oznámeniu z 25. júla 2007 ([3]),

— prijatie návrhu smernice zo strany Komisie, ktorou sa mení a dopĺňa (okrem iného) smernica 2002/58/ES týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií ([4]).

3. EDPS víta oznámenie Komisie o RFID, keďže sa zaoberá hlavnými otázkami vznikajúcimi v kontexte zavádzania technológie RFID, a to bez toho, aby sa zanedbávali určujúce otázky súvisiace s ochranou súkromia a údajov. Prospešnou pre toto oznámenie boli konzistentné a dôsledné prípravné práce. Oznámeniu predchádzalo päť tematických pracovných seminárov ([5]), ako aj online verejná konzultácia, ktorú iniciovala Komisia.

4. EDPS súhlasí s názorom, že systémy RFID by mohli zohrávať kľúčovú úlohu v rozvoji informačnej spoločnosti obvykle označovanej ako „internet vecí“, a tiež sa celkom stotožňuje s obavami, ktoré sa uvádzajú v odseku 3.2 oznámenia, že systémy RFID môžu ohroziť práva jednotlivca na ochranu súkromia a údajov. EDPS vo svojej výročnej správe za rok 2005 identifikuje RFID spolu s biometrickými údajmi, inteligentnými prostrediami a systémami riadenia identity ako príklady technologického vývoja, v súvislosti s ktorými sa očakáva veľký dosah na ochranu údajov.

5. Podľa EDPS sa udomácnenie technológií RFID a ich široké prijatie dosiahne nielen vďaka príťažlivosti ich jednoduchého využívania alebo novým službám, ktoré ponúkajú, ale uľahčia ho aj prínosy vhodne prispôsobených a konzistentných opatrení na ochranu údajov.

6. Stručne: EDPS kvalifikuje RFID ako zásadne nový produkt technologického vývoja, na ktorý Komisia v oznámení správne poukazuje ako na vstupnú bránu do novej etapy rozvoja informačnej spoločnosti.

7. Tento vývoj prináša dôležité otázky v rôznych oblastiach, z ktorých jednou je oblasť ochrany údajov a súkromia. Toto stanovisko EDPS sa obmedzuje práve na túto oblasť.

II. **ZAMERANIE STANOVISKA**

8. Toto stanovisko sa zameriava najmä na možné dôsledky uvedeného vývoja na ochranu údajov a súkromia. Tieto dosahy sú v danej chvíli neurčité a sú ovplyvnené aj tým faktom, že naplno pokračuje vývoj systémov RFID a ich udomácňovanie a vôbec nie je jasné, ako tento vývoj skončí.

9. Z tohto pohľadu EDPS zaujíma nasledujúci prístup:

— po prvé, je potrebné vyjasniť praktické dôsledky zavádzania systémov RFID na ochranu údajov a súkromia,

— po druhé, je potrebné tieto dôsledky špecifikovať v kontexte existujúceho právneho rámca pre ochranu údajov a súkromia,

— po tretie, EDPS sa zaoberá otázkou, či si tieto dôsledky vyžadujú špecifickejšie pravidlá zamerané na riešenie otázok súvisiacich s ochranou údajov, ktoré vyplývajú z využívania technológií RFID. Túto otázku už EDPS nastolil vo svojom stanovisku k oznámeniu o smernici o ochrane údajov a rozvinie ju v tomto stanovisku.

10. Cieľom EDPS je prostredníctvom tohto prístupu podporiť, aby vývoj systémov RFID a ich udomácňovanie zohľadňovali oprávnené obavy súvisiace s ochranou údajov a súkromia.

III. **VYJASNENIE DÔSLEDKOV**

Systémy a štítky RFID

11. Napriek skutočnosti, že – ako bolo povedané – vývoj naplno napreduje a výsledok je neurčitý, je možné veľmi dobre opísať hlavné charakteristiky tohto vývoja so zreteľom na ich dôsledky vo vzťahu k ochrane údajov.

([1]) Dokument WP 136 zverejnený na webovej stránke pracovnej skupiny.
([2]) Oznámenie Komisie Európskemu parlamentu a Rade zo 7. marca 2007 o pokračovaní pracovného programu pre lepšiu implementáciu smernice o ochrane údajov, KOM(2007) 87 v konečnom znení.
([3]) Ú. v. EÚ C 255, 27.10.2007, s. 1. Ďalej len „stanovisko k oznámeniu o smernici o ochrane údajov“.
([4]) Návrh z 13. novembra 2007 smernice Európskeho parlamentu a Rady, ktorou sa mení a dopĺňa smernica 2002/22/ES o univerzálnej službe a právach užívateľov týkajúcich sa elektronických komunikačných sietí a služieb, smernica 2002/58/ES týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií, smernica Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002 týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií, nariadenie (ES) č. 2006/2004 o spolupráci v oblasti ochrany spotrebiteľa, KOM(2007) 698 v konečnom znení. Na smernicu 2002/58/ES sa odkazuje ako na „smernicu o elektronickom súkromí“.
([5]) http://www.rfidconsultation.eu/

12. Pri posudzovaní možných aspektov ochrany údajov a súkromia v súvislosti s technológiou RFID je veľmi dôležité brať do úvahy nielen samotné štítky RFID, ale celkovú infraštruktúru RFID: štítok, čítačku, sieť, referenčnú databázu a databázu, v ktorej sa uchovávajú údaje vyplývajúce z komunikácie medzi štítkom a čítačkou. Ako sa stručne zdôrazňuje v úvode oznámenia, RFID nie sú iba „elektronické štítky“, a preto sa otázky ochrany údajov nebudú obmedzovať výlučne na štítky, ale budú sa týkať všetkých častí celkovej infraštruktúry RFID. Každý z týchto prvkov zohráva nejakú úlohu, ktorou prispieva k vykonávaniu európskeho právneho rámca na ochranu údajov, ak sa to vyžaduje. Ich vývoj budú podporovať hlavné trendy v rozvoji informačnej spoločnosti, ako napríklad takmer neobmedzený rozsah pásma, všadeprítomné sieťové pripojenia a neobmedzená kapacita pamäte.

Vplyv systémov a štítkov RFID

13. Bez ohľadu na potrebu širšieho prístupu, ako sa zdôrazňuje v prechádzajúcom odseku, je z rôznych dôvodov opodstatnené zamerať sa najprv na využívanie RFID v označovaní štítkami na úrovni jednotlivých výrobkov, pokiaľ ide o spotrebiteľské výrobky v maloobchodnom sektore. Jedným zo zrejmých dôvodov je očakávané zvýšené využívania RFID, ktoré, ako sa zdá, smeruje k širokému uplatňovaniu. V porovnaní s inými uplatneniami RFID, ktoré majú úzke alebo obmedzené využitie, má označovanie štítkami na úrovni jednotlivých výrobkov potenciál masového uplatňovania na trhu. Už teraz je veľa spotrebiteľských výrobkov vybavených štítkom RFID. S tým súvisí fakt, že takéto využívanie ovplyvní obrovský počet jednotlivcov, ktorých osobné údaje sa budú pravdepodobne spracovávať vždy, keď nadobudnú výrobok, ktorého súčasťou je štítok RFID.

14. Osobitná pozornosť by sa mala venovať dôsledkom označovania štítkami RFID pre majiteľov konkrétnych výrobkov. Systémy RFID by mohli rozšíriť vzťah medzi výrobkom a jej majiteľom. Keď sa tento vzťah rozšíri, majiteľa možno sledovať a zatriediť ako „nízkobonitného“ alebo ako „zaujímavý cieľ“ z hľadiska budúcich transakcií; rozsiahle individuálne priraďovanie (položka – majiteľ) ([1]) môže viesť k automatickému „potrestaniu“ určitého správania (povinnosť recyklácie, odpad atď.). Jednotlivci by nemali byť vystavení procesu automatizovaných nepriaznivých rozhodnutí. Touto schopnosťou RFID urýchľuje zvyšovanie rizika, že sa informačná spoločnosť priblíži k situácii, keď sa budú prijímať automatizované rozhodnutia a keď sa technológia bude zneužívať s cieľom regulovať správanie človeka.

15. Údaje, ktoré sa uchovávajú na štítkoch RFID alebo ktoré štítky RFID produkujú, môžu byť osobnými údajmi, ako ich vymedzuje článok 2 smernice o ochrane údajov. Napríklad čipové karty používané na cestovanie môžu obsahovať identifikačné informácie aj informácie o nedávnych cestách ich držiteľa. Ak by bezohľadný jednotlivec chcel sledovať fyzické osoby, stačilo by strategicky umiestniť čítačky, ktoré by poskytli informácie o pohyboch držiteľa karty, čím by došlo k narušeniu súkromia a ochrany osobných informácií.

16. Podobne môže byť súkromie ohrozené, aj keby informácie uložené na štítku RFID neobsahovali mená jednotlivcov. Štítky RFID obsahujú jedinečné identifikačné číslo (ID) priradené zákazníkovým výrobkom: ak má každý štítok jedinečné identifikačné číslo, potom sa takáto identifikácia môže využívať na účely sledovania. Ak napríklad niekto nosí hodinky, ktoré majú štítok RDIF obsahujúci identifikačné číslo, mohlo by to slúžiť aj ako jedinečný identifikátor osoby, ktorá nosí hodinky, aj keď jej totožnosť nie je známa. Podľa toho, ako sa tieto informácie využívajú – a ako sa dávajú do súvislosti so samotnými hodinkami alebo osobou – by sa smernica na situáciu vzťahovala alebo nevzťahovala. Vzťahovala by sa napríklad vtedy, ak by sa generovali informácie o miestach pobytu jednotlivcov, ktoré by sa pravdepodobne využívali na monitorovanie ich správania, alebo napríklad na individuálne určovanie cien, zamietnutie prístupu alebo neželané zverejnenie.

17. V tomto kontexte je nevyhnutné zabezpečiť, aby sa aplikácie RFID zavádzali s potrebnými technickými opatreniami na minimalizovanie rizika neželaného zverejnenia informácií. Takéto opatrenia môžu zahŕňať požiadavku navrhovať infraštruktúru RFID, najmä štítky RFID, tak, aby sa zabránilo takýmto dôsledkom. Štítky RFID sa napríklad môžu zaviesť s „príkazom na ukončenie“, ktorý umožňuje ich deaktiváciu. Táto možnosť sa ďalej preberie v kapitole IV tohto stanoviska.

18. Tým, že systémy RFID ponúkajú možnosti vystopovať výrobky po tom, čo opustia miesto predaja, vnášajú do diskusie o súkromí nové otázky. Pri analýze vplyvu týchto systémov sa budú musieť zohľadniť dva prvky: za nakoľko osobný sa výrobok považuje a mobilita výrobku ([2]).

19. Aj životný cyklus objektu môže doplniť požadovanú analýzu rizika a prispieť ku kvantitatívnemu posúdeniu potenciálnych hrozieb týkajúcich sa súkromia. Ak sa vezme do úvahy skutočnosť, že štítok nemožno deaktivovať, výrobok pre koncového používateľa s dlhou životnosťou bude môcť od majiteľa výrobku zhromaždiť viac súvisiacich údajov a zostaviť presnejší profil. Na druhej strane krátky životný cyklus výrobku, ako napríklad plechovky s nápojom, môže predstavovať od jej výroby až po jej recykláciu menšie riziká a mohol by si preto vyžadovať miernejšie opatrenia, než výrobok s oveľa dlhším životným cyklom.

([1]) Dr. Sarah Spiekermannová, riaditeľka Výskumného strediska pre ekonomiku internetu v Berlíne (Berlin Research Centre on Internet Economics), pracovný seminár o RFID a všadeprítomných počítačových systémoch, ktorý organizoval Transatlantický spotrebiteľský dialóg 13. marca 2007.

([2]) Dara J. Glasser, Kenneth W. Goodman a Norman G. Einspruch, Čipy, štítky a skenery: etické výzvy pre rádiofrekvenčnú identifikáciu, Etika a informačná technológia, zväzok 9, č. 2/2007.

Otázky ochrany súkromia a údajov pri zavádzaní systémov RFID

20. S cieľom lepšie porozumieť vplyvu systémov RFID na ochranu súkromia a údajov je možné rozlíšiť päť základných otázok súkromia a bezpečnosti.

21. Prvou otázkou je identifikácia dotknutej osoby. Pred viac ako šesťdesiatimi rokmi bolo účelom štítku RFID „identifikovať prichádzajúceho priateľa alebo nepriateľa“. Dnes dokážu systémy RFID nielen identifikovať všeobecné prvky objektu, ale viesť v konečnom dôsledku aj k identifikácii jednotlivca, a preto je potrebné, aby to vykonávali spôsobom, ktorý rešpektuje ochranu údajov.

22. Druhou otázkou je identifikácia kontrolóra/kontrolórov. V prípade systémov RFID môže byť identifikácia kontrolóra, ako sa vymedzuje v článku 2 písm. d) smernice o ochrane údajov, oveľa ťažšia, a preto si vyžaduje bližšie preskúmanie. Identifikácia kontrolóra však zostáva kritickým krokom pri určovaní povinností každého z príslušných aktérov, ktorí budú musieť dodržiavať právny rámec na ochranu údajov. Počas životného cyklu štítka by sa kontrolór, ktorý spracováva údaje, mohol niekoľkokrát zmeniť na základe doplnkových služieb, ktoré sa môžu poskytovať vo vzťahu k objektu označeného štítkom.

23. Treťou otázkou je znížený význam tradičného rozlišovania medzi súkromnou a verejnou sférou. Hoci rozlišovanie medzi súkromnými a verejnými priestormi nebolo ani v minulosti vždy jasne vymedzené, väčšina ľudí si hranice medzi nimi (a sivé zóny) uvedomuje a podľa toho prijíma rozhodnutia na základe informovanosti alebo intuície o tom, ako konať. Podľa Halla ([1]) sa osobný priestor obvykle premieta do fyzickej vzdialenosti od iných. Riadenie súkromia sa tiež môže považovať za proces riadenia dynamických hraníc ([2]). Preto nie je prekvapujúce, že bezdrôtová povaha komunikácie prostredníctvom štítkov ako aj to, že štítky môžu byť čítané aj keď je čítacie zariadenie mimo dohľadu, vyvolávajú obavy o súkromie, pretože zahmlievajú tieto tradičné hranice a ich riadenie. Existujú obavy, že by jednotlivec mohol čiastočne alebo celkovo stratiť kontrolu nad riadením vzdialenosti, ktorou doposiaľ disponoval. V tejto súvislosti sa na čítací dosah prvých zavedených systémov RFID zamerali rovnako ich podporovatelia ako aj odporcovia.

24. Štvrtá otázka sa musí zaoberať veľkosťou a fyzickými vlastnosťami štítkov RFID. Keďže je potrebné, aby štítky boli v zásade malé a lacné, bezpečnostné opatrenia, ktoré by sa mohli zaviesť v tejto časti systému RFID, sú prirodzene obmedzené. Avšak aj bezdrôtový aspekt komunikácie predstavuje isté pridané riziko v porovnaní s drôtovou komunikáciou, a preto sú potrebné ďalšie požiadavky na zabezpečenie.

25. Piatou otázkou je nedostatok transparentnosti spracovávania. Systémy RFID môžu viesť k nepovšimnutému zhromažďovaniu a spracovávaniu informácií, ktoré sa môžu použiť na profiláciu jednotlivca. Tento dôsledok sa môže veľmi dobre ilustrovať porovnaním systémov RFID a mobilných telefónov, teda porovnaním, ktoré sa používa často. Na jednej strane mobilný telefón využíval výhody z vysokej úrovne akceptácie nezávisle na potenciálnych rizikách spojených s narušením súkromia. Mohlo by sa dospieť k záveru, že RFID sa bude akceptovať rovnakým spôsobom. Na druhej strane sa musí zdôrazniť, že mobilný telefón je viditeľný objekt, ktorý má koncový používateľ ešte stále pod kontrolou, keďže sa môže vypnúť. To však nie je prípad RFID.

26. Hoci uvedené nepovšimnuté zhromažďovanie a spracovávanie informácií môže byť zákonné, je tiež možné a za rôznych okolností dokonca celkom pravdepodobné, že dôjde k nezákonnému zhromažďovaniu a spracovávaniu takýchto údajov.

27. Vyjasnenia uvedené v tejto kapitole odôvodňujú nasledujúci záver. Široké využívanie technológie RFID je v podstate nové a môže mať zásadný vplyv na našu spoločnosť a na ochranu základných práv v našej spoločnosti, akým je právo na ochranu súkromia a údajov. RFID môže priniesť kvalitatívnu zmenu.

IV. ŠPECIFIKOVANIE DÔSLEDKOV

Úvod

28. Táto kapitola sa zameria hlavne na vplyv RFID na ochranu základných práv v našej spoločnosti, akým je právo na súkromie a ochranu údajov. Táto špecifikácia bude mať dva kroky, prvým je krátky opis spôsobu, akým sa tieto základné práva chránia na v súčasnom právnom rámci. Ako druhý krok EDPS rozvedie možnosti plného využitia súčasného právneho rámca. Toto úsilie sa uviedlo v stanovisku k oznámeniu Komisie o smernici o ochrane údajov ako „úplné vykonávanie súčasných ustanovení smernice“.

29. Východiskový bod je takýto: nové produkty technologického vývoja, ako napríklad systémy RFID, jednoznačne ovplyvňujú požiadavky na účinný právny rámec pre ochranu údajov. Potreba účinnej ochrany osobných údajov jednotlivca však môže obmedzovať používanie týchto nových technológií. Vzájomné pôsobenie má teda dve stránky: technológia ovplyvňuje právne predpisy a právne predpisy ovplyvňujú technológiu ([3]).

([1]) Hall, E. T. 1966, Skrytá dimenzia (prvé vydanie). Garden City, N.Y: Doubleday.

([2]) Altman, I. 1975, Prostredie a sociálne správanie, Brooks/Cole Monterrey.

([3]) Pozri pripomienky EDPS z marca 2006 k oznámeniu Komisie o interoperabilite európskych databáz, zverejnené na webovej stránke EDPS.

Ochrana základných práv

30. Ochrana základných práv na ochranu súkromia a údajov v rámci Európskej únie je zaručená predovšetkým právnym rámcom, ktorý je potrebný, keďže sa zaoberáme právami, ktoré sa uznávajú v článku 8 Európskeho dohovoru o ľudských právach a základných slobodách a v článkoch 7 a 8 Charty základných práv Únie. Príslušný právny rámec pre ochranu údajov a RFID v podstate pozostáva zo smernice o ochrane údajov 95/46/ES a smernice o elektronickom súkromí 2002/58/ES ([1]).

31. Všeobecný právny rámec pre ochranu údajov, ako sa ustanovuje v smernici 95/46/ES, sa vzťahuje na RFID, pokiaľ údaje, ktoré spracúvajú systémy RFID, vyhovujú definícii osobných údajov. Zatiaľ čo v určitých prípadoch systémy RFID spracúvajú jednoznačne osobné údaje a nepochybne patria do pôsobnosti smernice o ochrane údajov, existujú aj uplatnenia, v prípade ktorých uplatniteľnosť smernice o ochrane údajov nemusí byť taká zrejmá. Stanovisko pracovnej skupiny na ochranu údajov podľa článku 29 č. 4/2007 o koncepcii osobných údajov má za cieľ prispieť k jasnejšiemu a všeobecne uznávanému chápaniu koncepcie osobných údajov a tým k zmierneniu neistoty ([2]).

32. Pokiaľ ide o smernicu o elektronickom súkromí, situácia je nasledovná. Doteraz nie je jasné, či sa táto smernica vzťahuje na systémy RFID. Z tohto dôvodu návrh Komisie na zmenu a doplnenie tejto smernice z 13. novembra 2007 obsahuje ustanovenie, ktorého účelom je upresniť, že smernica sa skutočne vzťahuje na niektoré uplatnenia RFID. Na iné uplatnenia RFID sa však smernica vzťahovať nemusí z dôvodu jej obmedzenia na spracovanie osobných údajov v spojení s poskytovaním verejne dostupných služieb elektronickej komunikácie vo verejných komunikačných sieťach.

33. Ochranu osobných údajov môže dopĺňať škála samoregulačných nástrojov (nelegislatívny rámec). Použitie týchto nástrojov sa aktívne podporuje v oboch smerniciach, najmä v článku 27 smernice o ochrane údajov, v ktorom sa uvádza, že členské štáty a Komisia nabádajú k vypracúvaniu kódexov správania, ktoré majú prispieť k riadnemu vykonávaniu smernice. Okrem toho by samoregulačné nástroje mohli účinne prispievať k vykonávaniu bezpečnostných opatrení, ktoré sa vyžadujú v článku 17 smernice o ochrane údajov a v článku 14 smernice o elektronickom súkromí.

([1]) Bod 59 tohto stanoviska sa zaoberá relevantnosťou tretej smernice, konkrétne smernice Európskeho parlamentu a Rady 1999/5/ES z 9. marca 1999 o rádiovom zariadení a koncových telekomunikačných zariadeniach a o vzájomnom uznávaní ich zhody (Ú. v. ES L 91, 7.4.1999, s. 10).

([2]) Pozri okrem iného s. 10 stanoviska, uvedeného v poznámke pod čiarou 5.

Úplné vykonávanie existujúceho rámca

34. V stanovisku k oznámeniu o smernici o ochrane údajov sa uvádza niekoľko nástrojov, ktoré možno použiť na jej lepšie vykonávanie. Väčšina nezáväzných nástrojov uvádzaných v stanovisku je vzhľadom na RFID relevantná, ako napríklad výkladové alebo iné oznámenia, podpora najlepších postupov, využívanie osvedčení o zachovaní dôverného charakteru informácií alebo audity ochrany súkromia vykonávané tretími stranami. Možnosťou prijímania osobitných pravidiel pre RFID sa zaoberá kapitola V. Ale zlepšenia sú možné aj v súčasnom rámci.

Samoregulačné nástroje

35. EDPS súhlasí s Komisiou, že v prvej fáze je vhodné ponechať priestor na samoreguláciu, čo umožní zainteresovaným stranám rýchlo vytvoriť a prostredie, ktoré bude v súlade s právnymi predpismi, a tak prispieť k vytvoreniu bezpečnejšieho právneho prostredia.

36. Očakáva sa, že Komisia bude tento proces samoregulácie stimulovať a riadiť, pričom sa bude radiť so skupinou strán zainteresovaných na RFID. EDPS v tejto súvislosti víta odporúčanie uvedené v oznámení, ktoré by malo obsahovať osobitné usmernenia určujúce *„zásady, ktoré by mali verejné orgány a iné zúčastnené strany uplatňovať vzhľadom na používanie RFID“*.

37. V oznámení sa predpokladá, že samoregulácia bude mať formu kódexu správania alebo kódexu osvedčených postupov. Nezávisle na tom, aká bude jej forma, by podľa EDPS samoregulácia mala:

— poskytovať konkrétne a praktické usmernenie, pokiaľ ide o osobitné typy uplatnení RFID, a tým prispievať k dodržiavaniu právneho rámca pre ochranu údajov,

— riešiť špecifické otázky ochrany údajov a problémy, ktoré vznikajú v súvislosti s uplatňovaním RFID vo všeobecnosti,

— prispievať k jednotnému a harmonizovanému uplatňovaniu smernice o ochrane údajov v celej EÚ, najmä v sektoroch, v ktorých sa pravdepodobne bude používať ten istý typ uplatnení RFID v celej EÚ,

— byť uplatňovaná všetkými relevantnými zainteresovanými stranami. Jej nedodržiavanie by malo mať negatívne (možno finančné) dôsledky.

38. EDPS poukazuje na jednu oblasť, v ktorej bude samoregulácia obzvlášť užitočná. V súvislosti s tými uplatneniami RFID, ktorých súčasťou je spracúvanie osobných údajov, ukladá smernica o ochrane údajov kontrolórom údajov rôzne povinnosti, najmä na základe článkov 17 (bezpečnosť spracúvania) a 7 (potreba spracúvať údaje iba na základe príslušných právnych dôvodov). Podľa týchto ustanovení musia kontrolóri údajov na jednej strane stanoviť opatrenia proti neoprávnenému zverejneniu údajov. Na druhej strane musia zabezpečiť, aby k prípadnému spracovaniu, ako napríklad zverejneniu informácií prostredníctvom čítačiek, dochádzalo iba s informovaným súhlasom jednotlivca, ktorého sa tieto informácie týkajú.

39. Tieto ustanovenia smernice o ochrane údajov sa môžu vykladať tak, že sa vyžaduje, aby sa systémy RFID zavádzali s potrebnými technickými riešeniami s cieľom zabrániť rizikám neželaného zverejnenia alebo minimalizovať ich a s cieľom zabezpečiť, aby sa prípadne spracovanie alebo prenos údajov vykonávali iba s informovaným súhlasom. Podľa názoru EDPS bude existencia takejto povinnosti (t. j. uplatňovať potrebné technické riešenia na zabránenie alebo minimalizovanie rizík neželaného zverejnenia) a jej záväzný charakter pre subjekty zavádzajúce systémy RFID ešte silnejší a jasnejší, ak sa táto požiadavka zohľadní v pripravovaných kódexoch správania alebo kódexoch osvedčených postupov uvedených vyššie. Z týchto dôvodov EDPS dôrazne odporúča, aby odporúčanie Komisie zahŕňalo takýto výklad smernice o ochrane údajov, pričom by malo zdôrazniť existenciu povinnosti zavádzať systémy RFID s potrebnými technickými opatreniami na zabránenie neželanému zhromažďovaniu alebo zverejňovaniu informácií.

Potreba usmernenia

40. EDPS odporúča, aby Komisia v úzkej spolupráci s expertnou skupinou pre RIFD vypracovala jeden alebo viac dokumentov, ktoré poskytnú jasné usmernenia o tom, ako uplatňovať súčasný právny rámec na prostredie RFID. V usmerneniach by sa mali uviesť praktické spôsoby, ako dodržiavať zásady ustanovené v smernici o ochrane údajov a v smernici o elektronickom súkromí. Pokiaľ ide o celkový prístup vyplývajúci z usmernenia a jeho konkrétny obsah, EDPS predkladá nasledovné návrhy.

41. Usmernenia, ktorými sa stanovia zásady, ktoré sa majú uplatňovať v súvislosti s používaním RFID, by mali byť dostatočne cielené a malo by sa v nich k jednotlivým sektorom pristupovať špecifickým spôsobom. Univerzálny prístup nebude spĺňať sledovaný cieľ, teda zabezpečenie jasného a súdržného rámca. Namiesto toho sa rozsah pôsobnosti usmernení musí obmedziť na dobre vymedzené sektorové uplatnenia RFID.

42. V usmerneniach sa okrem toho musia navrhnúť praktické a účinné metódy vývoja *techník a noriem*, ktoré by mohli prispieť k tomu, aby systémy RFID vyhovovali právnemu rámcu na ochranu údajov, a ktorých súčasťou bude použitie postupu na zabezpečenie „ochrany súkromia už v štádiu návrhu“.

43. Pri uplatňovaní súčasného právneho rámca na prostredie RFID sa musí venovať pozornosť najmä uplatňovaniu zásad ochrany údajov a povinností, ktoré sa vzťahujú na kontrolórov údajov pracujúcich so systémami RFID. Osobitne významné sú tieto povinnosti a zásady:

— zásada práva na informácie vrátane práva byť informovaný, keď sa údaje zhromažďujú prostredníctvom čítačiek, a v príslušných prípadoch o tom, že výrobky sú označené štítkami,

— koncepcia súhlasu ako jedného z právnych dôvodov na spracovanie údajov. Táto koncepcia sa premieta do povinnosti deaktivovať štítky RFID na mieste predaja, ak dotknutá osoba nedala svoj súhlas ([1]). Právo deaktivovať štítky RFID slúži aj na účel zaistenia bezpečnosti informácií, t. j. zaistenia toho, aby sa údaje spracúvané prostredníctvom štítkov RFID nezverejňovali neželaným tretím stranám,

— právo jednotlivca nebyť vystavený nepriaznivým rozhodnutiam len na základe automatizovaného spracovania definovaného osobného profilu.

44. Pokiaľ ide o právo na informácie, v usmerneniach by sa malo ustanoviť, že jednotlivcom sa musia poskytovať *informácie* týkajúce sa procesu spracovania ich osobných údajov. Mali by sa upozorňovať okrem iného najmä na: i) prítomnosť čítačiek a aktivovaných štítkov RFID na výrobkoch alebo ich obaloch, ii) dôsledky takejto prítomnosti, pokiaľ ide o zhromažďovanie informácií a iii) účely, na ktoré sa zhromaždené informácie majú použiť.

45. Vhodným opatrením na poskytovanie informácií môže byť použitie loga. Logá možno používať na upozornenie na prítomnosť čítačiek a štítkov RFID, ktoré by mali ostať aktívne. Samotné použitie loga však dostatočne nezabezpečí riadne spracovanie informácií, ktoré si vyžaduje, aby sa informácie poskytovali dotknutým osobám jasným a zrozumiteľným spôsobom. Použitie loga by sa malo zvážiť ako opatrenie na doplnenie poskytovania podrobnejších informácií.

([1]) Podrobnosti pozri v odsekoch 46 – 50 tohto stanoviska.

Základný kameň: Zásada predchádzajúceho súhlasu (opt-in)

46. Pri všetkých relevantných systémoch RFID by sa v riešeniach ako základný predpoklad mala dodržiavať a uplatňovať zásada predchádzajúceho súhlasu na mieste predaja. Možnosť, aby štítky RFID aj po opustení miesta predaja naďalej vysielali informácie, by bola v rozpore so zákonom okrem prípadov, keď by na to mal kontrolór údajov primerané zákonné dôvody. Za primerané zákonné dôvody by sa za bežných okolností považoval len: a) súhlas dotknutej osoby alebo v prípade, ak by takéto zverejnenie bolo potrebné na poskytnutie služby, b) konkrétna a nevynútená žiadosť dotknutej osoby ([1]). Oba zákonné dôvody by sa v takom prípade považovali za „predchádzajúci súhlas".

47. Podľa zásady predchádzajúceho súhlasu by sa štítky mali na mieste predaja deaktivovať, a to okrem prípadov, ak si osoba, ktorá si výrobok so štítkom kúpila, želá ponechať štítok aktívny. Využitím práva ponechať štítok aktívny by takáto osoba súhlasila s ďalším spracovaním svojich údajov, napríklad s prenosom údajov do čítačky pri ďalšej návšteve kontrolóra údajov.

48. Aby sa mohlo čeliť rastúcej rozmanitosti uplatnení RFID a aby sa uľahčil rozvoj nových inovačných obchodných modelov, EDPS zdôrazňuje dôležitosť pružného prístupu. Pružnosť sa musí zabezpečiť aj pri uplatňovaní zásady predchádzajúceho súhlasu.

49. Existuje viacero možností uplatňovania tejto zásady. Napríklad, ako alternatíva k odstráneniu štítka by sa dalo navrhnúť jeho blokovanie, čiastočné znefunkčnenie alebo uzamknutie pre konkrétneho používateľa podľa bezpečnostného modelu nazývaného „znovurodiace sa káčatko" ([2]). V prípade štítku s kratším životným cyklom by sa mohla z referenčnej databázy vymazať jeho adresa, ktorá smeruje k informáciám uloženým v databáze, čím by sa zabránilo spracovaniu dodatočných údajov, ktoré sa pomocou štítku zozbierali.

50. Na záver je potrebné dodať, že hoci podľa EDPS je „zásada predchádzajúceho súhlasu" na mieste predaja zákonnou povinnosťou, ktorá by sa vo väčšine situácií podľa smernice o ochrane údajov už mala dodržiavať, existujú dobré dôvody na to, aby sa táto povinnosť vymedzila aj v samoregulačných nástrojoch s cieľom okrem iného zabezpečiť jej čo najvhodnejšie uplatňovanie. Osobitné uplatňovanie je v každom prípade potrebné pri tých systémoch RFID, ktoré nepatria do rozsahu pôsobnosti smernice o ochrane údajov.

Potreba prihliadať na ochranu súkromia už v štádiu návrhu (privacy by design)

51. Aby sa minimalizovalo ohrozenie súkromia a údajov, v časti 3.2 na strane 6 oznámenia Komisie sa schvaľuje myšlienka vymedzenia a prijatia kritérií pre počiatočné štádium návrhu. EDPS tento prístup víta. Prijatie špecifikácií a kritérií pre návrhy, ktoré sa nazývajú aj „najlepšie využiteľné postupy" (Best Available Techniques – BAT), skutočne prispeje k regulácii ochrany údajov a k bezpečnostným požiadavkám v tejto oblasti. Uvedeným určením technických a organizačných kritérií sa v prípade ich pravidelného preskúmavania posilní symbiotický model požiadaviek na súkromie a bezpečnosť, ktorý vyvíja Európska únia.

52. Vhodné vymedzenie BAT v oblasti ochrany súkromia a bezpečnosti pre systémy RFID bude rozhodujúce aj pre vybudovanie dôveryhodného prostredia, ktoré posilní široké prijatie týchto postupov koncovými používateľmi, aj pre konkurencieschopnosť európskeho priemyslu.

53. Proces výberu BAT pre systémy RFID by sa mal urýchliť vypracúvaním posúdení vplyvu, ktorým sa musí venovať viac úsilia. EDPS sa domnieva, že k určeniu týchto najlepších postupov a k vývoju uvedených metodík môže prispieť Európska agentúra pre bezpečnosť sietí a informácií (ENISA) spolu so spoločnými výskumnými centrami Európskej komisie a v spojení s príslušnými zainteresovanými stranami z oblasti priemyslu. Vhodný ilustračný príklad ([3]) BAT, ktorý by sa teraz mal rozvinúť na európskej úrovni, poskytol nemecký Federálny úrad pre bezpečnosť informácií (BSI) prostredníctvom spustenia projektu „technické usmernenia pre RFID".

54. Pri rýchlej akceptácii zásady prihliadania na ochranu súkromia už v štádiu návrhu môžu hrať kľúčovú úlohu aj normy. Komisia by preto mala pri vývoji medzinárodných noriem pre RFID prispieť k prijatiu bezpečnostných záruk v oblasti ochrany súkromia a údajov. Pracovná skupina článku 29 jasne vo svojom pracovnom dokumente ([4]) o RFID jasne opísala, ako môžu normy prispieť k rozvoju systémov RFID, v ktorých sa zohľadňuje požiadavka na ochranu súkromia.

([1]) Pri niektorých uplatneniach RFID je možné sa odvolať na iné dôvody, ako napríklad článok 7f (legitímne záujmy kontrolóra s primeranou ochranou proti zneužitiu).

([2]) Tento model vytvorili Frank Stajano a Ross Anderson z Univerzity v Cambridge a jeho názov je inšpirovaný tým, „ako káčatko predpokladá, že prvý pohyblivý predmet, ktorý vidí, je určite jeho matka".

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

([4]) Pracovný dokument z 19. januára 2005 (WP 105) o otázkach ochrany údajov, ktoré sa týkajú technológie RFID.

55. Okrem toho EDPS víta stanovisko Komisie k výskumu a vývoju technológií RFID a potrebe zmiernenia rizík pre súkromie. Zásada prihliadania na ochranu súkromia už pri návrhu sa musí aplikovať v najskoršom štádiu vývoja technológií, čím sa lepšie prispeje k ich súladu s právnym rámcom ochrany údajov. EDPS, ako už stručne uviedol vo svojej výročnej správe za rok 2006, sa k týmto snahám pripojí prostredníctvom poskytovania stanovísk a rád k jednotlivým projektom 7. rámcového programu (2007 – 2013).

V. SÚ POTREBNÉ KONKRÉTNE LEGISLATÍVNE OPATRENIA?

56. Samoregulácia samotná nemusí ako prostriedok úplnej realizácie existujúceho rámca ochrany údajov a súkromia postačovať. Aj keby plnila požiadavky uvedené vyššie, jej uplatňovanie je dobrovoľné a nesúlad sa nedá vždy účinne postihovať. Okrem toho budú na zabezpečenie ochrany práv jednotlivcov na súkromie a ochranu údajov asi aj tak potrebné záväzné legislatívne opatrenia; a to najmä ako záruka v prípade zlyhania samoregulačného prístupu.

57. Kľúčovou otázkou je určenie právnych nástrojov, ktoré sú potrebné na zabezpečenie toho, aby sa systémy RFID skutočne používali spolu s potrebnými technickými riešeniami na zabránenie rizikám pre ochranu údajov alebo súkromie alebo na minimalizáciu týchto rizík, ako aj aby zodpovední kontrolóri prijali primerané opatrenia na dodržiavanie svojich záväzkov podľa existujúceho právneho rámca. Z uvedeného vyplývajú niektoré ďalšie otázky:

— sú potrebné špecifické pravidlá?

— ak áno, môžu sa prijať v rámci existujúceho právneho rámca, napríklad prostredníctvom využitia platných komitologických postupov?

— alebo je na zabezpečenie účinného použitia aplikácie RFID so zabudovanými technológiami na zvýšenie ochrany súkromia potrebný nový legislatívny nástroj?

58. V tejto kapitole sa budeme zaoberať vydávaním záväzných legislatívnych opatrení v rámci existujúceho právneho rámca, zatiaľ čo v kapitole VI preberieme ako osobitný problém potrebu nového legislatívneho nástroja.

59. Najprv by sme mali osobitnú pozornosť venovať ustanoveniam článku 17 smernice 95/46/ES, článku 14 ods. 3 smernice 2002/58/ES a článku 3 ods. 3 písm. c) smernice 1999/5/ES. Článok 14 ods. 3 umožňuje členským štátom prijať opatrenia, aby sa zabezpečilo, že koncové zariadenie je skonštruované v súlade s právom používateľov na ochranu a kontrolu použitia ich osobných údajov podľa smernice 1999/5/ES [1]. V článku 3 ods. 3 písmeno c) smernice 1999/5/ES sa ustanovuje, že Komisia môže komitologickým postupom rozhodnúť, že prístroje v rámci určitej triedy zariadení alebo prístroje konkrétneho typu majú byť skonštruované tak, aby mali zapracované bezpečnostné funkcie zaisťujúce ochranu osobných údajov a súkromia užívateľa alebo zákazníka. Článok 3 ods. 3 písm. c) smernice 1999/5/ES sa až doteraz nevyužíval.

60. Prostredníctvom týchto ustanovení sa zákonodarnému orgánu – na vnútroštátnej úrovni a na úrovni Spoločenstva – poskytuje právomoc ustanoviť povinnosť začleniť do výroby systémov RFID bezpečnostné funkcie zaisťujúce ochranu súkromia a údajov, čo je koncepcia ochrany už v štádiu návrhu („privacy by design“) [2]. Vyzýva sa v nej aj na využitie najlepších využiteľných postupov (BAT).

61. Aby sa využívanie koncepcie prihliadania na ochranu súkromia už v štádiu návrhu stalo povinnosťou, EDPS navrhuje, aby Komisia po porade s expertnou skupinou pre RFID použila mechanizmus ustanovený v článku 3 ods. 3 písm. c) smernice 1999/5/ES.

62. Po druhé, je možné vymedziť uplatňovanie existujúceho legislatívneho rámca na RFID prostredníctvom úprav samotných smerníc. Ako sme už spomenuli, Komisia nedávno predložila návrh na zmenu a doplnenie smernice o elektronickom súkromí, ktorá obsahuje nové ustanovenie s týmto výhľadom. EDPS víta prvé potvrdenie uplatniteľnosti uvedenej smernice na aplikácie RFID. EDPS sa bude zaoberať konkrétnymi otázkami, ktoré vyplynú zo vzťahu medzi smernicou o elektronickom súkromí a RFID, vo svojom stanovisku k návrhu na zmenu a doplnenie, ktoré sa predloží na začiatku roku 2008.

63. Vzhľadom na to, že Komisia v blízkej budúcnosti nepredpokladá žiadne úpravy smernice o ochrane údajov [3], možnosti na špecifikáciu vo vzťahu k uplatňovaniu existujúceho legislatívneho rámca na RFID sú obmedzené.

VI. POTREBUJEME PRE RFID OSOBITNÝ PRÁVNY RÁMEC?

Zámery Komisie

64. V predmetnom oznámení [4] sa zdôrazňuje dôležitosť bezpečnosti a prihliadania na ochranu súkromia už od návrhu. Vyžaduje sa v ňom aj zapojenie všetkých zainteresovaných strán. Hlavným výsledkom činnosti Komisie bude

[1] A v súlade s rozhodnutím Rady 87/95/EHS z 22. decembra 1986 o normalizácii v oblasti informačnej technológie a telekomunikácií (Ú. v. ES L 36, 7.2.1987, s. 31).
[2] Pozri kapitolu IV.
[3] EDPS tento prístup podporuje, pozri bod 64.
[4] Pozri bod 4.1 oznámenia.

„odporúčanie, v ktorom ustanoví zásady, ktoré by mali verejné orgány a iné zúčastnené strany uplatňovať vzhľadom na používanie RFID“. Odporúčanie sa pravdepodobne prijme na jar roku 2008. Legislatívne zámery, ktoré sa v oznámení uvádzajú, obsahujú dva kroky. Komisia:

— v pripravovanom návrhu na zmenu a doplnenie smernice o elektronickom súkromí zváži vhodné ustanovenia o RFID. Ako sa už povedalo, Komisia uvedený návrh predložila v novembri 2007, pričom v ňom potvrdila uplatniteľnosť smernice na systémy RFID ([1]), ale nenavrhla rozšírenie rozsahu pôsobnosti smernice o elektronickom súkromí na súkromné siete.

— posúdi potrebu ďalších legislatívnych opatrení na zabezpečenie ochrany údajov a súkromia.

65. Na základe tohto postupu sa dá očakávať, že Komisia – aspoň v najbližšom období – nepočíta s predložením nových, špecifických právnych predpisov na zabezpečenie ochrany údajov a súkromia v oblasti RFID.

Parametre pre zákonodarný orgán

66. V stanovisku k oznámeniu o smernici o ochrane údajov načrtol EDPS niekoľko legislatívnych činností týkajúcich sa spracúvania osobných údajov, ktoré by sa dali zhrnúť takto:

— po prvé, mali by sa zachovať ťažiskové zásady ochrany údajov: „Nie sú potrebné nové zásady, sú ale jasne potrebné iné administratívne opatrenia, ktoré sú na jednej strane účinné a vhodné pre spoločnosť prepojenú sieťami a na strane druhej minimalizujú administratívne náklady“ ([2]),

— po druhé, legislatívne návrhy by sa mali predkladať len v prípade, ak je dostatočne preukázaná ich potrebnosť a primeranosť. Z tohto dôvodu by sa všeobecný legislatívny rámec na ochranu údajov v krátkodobom horizonte meniť nemal,

— po tretie, zmeny v spoločenskom vývoji môžu viesť k vytvoreniu špecifických právnych rámcov s cieľom prispôsobiť zásady smernice o ochrane údajov otázkam, ktoré vyvolal nástup konkrétnych technológií, ako napríklad RFID. Je pochopiteľné, že aj v tomto kontexte sa musia splniť podmienky potrebnosti a primeranosti.

67. Ďalším užitočným krokom je vymedzenie očakávaní, s ktorými sa zákonodarný orgán musí v oblasti RFID vyrovnať:

— právne predpisy musia byť pružné a musia ponechať priestor na inovácie a technický rozvoj. Výsledkom by mali byť dostatočne technicky neutrálne predpisy,

— po druhé, právne predpisy musia poskytovať právnu istotu. Výsledkom by mali byť dostatočne konkrétne predpisy. Zainteresované strany musia presne vedieť, ako sa riadi ich činnosť,

— po tretie, právne predpisy musia účinne chrániť všetky ohrozené oprávnené záujmy. Toto si v každom prípade vyžaduje ich vynútiteľnosť a jasné vymedzenie zodpovedností (ktorá strana zodpovedá za aké správanie) ([3]). Uvedené požiadavky sa dostávajú ešte viac do popredia v situácii ohrozenia súkromia a ochrany údajov, pretože ide o základne práva jednotlivca podľa Európskeho dohovoru o ľudských právach a základných slobodách a Charty základných práv Európskej únie.

Názor EDPS

68. EDPS je jasné, že nie každý vývoj v oblasti techniky by mal viesť k reakcii európskeho zákonodarného orgánu. Zatiaľ čo prijatie a nadobudnutie účinnosti právnych predpisov si vyžaduje (a malo by si vyžadovať) čas, technický rozvoj je rýchly. Právne predpisy by mali byť výsledkom vyváženia všetkých záujmov, ktoré by mohli byť ohrozené. Ak sa ako právny nástroj zvolí smernica, je potrebný ešte dlhší čas, keďže smernice sa musia plne začleniť do právnych systémov členských štátov.

69. Ako sa však už v niektorých častiach tohto stanoviska zdôraznilo, RFID nie je len nejakou ďalšou novou technológiou. V oznámení sa o RFID hovorí ako o bráne k novej etape vývoja informačnej spoločnosti, ktorá sa často nazýva aj „internet vecí“, pričom štítky RFID budú predstavovať kľúčové prvky „inteligentných prostredí“. Tieto prostredia sú tiež dôležitým vývojovým krokom smerom k tzv. „monitorovanej spoločnosti“ ([4]). Na tomto základe je legislatívna činnosť v oblasti RFID naozaj opodstatnená. Technológia RFID môže priniesť kvalitatívnu zmenu.

([1]) Pozri navrhovaný nový článok 3 smernice 2002/58.
([2]) Bod 24 stanoviska k oznámeniu o smernici o ochrane údajov.
([3]) V oblasti ochrany údajov to znamená určenie „kontrolóra údajov“.
([4]) Toto posolstvo opätovne zaznelo vo vyhlásení európskych orgánov na ochranu údajov prijatom v Londýne 2. novembra 2006, ktoré je dostupné na webovej stránke EDPS: http://www.edps.europa.eu/EDPSWEB/edps/lang/en/pid/51

70. EDPS z tohto hľadiska odporúča zvážiť prijatie (alebo návrh) právnych predpisov Spoločenstva, ktorými sa upravia hlavné otázky používania RFID v príslušných sektoroch v prípade, ak by zlyhalo riadne vykonávanie existujúceho právneho rámca. Takéto legislatívne opatrenie sa po nadobudnutí účinnosti musí z hľadiska všeobecného rámca ochrany údajov považovať za „*lex specialis*“.

71. Prijatie uvedeného právneho nástroja by malo tieto výhody:

— jeho prostredníctvom by sa dali nastaviť zásadné parametre samoregulačných mechanizmov;

— perspektíva prijatia legislatívneho nástroja by v konečnom dôsledku mohla byť účinným stimulom, aby zainteresované strany zaviedli samoregulačné mechanizmy, ktoré poskytnú dôslednú ochranu.

72. Ešte praktickejšie by bolo, keby sa Komisia požiadala, aby pripravila konzultačný dokument o výhodách a nevýhodách konkrétneho právneho predpisu a jeho hlavných prvkoch. O pripomienky by sa samozrejme mohli požiadať aj zainteresované strany. Zapojiť by sa mohla i Pracovná skupina článku 29.

Možné riešenia

73. Zásah zákonodarného orgánu by mohol umožniť vytvorenie právneho rámca „ušitého na mieru“, ktorý by obsahoval zmes regulačných nástrojov špecifikujúcich a dopĺňajúcich súčasný právny rámec. Takýto rámec by mal vychádzať zo známych zásad ochrany údajov a mal by sa zamerať na rozdelenie zodpovedností a účinnosť kontrolných mechanizmov.

74. Konkrétny dôvod možnej potreby takýchto „na mieru ušitých“ právnych predpisov sa týka skutočnosti, že nie všetky systémy RFID zahŕňajú spracúvanie osobných údajov. Inými slovami, ak systémy RFID spracúvanie osobných údajov nezahŕňajú, strany zapojené do výroby a predaja výrobkov s technológiou RFID nie sú právne viazané realizovať žiadne technické opatrenia na zamedzenie odpočúvania alebo nastavenia čítačiek bez primeraného informovania dotknutých osôb. Ako sa preukázalo vyššie, aj pri takýchto aplikáciách RFID existujú riziká pre súkromie vyplývajúce z možného sledovania jednotlivcov, čo si vyžaduje rovnaké opatrenia na zabezpečenie ochrany súkromia. Konkrétnym príkladom môže byť štítkovanie jednotlivých kusov spotrebiteľských výrobkov *pred* predajom. V súhrne to znamená, že aj systémy RFID, ktoré nespracúvajú osobné údaje, môžu ohrozovať súkromie jednotlivca tak, že umožňujú jeho skryté sledovanie a použitie informácií na neprijateľné účely.

75. EDPS sa domnieva, že takémuto nešťastnému stavu by sa malo predísť. Vzhľadom na to, že v súčasných právnych predpisoch čiastočne (aspoň pre aplikácie RFID, ktoré nespracúvajú osobné údaje) chýbajú ustanovenia, v ktorých by sa tejto hrozbe pre súkromie čelilo, a vzhľadom na nedostatky nevynútiteľných právnych prostriedkov sa zdá, že na zabezpečenie uspokojivého výsledku je nevyhnutné využiť záväzné legislatívne opatrenia.

76. Takýmito opatreniami by sa v každom prípade:

— mala ustanoviť zásada predchádzajúceho súhlasu na mieste predaja ako presná a nepopierateľná právna povinnosť i pre systémy RFID, ktoré nepatria do rozsahu pôsobnosti smernice o ochrane údajov ([1]),

— malo zabezpečiť povinné vybavenie systémov RFID primeranými technickými prvkami na ochranu súkromia už v štádiu návrhu.

VII. **OTÁZKA SPRÁVY**

77. Hoci sa v oznámení Komisie „vo svojej podstate cezhraničný“ rozmer systémov RFID spomína len v rámci vnútorného trhu, EDPS sa nazdáva, že túto otázku treba riešiť na ešte vyššej medzinárodnej úrovni. Už v obchode sú systémy RFID „cezhraničné“, lebo činnosť štítku sa na mieste predaja nemusí skončiť. Na úrovni celého systému RFID sa tieto technológie stávajú cezhraničnými preto, že k prenosu osobných údajov do tretej krajiny môže dôjsť v prípade, ak má výrobca štítkovaného výrobku, ktorý je súčasťou systému RFID, sídlo mimo Európskej únie ([2]).

78. Z dlhodobejšieho hľadiska znamená správa referenčných databáz totožnosti RFID aj kľúčový rozmer pre náležité vynucovanie európskeho právneho rámca ochrany údajov. EDPS naliehavo vyzýva na nájdenie riešenia, pretože ďalšie chátranie tohto rámca by bolo neprijateľné.

79. EDPS predpokladá, že otázka správy RFID bude jednou z hlavných výziev, ktorá si vyžiada nemalé investície. Na zabezpečenie adekvátneho dodržiavania práv týkajúcich sa ochrany údajov v uvedených medzinárodných prostrediach sa bude musieť nájsť správne fórum na rokovania i najvhodnejšia riadiaca infraštruktúra.

([1]) V kapitole IV sa argumentuje, že zásada „predchádzajúceho súhlasu“ pri predaji je právnou povinnosťou, ktorá v smernici o ochrane údajov už existuje.

([2]) Povinnosti týkajúce sa prenosu osobných údajov sa riešia v článkoch 25 a 26 smernice o ochrane osobných údajov.

80. V tomto kontexte vyzýva EDPS Komisiu, aby predstavila svoj názor na otázku správy, a to podľa možností po porade so skupinou zainteresovaných strán pre RFID.

VIII. **ZÁVER**

81. EDPS víta oznámenie Komisie o RFID, keďže sa zaoberá hlavnými otázkami vznikajúcimi v kontexte zavádzania technológie RFID, a to bez toho, aby sa zanedbávali určujúce otázky súvisiace s ochranou súkromia a údajov. Súhlasí s názorom, že systémy RFID by mohli zohrávať kľúčovú úlohu pri rozvoji informačnej spoločnosti bežne nazývanej „internet vecí".

Vysvetlenie následkov

82. Široké využívanie technológie RFID je v podstate nové a môže mať zásadný vplyv na našu spoločnosť a na ochranu základných práv v našej spoločnosti, akými sú právo na ochranu súkromia a údajov. Technológia RFID môže priniesť kvalitatívnu zmenu.

83. V danom kontexte rozlišujeme päť základných oblastí týkajúcich sa súkromia a bezpečnosti:

— identifikácia dotknutej osoby,

— identifikácia kontrolóra údajov,

— znížený význam tradičného rozlišovania medzi súkromnou a verejnou sférou,

— dôsledky veľkosti a fyzických vlastností štítkov RFID,

— nedostatok transparentnosti pri spracúvaní.

Špecifikácia následkov

84. Všeobecný právny rámec ochrany údajov ustanovený v smernici 95/46/ES sa na RFID uplatňuje, pokiaľ údaje, ktoré spracúvajú systémy RFID, vyhovujú definícii osobných údajov.

85. Pokiaľ ide o smernicu o elektronickom súkromí, návrh Komisie z 13. novembra 2007 na zmenu a doplnenie tejto smernice obsahuje ustanovenie, ktorého účelom je upresniť, že smernica sa skutočne vzťahuje na určité systémy RFID. Z dôvodu obmedzenia tejto smernice na spracúvanie osobných údajov v spojení s poskytovaním verejne dostupných služieb elektronickej komunikácie vo verejných komunikačných sieťach by sa však nemusela vzťahovať na niektoré iné systémy RFID.

86. Ochranu osobných údajov môže dopĺňať škála samoregulačných nástrojov. Na takúto samoreguláciu je vhodné ponechať priestor, a to za predpokladu, že:

— poskytuje konkrétne a praktické usmernenia týkajúce sa konkrétnych typov uplatnení RFID,

— rieši špecifické otázky ochrany údajov a problémy, ktoré vznikajú v súvislosti so systémami RFID vo všeobecnosti,

— prispieva k jednotnému a zosúladenému uplatňovaniu smernice o ochrane údajov v rámci EÚ,

— ju uplatňujú všetky príslušné zainteresované strany.

87. EDPS odporúča, aby Komisia v úzkej spolupráci s expertnou skupinou pre RIFD vypracovala jeden alebo viac dokumentov, ktoré poskytnú jasné usmernenia o tom, ako uplatňovať súčasný právny rámec v prostredí RFID.

88. Usmernenia, ktorým sa stanovia zásady pre používanie RFID, by mali byť dostatočne adresné a malo by sa v nich k jednotlivým sektorom pristupovať špecifickým spôsobom. V usmerneniach by sa mali navrhnúť praktické a účinné metódy vývoja *techník a noriem*, ktoré by mohli prispieť k súladu systémov RFID s právnym rámcom ochrany údajov a ktorých súčasťou bude koncepcia ochrany súkromia už v štádiu návrhu.

89. EDPS víta prístup v oznámení Komisie, v ktorom sa schvaľuje myšlienka vymedzenia a prijatia kritérií pre počiatočné štádium návrhu.

90. Hoci sa EDPS domnieva, že „zásada predchádzajúceho súhlasu" na mieste predaja je zákonnou povinnosťou, ktorá by sa vo väčšine situácií podľa smernice o ochrane údajov už mala dodržiavať, táto povinnosť by sa mala vymedziť aj v samoregulačných mechanizmoch.

Sú potrebné špecifické opatrenia?

91. Aby sa využívanie koncepcie prihliadania na ochranu súkromia už v štádiu návrhu stalo povinnosťou, EDPS navrhuje, aby Komisia po porade s expertnou skupinou pre RFID použila mechanizmus ustanovený v článku 3 ods. 3 písm. c) smernice 1999/5/ES.

92. EDPS odporúča zvážiť prijatie (alebo návrh) právnych predpisov Spoločenstva, ktorými sa upravia hlavné otázky používania RFID v príslušných sektoroch v prípade, ak by zlyhalo riadne vykonávanie existujúceho právneho rámca. Takéto legislatívne opatrenie sa po nadobudnutí účinnosti musí z hľadiska všeobecného rámca ochrany údajov považovať za „*lex specialis*". Týmto legislatívnym opatrením by sa mali riešiť aj obavy týkajúce sa ochrany údajov a súkromia, ktoré vznikajú pri niektorých systémoch RFID, ako je napríklad štítkovanie jednotlivých kusov výrobkov pred predajom, pričom systém nemusí nevyhnutne zahŕňať spracovanie osobných údajov.

93. Komisia by mala pripraviť konzultačný dokument o výhodách a nevýhodách konkrétneho právneho predpisu a jeho hlavných prvkoch.

94. Zásah zákonodarného orgánu by mohol umožniť vytvorenie právneho rámca „ušitého na mieru“, ktorý by obsahoval zmes regulačných nástrojov špecifikujúcich a dopĺňajúcich súčasný právny rámec. Takýmito opatreniami by sa v každom prípade:

— mala ustanoviť zásada predchádzajúceho súhlasu na mieste predaja ako presná a nepopierateľná právna povinnosť i pre systémy RFID, ktoré nepatria do rozsahu pôsobnosti smernice o ochrane údajov ([1]),

— malo zabezpečiť povinné vybavenie aplikácií RFID primeranými technickými prvkami na ochranu súkromia už v štádiu návrhu.

Otázka správy

95. EDPS vyzýva Komisiu, aby predstavila svoj názor na otázku správy, a to podľa možností po porade so skupinou zainteresovaných strán pre RFID.

V Bruseli 20. decembra 2007

Peter HUSTINX

európsky dozorný úradník pre ochranu údajov

([1]) V kapitole IV sa argumentuje, že zásada „predchádzajúceho súhlasu“ pri predaji je právnou povinnosťou, ktorá v smernici o ochrane údajov už existuje.