I

(Uznesenia, odporúčania a stanoviská)

STANOVISKÁ

EURÓPSKY DOZORNÝ ÚRADNÍK PRE OCHRANU ÚDAJOV

Stanovisko Európskeho dozorného úradníka pre ochranu údajov k zvyšovaniu dôvery v informačnú spoločnosť podporovaním ochrany údajov a súkromia

(2010/C 280/01)

EURÓPSKY DOZORNÝ ÚRADNÍK PRE OCHRANU ÚDAJOV,

so zreteľom na Zmluvu o fungovaní Európskej únie, a najmä na jej článok 16,

so zreteľom na Chartu základných práv Európskej únie, a najmä na jej články 7 a 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 voľnom pohybe týchto údajov ([1]),

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 ([2]),

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 ([3]), a najmä na jeho článok 41,

PRIJAL TOTO STANOVISKO:

I. ÚVOD

1. Informačné a komunikačné technológie (IKT) otvárajú ohromné možnosti prakticky v každom aspekte nášho života – v práci, zábave, spoločenskom živote a vzdelávaní. Pre súčasnú informačnú ekonomiku a všeobecne pre spoločnosť sú neodmysliteľné.

2. Európska únia patrí k svetovým veľmociam v oblasti vyspelých IKT a je odhodlaná ňou naďalej zostať. S cieľom čeliť tejto výzve sa očakáva, že Európska komisia čoskoro prijme nový digitálny program, ktorý komisárka Kroesová, ako potvrdila, považuje za svoju prioritu ([4]).

3. Európsky dozorný úradník pre ochranu údajov uznáva výhody, ktoré IKT prinášajú, a súhlasí s tým, aby EÚ vyvíjala čo najväčšie úsilie na posilnenie ich rozvoja a všeobecného prijímania. Vyjadruje úplný súhlas so stanoviskami komisárok Kroesovej a Redingovej, že v centre tohto nového prostredia majú byť ľudia ([5]). Ľuďom by sa malo umožniť, aby sa mohli spoľahnúť na to, že IKT dokážu zachovať ochranu bezpečnosti ich informácií a kontrolovať ich používanie a aby sa mohli tiež spoľahnúť na to, že v digitálnom priestore sa budú rešpektovať ich práva na ochranu súkromia a údajov. Dodržiavanie týchto práv je základom pre získanie dôvery užívateľov. A takáto dôvera je podstatná, ak chceme, aby občania prijali nové služby za svoje ([6]).

([1]) Ú. v. ES L 281, 23.11.1995, s. 31.
([2]) Ú. v. ES L 201, 31.7.2002, s. 37.
([3]) Ú. v. ES L 8, 12.1.2001, s. 1.

([4]) Odpovede komisárky Neelie Kroesovej na dotazník Európskeho parlamentu v rámci vypočutí EP, ktoré predchádzali jej vymenovaniu za komisárku.

([5]) Odpovede komisársky Neelie Kroesovej na dotazník Európskeho parlamentu v kontexte vypočutí EP, ktoré predchádzali jej vymenovaniu; prejav komisárky Viviane Redingovej o „Európskom digitálnom programe pre nového digitálneho užívateľa, prednesený na fóre BEUC viacerých zainteresovaných strán na tému Súkromie spotrebiteľov a on-line marketing: trhové trendy a perspektívy politík (*BEUC Multi-stakeholder Forum on Consumer Privacy and Online Marketing: Market Trends and Policy Perspectives*)“, v Bruseli 12. novembra 2009.

([6]) Pozri napríklad správu RISEPTIS, „Trust in the Information Society“ (*Dôvera v informačnú spoločnosť*), správu poradného výboru, RISEPTIS (Research and Innovation on Security, Privacy and Trustworthiness in the Information Society *(Výskum a inovácie v oblasti bezpečnosti, súkromia a dôveryhodnosti v informačnej spoločnosti)*. K dispozícii na http://www.think-trust.eu/general/news-events/riseptis-report.html
Pozri tiež: J. B Horrigan, Broadband Adoption and Use in America, FCC Omnibus Broadband Initiative, OBI Working Paper Series No 1 *(J. B Horrigan, Prijatie a využitie širokého pásma v Amerike, Iniciatíva pre súhrnné široké pásmo FCC, Pracovný dokument ISŠP, č. série: 1)*.

4. EÚ má solídny právny rámec na ochranu údajov/súkromia, ktorého zásady platia v plnom rozsahu aj v digitálnom veku. S týmto sa však nemôžeme uspokojiť. IKT vyvolávajú mnohokrát nové obavy, ktoré v súčasnom rámci nie sú zohľadnené. Z tohto dôvodu sú potrebné niektoré opatrenia na zabezpečenie, aby jednotlivé práva zakotvené v práve EÚ poskytovali aj naďalej účinnú ochranu v tomto novom prostredí.

5. V tomto stanovisku sa rozoberajú opatrenia, ktoré by Európska únia mala presadzovať alebo prijať na zaručenie ochrany súkromia a údajov jednotlivcov v globalizovanom svete, ktorý sa aj naďalej bude zakladať na technológiách. Hovorí sa v ňom o legislatívnych aj nelegislatívnych nástrojoch.

6. Po prehľade o IKT ako novom trende, ktorý pomáha vytvárať nielen príležitosti, ale aj riziká, sa v stanovisku rozoberá potreba integrovať na praktickej úrovni ochranu údajov a súkromia od samého vzniku nových informačných a komunikačných technológií (čo sa nazýva zásada „ochrany súkromia už od štádia návrhu systému“). S cieľom presadiť dodržiavanie tejto zásady sa v stanovisku hovorí o potrebe zahrnúť zásadu „ochrany súkromia už od štádia návrhu systému“ do právneho rámca na ochranu údajov aspoň dvomi rôznymi spôsobmi. Po prvé tak, že sa zahrnie ako všeobecná, záväzná zásada a po druhé, že sa zahrnie do konkrétnych oblastí IKT, ktoré predstavujú osobitné riziká pre ochranu údajov/súkromia a ktoré možno zmierniť vhodnou technickou architektúrou a dizajnom. Takýmito oblasťami sú rádiofrekvenčná identifikácia (RFID), aplikácie sociálnej siete a aplikácie prehliadačov. Napokon sa v stanovisku uvedú návrhy týkajúce sa ďalších nástrojov a zásad zameraných na ochranu súkromia a ochranu údajov jednotlivcov v sektore IKT.

7. V rámci riešenia uvedeného sa v stanovisku rozvíjajú niektoré body, ktoré predložila pracovná skupina zriadená podľa článku 29 vo svojom príspevku k verejnej diskusii o budúcnosti súkromia ([1]). Ďalej nadväzuje na predchádzajúce stanoviská európskeho dozorného úradníka pre ochranu údajov, napríklad stanovisko z 25. júla 2007 o vykonávaní smernice o ochrane údajov, stanovisko z 20. decembra 2007 k RFID a dve stanoviská k smernici o elektronickom súkromí ([2]).

II. **IKT PONÚKAJÚ NOVÉ PRÍLEŽITOSTI, ALE PREDSTAVUJÚ AJ NOVÉ RIZIKÁ**

8. IKT sa porovnávajú s ďalšími dôležitými vynálezmi z minulosti, ako napríklad elektrická energia. Aj keď môže byť ešte predčasné hodnotiť ich skutočný historický dosah, vzťah medzi IKT a ekonomickým rastom v rozvinutých krajinách je jasný. IKT vytvárajú pracovné miesta, hospodárske výhody a prispievajú k celkovému blahobytu. Vplyv IKT ide nad rámec čisto ekonomických hľadísk, pretože zohráva významnú úlohu pri podpore inovácií a kreativity.

9. IKT navyše zmenili spôsob práce, socializácie a komunikácie ľudí. Ľudia sa čoraz viac opierajú o IKT napríklad v oblasti spoločenských a ekonomických vzťahov. Môžu využívať širokú škálu nových aplikácií IKT, ako napríklad elektronické zdravotníctvo (*eHealth*), elektronická doprava (*eTransport*), elektronická štátna správa (*eGoverment*), rovnako ako inovatívne interaktívne systémy na zábavu a vzdelávanie.

10. Vzhľadom na tieto výhody európske inštitúcie vyjadrili svoje odhodlanie podporiť IKT ako potrebný nástroj na zvýšenie konkurencieschopnosti európskeho priemyslu a urýchlenie obnovy európskeho hospodárstva. V auguste 2009 Komisia skutočne prijala Správu o digitálnej konkurencieschopnosti EÚ ([3]) a začala verejnú diskusiu o príslušných budúcich stratégiách na podporu IKT. Rada predložila 7. decembra 2009 príspevok k tejto diskusii s názvom „Obdobie po stratégii i-2010 – smerovanie k otvorenej, ekologickej a konkurencieschopnej znalostnej spoločnosti“ ([4]). Európsky parlament len

([1]) Stanovisko 168 pracovnej skupiny zriadenej podľa článku 29 o budúcnosti súkromia, Spoločný príspevok ku konzultáciám Európskej komisie o právnom rámci pre základné právo na ochranu osobných údajov, prijaté 1. decembra 2009.

([2]) Stanovisko z 25. júla 2007 k oznámeniu Komisie Európskemu parlamentu a Rade o pokračovaní pracovného programu pre lepšiu implementáciu smernice o ochrane údajov, Ú. v. EÚ C 255, 27.10.2007, s. 1; stanovisko z 20. decembra 2007 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], Ú. v. EÚ C 101, 23.4.2008, s. 1; stanovisko z 10. apríla 2008 k návrhu smernice, ktorou sa okrem iných právnych predpisov mení a dopĺňa smernica 2002/58/ES týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách), Ú. v. EÚ C 181, 18.7.2008, s. 1; druhé stanovisko z 9. januára 2009 k preskúmaniu smernice 2002/58/ES týkajúcej sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií.

([3]) Správa o digitálnej konkurencieschopnosti EÚ – Hlavné výsledky stratégie i-2010 v období 2005 – 2009, [SEK (2009) 1060].

([4]) Závery Rady „Obdobie po stratégii i-2010“ – smerovanie k otvorenej, ekologickej a konkurencieschopnej znalostnej spoločnosti. (17107/09), prijaté 18. 12. 2009.

nedávno prijal správu určenú na usmernenie Komisie pri stanovení digitálneho programu ([1]).

11. S príležitosťami a výhodami, ktoré sprevádzajú rozvoj IKT, prichádzajú nové riziká, najmä pre súkromie jednotlivcov a ochranu ich osobných údajov. IKT často vedú k šíreniu (pomerne často spôsobmi, ktoré sú mimo dohľadu jednotlivcov) množstva informácií, ktoré sa zhromažďujú, triedia, filtrujú, prenášajú alebo iným spôsobom uchovávajú, a tak sa riziká pre tieto údaje znásobujú.

12. Napríklad čipy RFID nahrádzajú čiarové kódy na (niektorých) spotrebiteľských výrobkoch. Predpokladá sa, že zo zlepšenia toku informácií v dodávateľskom reťazci (a teda zníženia potreby po „bezpečnostných" zásobách, poskytovania presnejších predpovedí a pod.) budú mať prospech podniky i spotrebitelia. Zároveň to však vyvoláva znepokojenie z možnosti byť sledovaný na rôzne ciele a rôznymi subjektmi prostredníctvom označených osobných vecí.

13. Ďalším príkladom je tzv. *cloud computing*, čo je v podstate poskytovanie hostiteľských užívateľských a neužívateľských aplikačných služieb prostredníctvom internetu. Tieto služby bývajú v rozsahu od knižníc fotografií, kalendárov, webmailu a databáz spotrebiteľov až po zložitejšie služby súvisiace s podnikaním. Výhody pre podniky a jednotlivcov sú jasné, zníženie nákladov (náklady sú prírastkové), nezávislosť na lokalite (ľahký prístup k informáciám kdekoľvek na svete), automatizácia (nie sú potrebné zdroje vyčlenené na IT a udržiavanie aktuálnosti softvéru) atď. Zároveň však existujú riziká narušenia bezpečnosti a tzv. hackerstva (počítačového pirátstva) a sú veľmi reálne. Existujú tiež obavy zo straty prístupu a kontroly nad vlastnými údajmi.

14. Ukázalo sa, že v iných oblastiach využívania aplikácií IKT môžu výhody a riziká existovať vedľa seba. Ako príklad môžeme uviesť *eHealth*, ktoré môže zvýšiť efektivitu, znížiť náklady, zvýšiť dostupnosť a všeobecne zlepšiť kvalitu zdravotníckych služieb. V prípade aplikácie *eHealth* sa však často objavuje otázka legitimity sekundárnych využití informácií z aplikácie *eHealth*, čo si vyžaduje dôkladnú analýzu cieľov každého prípadného sekundárneho využitia ([2]). Navyše dochádza k rozsiahlejšiemu využívaniu elektronických zdravotných záznamov a samotné systémy prenasledujú škandály v súvislosti s odhalením mnohých prípadov napadnutia elektronických zdravotných záznamov tzv. hackermi.

15. V krátkosti určitá úroveň reziduálneho rizika tu môže zostať naďalej aj po správnom posúdení a uplatnení potrebných opatrení. Dosiahnuť nulové riziko by nebolo reálne. Ako sa uvádza ďalej, na obmedzenie týchto rizík na príslušných úrovniach sa však môžu a musia zaviesť opatrenia.

III. OCHRANA SÚKROMIA UŽ OD ŠTÁDIA NÁVRHU SYSTÉMU AKO HLAVNÝ NÁSTROJ NA BUDOVANIE DÔVERY JEDNOTLIVCA V IKT

16. Potenciálne výhody IKT možno využívať len v praxi, ak si dokážu získať dôveru, inými slovami, ak dokážu zabezpečiť, že užívateľ bude ochotný byť závislý od IKT na základe ich vlastností a výhod. Takáto dôvera sa vytvorí len vtedy, ak IKT budú spoľahlivé, bezpečné, budú pod kontrolou jednotlivcov a ak bude zaručená ochrana ich osobných údajov a súkromia.

17. Rozsiahle riziká a zlyhania, ako napríklad uvedené vyššie, najmä vtedy, ak majú za následok zneužitie alebo prezradenie osobných údajov s odhalením súkromia jednotlivcov, môžu ohroziť dôveru užívateľov v informačnú spoločnosť, čo by mohlo vážne ohroziť rozvoj IKT a výhody, ktoré by mohli prinášať.

18. Riešením týchto rizík pre ochranu súkromia a údajov však nemôže byť eliminácia, vylúčenie alebo odmietnutie používania alebo presadzovania IKT. Nebolo by to ani možné, ani reálne. Zabránilo by to jednotlivcom využívať výhody IKT a vážne by to obmedzilo celkové prínosy, ktoré sa dajú docieliť.

19. Európsky dozorný úradník pre ochranu údajov sa domnieva, že pozitívnejším riešením je navrhovať a rozvíjať IKT spôsobom, pri ktorom sa zohľadňuje ochrana súkromia a údajov. Preto je nevyhnutné, aby ochrana súkromia a údajov bola obsiahnutá v celom životnom cykle tejto technológie, od úplného začiatku fázy prípravy návrhu až po konečné rozšírenie, používanie a záverečné zneškodnenie. Toto sa zvykne označovať ako „ochrana súkromia už od štádia návrhu systému" a rozoberá sa ďalej v texte.

20. Ochrana súkromia už od štádia návrhu systému môže znamenať rôzne kroky v závislosti od konkrétneho prípadu alebo aplikácie. Napríklad v niektorých prípadoch si to môže vyžadovať elimináciu/obmedzenie osobných údajov alebo zabránenie zbytočného a/alebo nežiaduceho spracovania. V iných prípadoch ochrana súkromia už od štádia návrhu systému môže znamenať ponuku

([1]) Správa o vymedzení nového digitálneho programu pre Európu: od i-2010 k digital.eu (2009/2225 (INI)), prijatá 18.3.2010.

([2]) Napríklad predávanie alebo používanie informácií o zdravotnom stave zhromaždených na účely poskytovania ošetrenia sa nesmie použiť na výber lokalít pre satelitné kliniky, zriadenie ambulantných chirurgických centier a plánovanie budúcich aktivít s finančnými dôsledkami inými spôsobmi by si vyžadovalo starostlivé posúdenie.

nástrojov na zvýšenie kontroly jednotlivcov nad svojimi osobnými údajmi. Tieto opatrenia by sa mali zvážiť pri stanovovaní noriem a/alebo osvedčených postupov. Môžu byť tiež začlenené do architektúry informačných a komunikačných systémov alebo do štrukturálnej organizácie subjektov, ktoré spracúvajú osobné údaje.

III.1. **Zásada ochrany súkromia už od štádia návrhu systému uplatniteľná v rôznych prostrediach IKT a ich dosah**

21. Potreba zásady ochrany súkromia už od štádia návrhu systému sa môže vyskytovať v rozličných prostrediach IKT. Napríklad v sektore zdravotnej starostlivosti sa čoraz viac využívajú infraštruktúry IKT, čo znamená často centralizované uchovávanie informácií o zdravotnom stave pacientov. Uplatňovanie zásady ochrany súkromia už od štádia návrhu systému v sektore zdravotnej starostlivosti by si vyžadovalo posúdenie vhodnosti rôznych opatrení, ako napr. možnosť minimalizovať centrálne uchovávané údaje alebo obmedziť ich na index pomocou šifrovacích nástrojov, prideľovať prístupové práva striktne na základe oprávnenia na prístup, anonymizácia údajov potom, čo už nie sú potrebné a pod.

22. Podobne aj dopravné systémy sa čoraz častejšie poskytujú štandardne s modernými aplikáciami IKT, ktoré komunikujú s vozidlom a jeho okolím na rôzne ciele a činnosti. Vozidlá sú napríklad stále častejšie vybavené novými funkciami IKT (GPS, GSM, siete senzorov atď.), ktoré poskytujú informácie nielen o ich polohe, ale aj ich technických podmienkach v reálnom čase. Tieto informácie by sa mohli využiť napríklad na nahradenie existujúceho systému cestnej dane cestným poplatkom v závislosti od využívania. Použitie zásady ochrany súkromia už od štádia návrhu systému na návrh architektúry týchto systémov by malo podporiť spracovanie a následný presun čo možno najmenšieho množstva osobných údajov ([1]). Pri dodržiavaní tejto zásady by decentralizované alebo polodecentralizované architektúry obmedzujúce zverejnenie údajov o polohe do centrálneho miesta boli vhodnejšie ako centralizované.

23. Z uvedených príkladov vyplýva, že pri budovaní informačných a komunikačných technológií podľa zásady ochrany súkromia už od štádia návrhu systému sa riziká pre ochranu súkromia a údajov môžu výrazne znížiť.

III.2. **Nedostatočné zavádzanie IKT uplatňujúcich zásadu ochrany súkromia už od štádia návrhu systému**

24. Dôležitou otázkou je, či sa hospodárske subjekty, výrobcovia/poskytovatelia IKT a prevádzkovatelia údajov zaujímajú o marketing a realizáciu zásady ochrana súkromia už od štádia návrhu systému. V tejto súvislosti je tiež dôležité posúdiť dopyt užívateľov po ochrane súkromia už od štádia návrhu systému.

25. Komisia vydala v roku 2007 oznámenie, v ktorom vyzvala podniky, aby využili svoju silu inovovať na vytvorenie a realizáciu technológií na ochranu súkromia ako spôsobu na zvýšenie ochrany súkromia a osobných údajov hneď od začiatku vývojového cyklu ([2]).

26. K dnešnému dňu však z dostupných dôkazov vyplýva, že ani výrobcom IKT, ani prevádzkovateľom údajov (buď v súkromnom alebo verejnom sektore) sa nepodarilo zásadu ochrany súkromia už od štádia návrhu systému dôsledne realizovať alebo uviesť na trh. Uvádzajú sa rôzne pohnútky vrátane nedostatku ekonomických stimulov alebo inštitucionálnej podpory, nedostatočného dopytu a pod ([3]).

27. Zároveň dopyt užívateľov po ochrane súkromia už od štádia návrhu systému je pomerne nízky. Užívatelia výrobkov a služieb IKT asi právom predpokladajú, že ich súkromie a osobné údaje sú *de facto* chránené, i keď v mnohých prípadoch nie sú. Niekedy jednoducho nedokážu prijať bezpečnostné opatrenia potrebné na ochranu buď svojich vlastných osobných údajov, alebo údajov iných. Mnohokrát preto, lebo buď celkom, alebo čiastočne nevedia o rizikách. Napríklad vo všeobecnosti mladí ľudia neberú na vedomie riziká pre súkromie súvisiace s odhalením osobných informácií na sociálnych sieťach a často ignorujú nastavenia ochrany súkromia. Aj keď ostatní užívatelia si uvedomujú riziká, nemusia však mať potrebné odborné znalosti na zavedenie ochranných technológií, napr. takých, ktoré chránia ich internetové pripojenie, alebo nevedia ako zmeniť nastavenie prehliadača na minimalizáciu profilovania založenom na sledovaní ich surfovania po webe.

28. A predsa sú riziká pre ochranu súkromia a údajov veľmi reálne. Ak sa ochrana súkromia a údajov nezohľadní od úplného začiatku, často je potom príliš neskoro

([1]) Pozri stanovisko európskeho dozorného úradníka pre ochranu údajov z 22. februára 2010 k oznámeniu Komisie o akčnom pláne zavádzania inteligentných dopravných systémov v Európe a k sprievodnému návrhu smernice Európskeho parlamentu a Rady, ktorou sa ustanovuje rámec na zavedenie inteligentných dopravných systémov v oblasti cestnej dopravy a na rozhrania s inými druhmi dopravy, k dispozícii na: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2009/09-07-22_Intelligent_Transport_Systems_EN.pdf

([2]) Oznámenie Komisie Európskemu parlamentu a Rade z 2.5.2007 o podpore ochrany údajov prostredníctvom technológií na zvyšovanie súkromia (PETs), KOM(2007) 228 v konečnom znení.

([3]) Štúdia o ekonomických výhodách technológií na zvyšovanie súkromia (PETS) jls/2008/D4/036.

a ekonomicky je príliš náročné nastaviť systémy a je príliš neskoro na nápravu spôsobených škôd. Rastúci počet porušení ochrany údajov v posledných rokoch dokonale dokazuje existenciu tohto problému a zdôrazňuje potrebu ochrany súkromia už od štádia návrhu systému.

29. Z uvedeného jasne vyplýva, že výrobcovia a dodávatelia technológií IKT určených na spracovanie osobných údajov by mali byť spolu s prevádzkovateľmi údajov zodpovední za to, aby sa tieto technológie navrhovali so zabudovanými bezpečnostnými zariadeniami na ochranu údajov a súkromia. V mnohých prípadoch by to znamenalo, že by sa mali navrhovať so štandardnými nastaveniami ochrany údajov.

30. V tejto súvislosti musíme posúdiť, aké opatrenia by mali tvorcovia politík prijať na podporu ochrany súkromia už od štádia návrhu systému pri vývoji IKT. Prvou otázkou je, či súčasný právny rámec na ochranu údajov obsahuje príslušné ustanovenia na zabezpečenie uplatňovania zásady ochrany súkromia už od štádia návrhu systému prevádzkovateľmi údajov, ako aj výrobcami/vývojármi. Druhou otázkou je, čo by sa malo urobiť v rámci európskeho digitálneho programu na zabezpečenie toho, aby sektor IKT získal dôveru spotrebiteľov.

IV. ZAHRNUTIE ZÁSADY OCHRANY SÚKROMIA UŽ OD ŠTÁDIA NÁVRHU SYSTÉMU DO ZÁKONOV A POLITÍK EÚ

IV.1. Súčasný právny rámec na ochranu údajov a súkromia

31. EÚ má rozsiahly rámec na ochranu údajov a súkromia zakotvený v smernici 95/46/ES ([1]), smernici 2002/58/ES ([2]) a judikatúre Európskeho súdu pre ľudské práva ([3]) a Súdneho dvora.

32. Smernica o ochrane údajov sa uplatňuje na „akúkoľvek operáciu alebo komplex operácií, ktorá sa vykonáva na osobných údajoch“ (zber, uchovávanie, zverejňovanie atď.). Ukladá tým, ktorí spracúvajú osobné údaje („prevádzkovatelia údajov“) dodržiavať určité zásady a povinnosti. Stanovuje individuálne práva, napr. právo na prístup k osobným údajom. Smernica o elektronickom súkromí sa zaoberá konkrétne ochranou súkromia v sektore elektronických komunikácií ([4]).

33. Súčasná smernica o ochrane údajov neobsahuje výslovnú požiadavku na ochranu súkromia už od štádia návrhu systému. Obsahuje však ustanovenia, ktoré nepriamo v rôznych situáciách môžu skutočne vyžadovať zavedenie zásady ochrany súkromia už od štádia návrhu systému. Najmä článok 17 vyžaduje, aby prevádzkovatelia údajov zaviedli príslušné technické a organizačné opatrenia na zabránenie nezákonnému spracovaniu ([5]). Ochrana súkromia už od štádia návrhu systému je teda zahrnutá len veľmi všeobecne. Okrem toho ustanovenia smernice sú určené najmä prevádzkovateľom údajov a ich spracovávaniu osobných údajov. Nevyžadujú výslovne, aby informačné a komunikačné technológie boli v súlade s ochranou súkromia a údajov, čo si tiež vyžaduje zamerať sa na konštruktérov a výrobcov IKT vrátane činností vykonávaných vo fáze normalizácie.

34. Smernica o elektronickom súkromí je presnejšia. V článku 14 ods. 3 sa uvádza, že „V prípade, že sa to požaduje, môžu sa prijať opatrenia, ktoré sa týkajú kompatibility konštrukcie koncového zariadenia s právom užívateľov na ochranu a kontrolu používania ich osobných údajov v súlade so smernicou 1999/5/ES a rozhodnutím Rady 87/95/EHS z 22. decembra 1986 o normalizácii v oblasti informačnej technológie a telekomunikácií“. Toto ustanovenie sa však nikdy nepoužilo ([6]).

35. Kým uvedené ustanovenia oboch smerníc sú užitočné na *presadzovanie* ochrany súkromia už od štádia návrhu systému, v praxi nie sú dostačujúce na *zabezpečenie* toho, aby sa ochrana súkromia zaviedla do IKT.

36. Výsledkom uvedenej situácie je, že právo dostatočne presne nevyžaduje, aby sa IKT navrhovali v súlade so zásadou ochrany súkromia už od štádia návrhu systému.

([1]) Smernica 95/46/ES Európskeho parlamentu a Rady (ďalej len „smernica o ochrane údajov“).

([2]) Smernica Európskeho parlamentu a Rady 2002/58/ES (ďalej len „smernica o elektronickom súkromí“).

([3]) Vysvetlenie hlavných prvkov a podmienok uvedených v článku 8 Európskeho dohovoru Rady Európy o ochrane ľudských práv a základných slobôd (EDĽP) prijatého v Ríme 4. novembra 1950, pretože sa uplatňujú na rôzne oblasti.

([4]) Lisabonská zmluva posilnila túto ochranu uznaním rešpektovania súkromného života a ochrany osobných údajov ako samostatných základných práv v článku 7 a 8 Charty základných práv EÚ. Charta základných práv EÚ sa stala záväznou po nadobudnutí účinnosti Lisabonskej zmluvy.

([5]) Článok 17 znie takto: „Členské štáty zabezpečia, zavedenie príslušných technických a organizačných opatrení na ochranu osobných údajov pred náhodným alebo nezákonným poškodením alebo náhodnej strate, zmene, neoprávnenému prezradeniu alebo sprístupneniu, najmä, kde spracovanie obsahuje prenos údajov cez sieť a proti všetkým iným nezákonným formám spracovania.“ Odôvodnenie 46 to dopĺňa týmto „keďže ochrana práv a slobôd osôb pracujúcich s údajmi v súvislosti so spracovaním osobných údajov si vyžaduje, aby sa vykonali primerané technické a organizačné opatrenia, aj v čase navrhovania systému spracovania aj v čase samotného spracovania, predovšetkým preto, aby sa udržala bezpečnosť, a tým sa predišlo akémukoľvek nedovolenému spracovaniu“.

([6]) Komisia oznámila, že koncom roka 2010 plánuje aktualizovať smernicu 1999/5/ES.

Ani orgány na ochranu údajov nemajú dostatočné právomoci, aby zabezpečili zavedenie tejto zásady. Výsledkom toho je neúčinnosť. Napríklad orgány na ochranu údajov môžu uložiť sankcie za neodpovedanie na žiadosti o prístup zo strany jednotlivcov a budú mať právomoci vyžadovať uplatňovanie určitých opatrení na zamedzenie nezákonného spracovania údajov. Pritom nie je vždy dostatočne jasné, či majú právomoci, aby mohli vyžadovať navrhovanie systému spôsobom, ktorý podporuje práva jednotlivcov na ochranu údajov ([1]). Napríklad na základe platných právnych predpisov nie je jasné, či by sa mohlo vyžadovať, aby architektúra informačného systému bola navrhnutá tak, aby podniky mohli odpovedať na žiadosti o prístup zo strany jednotlivcov spôsobom umožňujúcim, aby sa takéto žiadosti mohli riešiť automaticky a rýchlejšie. Okrem toho neskoršie snahy o zmenu technológie po ich návrhu alebo zavedení môžu mať za následok rôznorodé riešenia, ktoré úplne nefungujú, okrem toho, že sú ekonomicky nevýhodné.

37. Podľa stanoviska európskeho dozorného úradníka pre ochranu údajov spoločného so stanoviskom pracovnej skupiny zriadenej podľa článku 29 ([2]) existujúci právny rámec ponecháva priestor na jasnejšie potvrdenie zásady ochrany súkromia už od štádia návrhu systému.

IV.2. **Zavedenie ochrany súkromia už od štádia návrhu systému na rôznych úrovniach**

38. Vzhľadom na uvedené európsky dozorný úradník pre ochranu údajov odporúča Komisii, aby sledovala štyri smery činnosti, a síce aby:

a) navrhla zahrnúť všeobecné ustanovenie o ochrane súkromia už od štádia návrhu systému do právneho rámca na ochranu údajov.

b) vypracovala toto všeobecné ustanovenie v osobitných predpisoch po navrhnutí konkrétnych právnych nástrojov v jednotlivých sektoroch. Tieto osobitné ustanovenia by sa mohli už teraz zahrnúť do právnych nástrojov na základe článku 17 smernice o ochrane údajov (a iných existujúcich právnych predpisov).

c) zahrnula ochranu súkromia už od štádia návrhu systému ako vedúcu zásadu do digitálneho programu Európy.

d) zaviedla ochranu súkromia už od štádia návrhu systému ako zásadu do ďalších iniciatív EÚ (hlavne nelegislatívnych).

Všeobecné ustanovenie o ochrane súkromia už od štádia návrhu systému

39. Európsky dozorný úradník pre ochranu údajov navrhuje jednoznačne a výslovne zahrnúť zásadu ochrany súkromia už od štádia návrhu systému do existujúceho regulačného rámca v oblasti ochrany údajov. Tým by sa stala zásada ochrany súkromia už v štádiu návrhu silnejšou, explicitnejšou, čo prispeje k jej účinnému zavádzaniu a okrem toho by sa orgánom presadzovania práva zabezpečila väčšia legitimita na vyžadovanie jej skutočného uplatňovania v praxi. Je to obzvlášť potrebné vzhľadom na uvedené skutočnosti, a to nielen z hľadiska samotného významu ako nástroja na posilnenie dôvery, ale aj ako stimulu pre zainteresované strany na zavedenie zásady ochrany súkromia už v štádiu návrhu a posilnenia záruk, ktoré sú uvedené v existujúcom právnom rámci.

40. Tento návrh vychádza z odporúčania pracovnej skupiny zriadenej podľa článku 29, aby sa zásada „ochrany súkromia už v štádiu návrhu“ zaviedla ako všeobecná zásada do právneho rámca na ochranu údajov, najmä do smernice o ochrane údajov. Podľa pracovnej skupiny zriadenej podľa článku 29: „Táto zásada by mala byť záväzná pre konštruktérov a výrobcov technológií, ako aj pre prevádzkovateľov údajov, ktorí musia rozhodnúť o nadobudnutí a využívanie IKT. Mali by povinne zohľadňovať technologickú ochranu údajov už v štádiu plánovania informačno-technologických postupov a systémov. Poskytovatelia takýchto systémov alebo služieb, ako aj prevádzkovatelia údajov by mali preukázať, že prijali všetky opatrenia potrebné na dosiahnutie súladu s týmito požiadavkami“.

41. Európsky dozorný úradník pre ochranu údajov tiež víta, že komisárka Viviane Reding potvrdila zásadu ochrany súkromia už v štádiu návrhu v rámci oznámenia revízie smernice o ochrane údajov ([3]).

42. Toto vedie k obsahu takého predpisu. Najdôležitejšie je, aby všeobecná zásada ochrany súkromia už v štádiu návrhu bola technologicky neutrálna. Cieľom tejto zásady by nemala byť regulácia technológií, t. j. nemala by predpisovať konkrétne technické riešenia. Namiesto toho by mala predpisovať integráciu existujúcich zásad ochrany

([1]) Pozri správu Úradu komisára pre informácie Spojeného kráľovstva s názvom: „Privacy by Design“ *(Ochrana súkromia už od štádia návrhu systému)*, uverejnenú v novembri 2008.

([2]) Stanovisko 168 pracovnej skupiny zriadenej podľa článku 29 o budúcnosti súkromia, spoločný príspevok ku konzultáciám Európskej komisie o právnom rámci pre základné právo na ochranu osobných údajov, prijaté 1. decembra 2009.

([3]) „Ochrana súkromia už v štádiu návrhu je zásadou, ktorá je v záujme občanov i podnikov. Ochrana súkromia už v štádiu návrhu povedie k lepšej ochrane jednotlivcov, ako aj k dôvere a viere v nové služby a výrobky, čo bude mať zase pozitívny vplyv na ekonomiku. Vidím niektoré povzbudivé príklady, je však ešte potrebné urobiť oveľa viac“. Zásadný prejav v Deň ochrany údajov, 28. januára 2010, Európsky parlament, Brusel.

súkromia a údajov do informačných a komunikačných systémov a riešení. Umožnilo by to zainteresovaným stranám, výrobcom, prevádzkovateľom údajov a orgánom na ochranu údajov interpretovať význam zásady v každom jednotlivom prípade. Po druhé, dodržiavanie zásady by malo byť povinné v jednotlivých štádiách, od tvorby noriem a navrhovania architektúry až po ich zavádzanie prevádzkovateľom údajov.

Ustanovenia v konkrétnych právnych nástrojoch

43. Súčasné a budúce legislatívne nástroje musia integrovať zásadu ochrana súkromia už v štádiu návrhu na základe existujúceho právneho rámca a po prijatí všeobecného ustanovenia uvedeného vyššie, a to na základe tohto posledného zmieneného ustanovenia. Napríklad podľa súčasných iniciatív týkajúcich sa inteligentných dopravných systémov Komisia bude znášať osobitnú počiatočnú zodpovednosť pri stanovovaní opatrení, iniciatív v oblasti normalizácie, postupov a osvedčených postupov. Pri vykonávaní týchto úloh by ochrana súkromia už od štádia návrhu systému mala byť hlavnou zásadou.

44. Európsky dozorný úradník pre ochranu údajov ďalej konštatuje, že zásada ochrany súkromia od štádia návrhu systému má tiež osobitný význam v oblasti slobody, bezpečnosti a spravodlivosti, najmä vo vzťahu k plneniu cieľov stratégie riadenia informácií, ako sa predpokladá v Štokholmskom programe ([1]). Vo svojom stanovisku týkajúcom sa Štokholmského programu európsky dozorný úradník pre ochranu údajov zdôraznil, že architektúra na výmenu informácií by mala byť založená na „ochrane súkromia už v štádiu návrhu" ([2]): „To konkrétnejšie znamená, že informačné systémy, ktoré sú určené na účely verejnej bezpečnosti by sa mali vždy budovať v súlade so zásadou ochrana súkromia už v štádiu návrhu".

45. V stanovisku pracovnej skupiny zriadenej podľa článku 29 o budúcnosti súkromia ([3]) sa kladie dôraz dokonca na ešte presnejšie podmienky ako v priestore slobody, bezpečnosti a spravodlivosti – kde verejné orgány sú hlavnými aktérmi a kde opatrenia spočívajúce vo zvýšení dohľadu priamo ovplyvňujú základné práva na ochranu súkromia a údajov – požiadavky na ochranu súkromia od štádia návrhu systému by mali byť povinné. Zavedením týchto požiadaviek do informačných systémov by vlády podnietili aj ochranu súkromia od štádia návrhu systému vo svojom postavení prvých klientov.

Ochrana súkromia už od štádia návrhu systému ako prvoradá zásada v digitálnom programe Európy

46. Informačné a komunikačné technológie sú čoraz zložitejšie a znamenajú väčšie riziká pre ochranu súkromia a údajov. Všeobecne platí, že digitalizované informácie, ku ktorým je ľahší prístup, ktoré sa ľahšie dajú kopírovať a posielať, sú vystavené oveľa väčším rizikám ako tlačené informácie. Posunom k sieťam vzájomne prepojených objektov sa riziká budú zvyšovať. Čím väčšie budú riziká pre ochranu súkromia/údajov, tým väčší bude dopyt po posilnení bezpečnostných opatrení na ochranu údajov/súkromia. Preto sú dôvody na zavedenie ochrany súkromia od štádia návrhu systému naliehavejšie v sektore IKT. Okrem toho, ako už bolo uvedené, podstatná je dôvera jednotlivcov v IKT, ak majú občania prijať tieto nové služby a ochrana súkromia a údajov je kľúčovým prvkom tejto dôvery.

47. Z uvedeného vyplýva, že stratégia vývoja IKT musí potvrdiť, že je potrebné, aby sa navrhovali so zabudovaným prvkom ochrany súkromia a údajov, t. j. aby sa zohľadnila zásada ochrany súkromia už v štádiu návrhu.

48. V európskom digitálnom programe by sa preto mala výslovne potvrdiť zásada ochrany súkromia už v štádiu návrhu ako nevyhnutný prvok na zabezpečenie dôvery občanov v IKT a on-line služby. Malo by sa uznať, že ochrana súkromia a dôvera navzájom súvisia a že ochrana súkromia už v štádiu návrhu by mala byť hlavným faktorom vo vývoji dôveryhodného sektora IKT.

Ochrana súkromia už od štádia návrhu systému ako zásada v iných iniciatívach EÚ

49. Pre Komisiu by ochrana súkromia od štádia návrhu systému mala byť prvoradou zásadou pri uskutočňovaní politík, činností a iniciatív v konkrétnych sektoroch IKT vrátane elektronického zdravotníctva (*eHealth*), elektronického verejného obstarávania (*eProcurement*), elektronického sociálneho zabezpečenia (*eSocial Security*), elektronického vzdelávania (*eLearning*) atď. Mnohé z týchto iniciatív budú uvedené v európskom digitálnom programe.

50. To znamená napríklad, že iniciatívy na zabezpečenie, aby vládne aplikácie boli účinnejšie a modernejšie tak, aby sa jednotlivci mohli komunikovať so správami, by mali zahŕňať aj potrebu, aby boli navrhnuté a prevádzkované v súlade so zásadou ochrany súkromia od štádia návrhu systému. To isté platí pre politiky a aktivity Komisie na zaistenie rýchlejšieho internetu, digitálneho obsahu alebo na celkovú podporu pevných a bezdrôtových komunikácií a prenosu údajov.

([1]) Štokholmský program – Otvorená a bezpečná Európa, ktorá slúži občanom a chráni ich, schválený Európskou radou v decembri 2009.

([2]) Stanovisko z 10. júla 2009 k oznámeniu Komisie Európskemu parlamentu a Rade o priestore slobody, bezpečnosti a spravodlivosti pre občanov, Ú. v. EÚ C 276, 17.11.2009, s. 8, bod 60.

([3]) Stanovisko 168 pracovnej skupiny zriadenej podľa článku 29 o budúcnosti súkromia, Spoločný príspevok ku konzultáciám Európskej komisie o právnom rámci pre základné právo na ochranu osobných údajov, prijaté 1. decembra 2009.

51. Uvedené zahŕňa aj oblasti, kde Komisia je zodpovedná za rozsiahle IT systémy, ako napr. SIS a VIS, ako aj za tie prípady, keď sa zodpovednosť Komisie obmedzuje na rozvoj a údržbu spoločnej infraštruktúry takého systému, ako napr. Európsky informačný systém registrov trestov (ECRIS).

52. Ako presne sa zásada ochrany súkromia od štádia návrhu systému bude rozvíjať, bude závisieť od každého jednotlivého sektoru a situácie. Napríklad, ak iniciatívy Komisie budú sprevádzať legislatívne návrhy týkajúce sa konkrétneho sektora IKT, mnohokrát bude vhodné zahrnúť výslovný odkaz na pojem ochrana súkromia od štádia návrhu systému týkajúci sa návrhu konkrétnej aplikácie alebo systému IKT. Ak sa budú navrhovať akčné plány pre konkrétnu oblasť, mali by systematicky zabezpečovať uplatňovanie právneho rámca a najmä zaručiť, aby sa príslušné technológie IKT budovali s prihliadnutím na ochranu súkromia od štádia návrhu systému.

53. Pokiaľ ide o výskum, mal by sa použiť siedmy rámcový program a nasledovné programy ako nástroj na podporu projektov zameraných na analyzovanie noriem, IKT technológií a architektúry, ktoré lepšie poslúžia ochrane súkromia a najmä zásade ochrany súkromia od štádia návrhu systému. Okrem toho ochrana súkromia od štádia návrhu systému by tiež mala byť nevyhnutným prvkom, ktorý sa bude posudzovať v rozsiahlejších projektoch IKT zameraných na spracovanie osobných údajov jednotlivcov.

Oblasti osobitného záujmu

54. V niektorých prípadoch na základe osobitných rizík pre ochranu súkromia a údajov jednotlivcov alebo na základe iných faktorov (neochota priemyselného odvetvia dodávať výrobky zohľadňujúce ochranu súkromia od štádia návrhu systému, spotrebiteľský dopyt a pod.) môže byť potrebné stanoviť presnejšie a konkrétnejšie opatrenia na ochranu súkromia už v štádiu návrhu, ktoré sa musia zaviesť do daného typu produktu/technológie v oblasti IKT buď v legislatívnych nástrojoch, alebo nelegislatívnych nástrojoch.

55. Európsky dozorný úradník pre ochranu údajov uviedol viaceré oblasti (RFID, sociálne siete a aplikácie prehliadačov), ktoré podľa neho v tomto štádiu vyžadujú dôkladné posúdenie zo strany Komisie a praktickejší zásah odporučený vyššie. Tieto tri oblasti sa ďalej podrobnejšie rozoberajú.

V. **RADIOFREKVENČNÁ IDENTIFIKÁCIA – RFID**

56. Štítky RFID sa môžu integrovať do objektov, zvierat a ľudí. Môžu sa použiť na zhromažďovanie a uchovávanie osobných údajov, ako napr. lekárske záznamy, sledovanie pohybu osôb alebo získanie prehľadu o ich správaní na rôzne účely. Je to možné robiť bez toho, aby o tom jednotlivci vedeli ([1]).

57. Účinné záruky týkajúce sa ochrany údajov, súkromia a všetkých súvisiacich etických rozmerov majú zásadný význam pre dôveru verejnosti v RFID a budúcnosť internetu vecí. Len potom môže technológia poskytovať množstvo hospodárskych a spoločenských výhod.

V.1. **Medzery v platnom právnom rámci na ochranu údajov**

58. Smernica o ochrane údajov a smernica o elektronickom súkromí sa vzťahujú na zhromažďovanie údajov vykonávané prostredníctvom aplikácií RFID ([2]). Vyžadujú si okrem iného, aby sa na prevádzku aplikácií RFID zaviedli primerané bezpečnostné opatrenia na ochranu súkromia ([3]).

59. Tento právny rámec však úplne nerieši všetky aspekty ochrany údajov a súkromia tejto technológie, ktoré vyvolávajú obavy, pretože tieto smernice nie sú dostatočne podrobné, čo sa týka typu bezpečnostných opatrení, ktoré by sa mali zaviesť do aplikácií RFID. Súčasné

([1]) RFID znamená rádiofrekvenčnú identifikáciu. Hlavnými súčasťami technológie rádiofrekvenčnej identifikácie *alebo* infraštruktúry sú *štítok* (t. j. mikročip), čítačka a aplikácia súvisiaca so štítkami a čítačkami prostredníctvom midlevéru a spracovaním poskytnutých údajov. Štítok pozostáva z elektronického obvodu, v ktorom sa uchovávajú údaje a antény, ktorou sa prenášajú údaje rádiovými vlnami. Čítačka pozostáva z antény a demodulátora, ktorý prekladá prichádzajúce analógové informácie z rádiového spojenia na digitálne údaje. Informácie sa potom môžu odoslať prostredníctvom sietí do databáz a serverov, aby sa mohli počítačovo spracovať.

([2]) V smernici o elektronickom súkromí sa uvádza odkaz na RFID v článku 3 „Táto smernica sa vzťahuje na spracúvanie osobných údajov v súvislosti s poskytovaním verejne dostupných elektronických komunikačných služieb vo verejných komunikačných sieťach v Spoločenstve vrátane verejných komunikačných sietí, ktoré podporujú zariadenia na zber údajov a identifikáciu.“ Toto dopĺňa odôvodnenie 56 „Pokrok v technológiách umožňuje vyvíjať nové aplikácie na základe zariadení určených na zhromažďovanie a identifikáciu údajov, pričom tými zariadeniami môžu byť bezkontaktné zariadenia využívajúce rádiové frekvencie. Napríklad zariadenia na identifikáciu pomocou rádiovej frekvencie [Radio Frequency Identification Devices (RFID)] využívajú rádiové frekvencie na zachytenie údajov z jedinečne označených štítkov; údaje sa potom môžu preniesť cez existujúce komunikačné siete. Široké využívanie takýchto technológií môže priniesť značné hospodárske a spoločenské výhody a môže byť výrazným prínosom pre vnútorný trh, ak ich využívanie bude prijateľné pre občanov. Na dosiahnutie tohto cieľa je potrebné zabezpečiť ochranu základných práv jednotlivcov vrátane ich práva na súkromie a ochranu údajov. Keď sú takéto zariadenia pripojené na verejne dostupné elektronické komunikačné siete alebo keď využívajú elektronické komunikačné služby ako základnú infraštruktúru, mali by sa uplatňovať príslušné ustanovenia smernice 2002/58/ES (smernica o súkromí a elektronických komunikáciách) vrátane ustanovení o bezpečnosti, prevádzke a lokalizačných dátach, ako aj ustanovení o dôvernosti.“

([3]) Napríklad v článku 17 smernice o ochrane údajov sa ukladá povinnosť zaviesť príslušné technické a organizačné opatrenia na ochranu osobných údajov pred náhodným alebo nezákonným poškodením alebo neoprávnenému prezradeniu.

pravidlá je potrebné doplniť o ďalšie, ktorými sa uložia osobitné bezpečnostné opatrenia, najmä uložením povinnosti zaviesť technické riešenia (ochrana súkromia od štádia návrhu systému) do technológie RFID. Platí to pre štítky, na ktorých sa uchovávajú osobné údaje a ktoré by mali mať príkazy na ukončenie a v štítkoch uchovávajúcich určité druhy osobných informácií by sa mala využívať kryptografia.

V.2. **Samoregulácia ako prvý krok**

60. V marci 2007 Komisia prijala oznámenie ([1]), v ktorom okrem iného uznala, že je potrebné podrobné usmernenie k praktickému vykonávaniu RFID a že je vhodné prijať kritériá pre navrhovanie, aby sa zabránilo rizikám pre súkromie a bezpečnosť.

61. Na dosiahnutie týchto cieľov Komisia prijala v máji 2009 odporúčanie o vykonávaní zásad ochrany súkromia a údajov v aplikáciách RFID ([2]). V maloobchodnom predaji aplikácií RFID sa požaduje deaktivácia štítku v mieste predaja, pokiaľ jednotlivci nevyjadrili súhlas. Toto sa uplatňuje, pokiaľ hodnotenie vplyvu na ochranu súkromia a údajov nepreukáže, že štítky nepredstavujú pravdepodobnú hrozbu pre súkromie alebo ochranu osobných údajov a v takomto prípade by zostali funkčné bez poplatkov po mieste predaja, pokiaľ jednotlivci nerozhodnú pre možnosť tzv. opt-out (deaktiváciu).

62. Európsky dozorný úradník pre ochranu údajov súhlasí s prístupom Komisie, že sa budú využívať samoregulačné nástroje. Ako sa však uvádza ďalej v texte, je možné, že samoregulácia neprinesie očakávané výsledky, a preto ho vyzýva Komisiu, aby bola pripravená prijať alternatívne opatrenia.

V.3. **Oblasti vyvolávajúce obavy a možné ďalšie opatrenia v prípade zlyhania samoregulácie**

63. Európsky dozorný úradník pre ochranu údajov je znepokojený tým, že organizácie prevádzkujúce aplikácie RFID v maloobchodnom sektore môžu opomenúť existenciu možnosti sledovania štítkov RFID nežiaducimi tretími stranami. Takéto sledovanie by mohlo odhaliť osobné údaje uchovávané na štítku (ak existujú), umožnilo by však tretej strane tiež sledovať alebo identifikovať osobu v priebehu času jednoducho na základe jedinečných identifikátorov nachádzajúcich sa na jednom alebo viacerých štítkoch, ktoré má jednotlivec pri sebe, v prostredí, ktoré môže byť dokonca mimo prevádzkového obvodu aplikácie RFID. Ďalej ho znepokojuje, že prevádzkovateľov aplikácií RFID môže lákať prílišné spoliehanie sa na výnimku, a tak môžu ponechať štítok funkčný aj po opustení predajného miesta.

64. Ak dôjde k uvedenej situácii, môže byť príliš neskoro na zmiernenie rizík pre ochranu údajov a súkromia jednotlivcov, ktoré už bolo ohrozené. Okrem toho vzhľadom na charakter samoregulácie vnútroštátne orgány presadzovania práva môžu byť v slabšej pozícii, keď budú vyžadovať od organizácií prevádzkujúcich aplikácie RFID, aby uplatňovali osobitné opatrenia v rámci ochrany súkromia od štádia návrhu systému.

65. Vzhľadom na uvedené európsky dozorný úradník pre ochranu údajov vyzýva Komisiu, aby bola pripravená navrhnúť legislatívne nástroje upravujúce hlavné otázky používania RFID v prípade, keď zlyhá efektívne uplatňovanie existujúceho právneho rámca. Komisia by nemala príliš odkladať svoje hodnotenie. Odkladom by sa ohrozili jednotlivci a bolo by tiež kontraproduktívne pre priemysel, pretože právne neistoty sú príliš vysoké a je väčšia pravdepodobnosť, že zakorenené problémy sa budú ťažšie a nákladnejšie napravovať.

66. V rámci opatrení, ktoré môže byť potrebné navrhnúť, európsky dozorný úradník pre ochranu údajov odporúča ustanoviť zásadu predchádzajúceho súhlasu s aktiváciou (*opt-in*) v mieste predaja, podľa ktorej by sa všetky štítky RFID pripojené k spotrebnému tovaru štandardne deaktivovali v mieste predaja. Nie je potrebné, ani vhodné, aby Komisia špecifikovala konkrétnu technológiu, ktorá sa má použiť. Namiesto toho sa v práve Únie musí ustanoviť právna povinnosť získať predchádzajúci súhlas, takže prevádzkovateľom sa poskytne priestor, aby rozhodli o spôsobe, ako splniť túto požiadavku.

V.4. **Ďalšie otázky, ktoré je potrebné posúdiť: riadenie internetu vecí**

67. Informácie poskytované štítkami RFID, napr. informácie o výrobku, sa môžu prípadne prepojiť do celosvetovej siete komunikačnej infraštruktúry. Obvykle sa to označuje ako „internet vecí“. Objavujú sa otázky týkajúce sa ochrany údajov/súkromia, pretože objekty reálneho sveta môžu byť označené štítkami RFID, ktoré okrem informácií o výrobku môžu obsahovať osobné údaje.

68. Existuje mnoho otvorených otázok o tom, kto bude riadiť uchovávanie informácií v súvislosti s predmetmi označenými štítkami. Ako sa to bude organizovať? Kto k nim bude mať prístup? V júni 2009 Komisia prijala oznámenie o internete vecí ([3]), v ktorom výslovne uviedla potenciálne problémy ochrany údajov a súkromia v súvislosti s týmto fenoménom.

([1]) Oznámenie Komisie Rade, Európskemu parlamentu, Európskemu hospodárskemu a sociálnemu výboru a výboru regiónov z 15.3.2007 – Rádiofrekvenčná identifikácia (RFID) v Európe: kroky k politickému rámcu, KOM(2007) 96 v konečnom znení.

([2]) Odporúčanie Komisie z 12.5.2009 o vykonávaní zásad ochrany súkromia a údajov v aplikáciách podporovaných rádiofrekvenčnou identifikáciou [(K(2009) 3200 v konečnom znení)].

([3]) Oznámenie Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov Internet vecí – akčný plán pre Európu, KOM(2009) 278 v konečnom znení.

69. Európsky dozorný úradník pre ochranu údajov by rád poukázal na niektoré z otázok v oznámení, ktoré si podľa jeho názoru zaslúžia zvýšenú pozornosť, keďže internet vecí sa vyvíja. Po prvé, zodpovednosť a vymáhateľnosť právneho rámca EÚ sa môže zvýšiť potrebou decentralizovanej architektúry. Po druhé, právo jednotlivcov nebyť sledovaní by sa malo v najvyššej možnej miere zachovať. Inými slovami, možnosť sledovať jednotlivcov pomocou štítkov RFID bez ich súhlasu by mala existovať len vo veľmi obmedzených prípadoch. Tento súhlas by mal byť jasný. Obvykle sa to označuje ako „mlčanie čipov" a právo nebyť obťažovaní. A napokon, pri navrhovaní internetu vecí by zásada ochrany súkromia od štádia návrhu systému mala byť hlavnou zásadou. Vyžadovalo by si to napríklad, aby sa konkrétne aplikácie RFID, ktoré majú zabudované mechanizmy na poskytovanie kontroly užívateľom, navrhovali so štandardnými nastaveniami ochrany údajov.

70. Európsky dozorný úradník pre ochranu údajov očakáva, že sa s ním bude konzultovať, keďže Komisia zavádza opatrenia predpokladané v oznámení, a to najmä návrh oznámenia o súkromí a dôvere vo všadeprítomnú informačnú spoločnosť.

VI. SOCIÁLNE SIETE A POTREBA ŠTANDARDNÝCH NASTAVENÍ OCHRANY SÚKROMIA

71. Sociálne siete sú „hitom mesiaca". Zdá sa, že v obľúbenosti prekonávajú e-mail. Spájajú navzájom ľudí, ktorí majú podobné záujmy a/alebo činnosti. Ľudia môžu mať svoje profily on-line a môžu so vymieňať mediálne súbory, ako napr. videá, fotografie, hudbu, ako aj svoje profesijné profily.

72. Mladí ľudia si rýchlo osvojili zapájanie sa do sociálnych sietí a tento trend pokračuje. Priemerný vek užívateľov internetu v posledných rokoch v Európe klesol: 9 – 10-roční sa pripájajú niekoľkokrát za týždeň, 12 – 14-roční sú on-line každý deň, často jednu až tri hodiny.

VI.1. Sociálne siete a platný právny rámec na ochranu údajov a súkromia

73. Rozvoj sociálnych sietí umožnil užívateľom vkladať na internet informácie o sebe a tretích stranách. Pri tejto činnosti podľa pracovnej skupiny zriadenej podľa článku 29 ([1]) užívatelia internetu konajú v prípade údajov, ktoré vkladajú, ako prevádzkovatelia údajov, bývalý článok 2 písm. d) smernice o ochrane údajov ([2]). Vo väčšine prípadov však takéto spracovanie spadá pod výnimku pre domácnosti podľa bývalého článku 3 ods. 2 smernice. Zároveň sa služby sociálnych sietí považujú za prevádzkovateľov údajov, pretože poskytujú prostriedky na spracovanie údajov užívateľov a poskytujú všetky základné služby súvisiace so správou užívateľov (napr. registrácia a vymazanie účtov).

74. Z právneho hľadiska to znamená, že užívatelia internetu a služieb sociálnych sietí majú spoločnú zodpovednosť za spracovanie osobných údajov ako „prevádzkovatelia údajov" v zmysle článku 2 písm. d) smernice, aj keď v rôznej miere a s odlišnými povinnosťami.

75. Na základe toho by užívatelia mali vedieť a rozumieť, že tým, že spracovávajú svoje osobné informácie a informácie o iných osobách, spadajú pod ustanovenia právnych predpisov EÚ o ochrane údajov, ktoré okrem iného vyžadujú získanie informovaného súhlasu tých osôb, ktorých informácie sa vkladajú a poskytnutie tým, ktorých sa to týka, právo na opravu, právo vzniesť námietky a pod. Podobne musia služby sociálnych sietí prijať okrem iného primerané technické a organizačné opatrenia, aby zabránili neoprávnenému spracovaniu, s prihliadnutím na riziká v súvislosti so spracovaním údajov a charakterom údajov. Toto zase znamená, že služby sociálnych sietí by mali zabezpečiť štandardné nastavenia zohľadňujúce ochranu súkromia vrátane nastavení, ktoré vyhradzujú prístup k profilom pre kontakty vybrané samotným užívateľom. Nastavenia by mali tiež požadovať potvrdzujúci súhlas užívateľa predtým, ako sa akýkoľvek profil sprístupní ďalším tretím stranám a vyhradené prístupové profily by nemali byť identifikovateľné pomocou interných vyhľadávačov.

76. Žiaľ, medzi právnymi požiadavkami a skutočným dodržiavaniam je rozdiel. Kým z právneho hľadiska sa užívatelia internetu považujú za prevádzkovateľov údajov a sú viazaní právnym rámcom EÚ na ochranu údajov a súkromia, v skutočnosti často nevedia o tejto úlohe. Vo všeobecnosti dobre nechápu, že spracovávajú osobné údaje a že zverejňovanie takýchto informácií zahŕňa riziká pre ochranu súkromia a údajov. Predovšetkým mladí ľudia posielajú obsah online a podceňujú dôsledky, ktoré z toho môžu vyplynúť pre nich a ostatných, napríklad v súvislosti s následným zápisom do vzdelávacích inštitúcií alebo žiadosťami o zamestnanie.

([1]) Pozri stanovisko 163, 5/2009 pracovnej skupiny zriadenej podľa článku 29 k on-line sociálnym sieťam prijaté 12. júna 2009.

([2]) „Prevádzkovateľ" znamená fyzickú alebo právnickú osobu, verejný orgán, agentúru alebo akýkoľvek iný orgán, ktorý sám alebo v spojení s inými určuje účely a prostriedky spracovania osobných údajov; tam, kde sú účely a prostriedky spracovania stanovené vnútroštátnymi zákonmi a nariadeniami, alebo zákonmi a nariadeniami Spoločenstva, ten, kto spracovanie riadi, alebo konkrétne kritériá pre jeho menovanie môžu byť navrhnuté na základe vnútroštátneho práva alebo práva Spoločenstva.

77. Zároveň poskytovatelia sociálnych sietí často vopred zvolia štandardné nastavenia založené na tzv. možnosti *opt-out*, a tak umožnia zverejňovanie osobných informácií. Niektoré umožňujú, aby boli profily štandardne prístupné bežným vyhľadávačom. Vyvoláva to otázky týkajúce sa toho, či jednotlivci skutočne súhlasili so zverejnením, ako aj toho, či sociálne siete dodržiavajú článok 17 smernice (pozri vyššie), v ktorom sa požaduje, aby prijali primerané technické a organizačné opatrenia na zabránenie neoprávnenému spracovaniu.

VI.2. **Riziká sociálnych sietí a navrhované opatrenia na ich riešenie**

78. Z uvedeného vyplýva zvýšené riziko pre ochranu súkromia a údajov jednotlivcov. Na základe toho sú užívatelia internetu a osoby, ktorých údaje boli vložené, vystavení zjavnému porušovaniu ochrany súkromia a údajov.

79. V tejto súvislosti by sa Komisia mala zaoberať otázkou, čo by sa malo a mohlo urobiť na riešenie tejto situácie. Toto stanovisko neposkytuje vyčerpávajúcu odpoveď na túto otázku, namiesto toho sa však v ňom predkladá niekoľko návrhov na ďalšie zváženie.

Investícia do výchovy užívateľov internetu

80. Prvým návrhom je investovať do výchovy užívateľa. V tejto súvislosti by inštitúcie EÚ a vnútroštátne orgány mali investovať do výchovy a zvyšovania povedomia o hrozbách, ktoré predstavujú webové stránky sociálnych sietí. Napríklad GR pre informačnú spoločnosť spustilo program Bezpečnejší internet, ktorý je zameraný na podporu a ochranu detí a mladých ľudí napríklad pomocou aktivít na zvyšovanie informovanosti ([1]). Inštitúcie EÚ spustili nedávno kampaň „Premysli si, čo zverejníš!“ na zvýšenie informovanosti o rizikách výmeny osobných informácií s cudzími ľuďmi.

81. Európsky dozorný úradník pre ochranu informácií vyzýva Komisiu, aby aj naďalej podporovala tento druh činnosti. Samotní poskytovatelia sociálnych sietí by však mali zohrávať aktívnu úlohu, pretože sú právne a spoločensky zodpovední za vzdelávanie užívateľov v tom, ako majú využívať ich služby spôsobom, ktorý je bezpečný a zohľadňuje súkromie.

82. Ako už bolo uvedené, pri zverejňovaní informácií na sociálnych sieťach, informácie sa môžu štandardne sprístupniť mnohých rôznymi cestami. Napríklad informácie môžu byť prístupné širokej verejnosti vrátane vyhľadávačov, ktoré ich môžu označiť indexom, a tak poskytnúť na ne priame odkazy. Na druhej strane informácie môžu byť vyhradené pre „vybraných priateľov“ alebo môžu byť úplne súkromné. Je zrejmé, že používané profilové oprávnenia a terminológia sú odlišné na jednotlivých lokalitách.

83. Ako však už bolo uvedené, len veľmi málo užívateľov služieb sociálnych sietí vie, ako kontrolovať prístup k informáciám, ktoré zverejňujú, a tobôž, ako zmeniť štandardné nastavenia ochrany osobných údajov. Nastavenia ochrany osobných údajov zvyčajne zostávajú bezo zmeny, pretože si neuvedomujú dôsledky toho, čo sa stane, keď ich nezmenia, alebo nevedia, ako to urobiť. Nezmenenie nastavení ochrany súkromia teda častejšie neznamená, že jednotlivci poskytli informované rozhodnutie, že súhlasia s výmenou informácií. V tejto súvislosti je obzvlášť dôležité, aby tretie strany, ako napríklad vyhľadávače sa nepripojili k jednotlivým profilom v domnienke, že používatelia štandardne súhlasili (nezmenením nastavenia ochrany osobných údajov), že informácie budú dostupné bez obmedzení.

84. Aj keď výchova užívateľov môže pomôcť pri riešení tejto situácie, samé to nebude fungovať. Ako vyplýva z odporúčaní pracovnej skupiny zriadenej podľa článku 29 v jej stanovisku k sociálnym sieťam, poskytovatelia sociálnych sietí by mali ponúkať bezplatné štandardné nastavenia zohľadňujúce súkromie. Takto by si užívatelia viac uvedomili svoje konanie a umožnilo by im to uskutočňovať lepšie rozhodnutia, pokiaľ ide o to, či si chcú vymieňať informácie a s kým.

Úloha samoregulácie

85. Komisia uzavrela dohodu s dvadsiatimi poskytovateľmi sociálnej siete známu ako „Bezpečnejšie zásady sociálnych sietí pre EÚ“ ([2]). Cieľom dohody je zvýšiť bezpečnosť neplnoletých pri využívaní lokalít sociálnych sietí v Európe. Tieto zásady zahŕňajú mnohé už uvedené požiadavky odvodené z uplatňovania právneho rámca na ochranu údajov. Patrí k nim napríklad požiadavka oprávniť užívateľov prostredníctvom nástrojov a technológií, aby sa zabezpečilo, že budú môcť kontrolovať využívanie a šírenie svojich osobných údajov. Zahŕňajú aj potrebu poskytovať štandardné nastavenie ochrany súkromia.

86. Začiatkom januára 2010 Komisia sprístupnila závery správy, v ktorej sa hodnotila realizácia zásad ([3]). Európskeho dozorného úradníka pre ochranu informácií znepokojuje, ako z tejto správy vyplýva, že aj keď sa síce niektoré kroky podnikli, mnoho ďalších nie. V správe sa

([1]) Informácie o tomto programe sú k dispozícii na: http://ec.europa.eu/information_society/activities/sip/index_en.htm

([2]) Tieto zásady sú k dispozícii na: http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf

([3]) Správa o hodnotení realizácie Bezpečnejšie zásady sociálnych sietí pre EÚ je k dispozícii na: http://ec.europa.eu/information_society/activities/social_networking/docs/final_report/first_part.pdf

napríklad uvádzalo, že sa zistili problémy týkajúce sa oznamovania bezpečnostných opatrení a nástrojov dostupných na týchto lokalitách. Zistilo sa tiež, že menej ako polovica zo signatárov dohody vyhradzuje prístup k profilom neplnoletých len pre ich priateľov.

Potreba povinných štandardných nastavení ochrany súkromia

87. V tejto súvislosti je rozhodujúce, či sú potrebné ďalšie politické opatrenia na zabezpečenie, aby sociálne siete zriaďovali svoje služby so štandardnými nastaveniami ochrany súkromia. Na toto upozornila bývalá komisárka pre informačnú spoločnosť Viviane Reding a uviedla, že môže byť potrebná právna úprava ([1]). Rovnako aj Európsky hospodársky a sociálny výbor uviedol, že popri samoregulácii by sa mali minimálne úrovne ochrany uložiť právnym predpisom ([2]).

88. Ako už bolo uvedené, povinnosť poskytovateľov sociálnych sietí zaviesť štandardné nastavenia ochrany súkromia možno odvodiť nepriamo z článku 17 smernice o ochrane údajov ([3]), v ktorom sa prevádzkovateľom údajov ukladá prijať primerané technické a organizačné opatrenia („aj v čase navrhovania systému spracovania aj v čase samotného spracovania“) na udržanie bezpečnosti a zabránenie neoprávnenému spracovaniu s prihliadnutím na riziká v súvislosti so spracovaním údajov a charakterom údajov.

89. Tento článok je však príliš všeobecný a chýba mu konkrétne zameranie, aj v tejto súvislosti. Neuvádza sa v ňom jasne, čo znamenajú primerané technické a organizačné opatrenia v súvislosti so sociálnymi sieťami. Súčasná situácia je preto prípadom právnej neistoty, čo spôsobuje problémy tak regulačným orgánom, ako aj jednotlivcom, ktorých súkromie a osobné údaje nie sú plne chránené.

90. Vzhľadom na uvedené, európsky dozorný úradník pre ochranu informácií vyzýva Komisiu, aby pripravila právne predpisy, ktoré by minimálne obsahovali všeobecnú povinnosť vyžadujúcu povinné nastavenia ochrany súkromia spolu s presnejšími požiadavkami:

a) zabezpečiť nastavenia, ktoré prístup k profilom užívateľov vyhradzujú pre kontakty vybrané samotným užívateľom; nastavenia by mali tiež vyžadovať súhlas užívateľa pred sprístupnením každého profilu tretím stranám;

b) za predpokladu, že vyhradené prístupové profily sa nebudú dať identifikovať pomocou interných/externých vyhľadávačov.

91. Okrem stanovenia záväzných štandardných nastavení na ochranu súkromia ešte zostáva otázka, či môže byť ešte vhodná aj ďalšia špecifická ochrana údajov a iné opatrenia (napríklad týkajúce sa neplnoletých). Z tohto vyplýva širšia otázka, či by nebolo vhodné, aby sa vytvoril konkrétny rámec pre tieto typy služieb, ktoré by okrem poskytovania povinných nastavení ochrany súkromia regulovali ďalšie aspekty. Európsky dozorný úradník pre ochranu informácií žiada Komisiu, aby túto otázku mala na zreteli.

VII. ŠTANDARDNÉ NASTAVENIA PREHLIADAČA NA OCHRANU SÚKROMIA NA ZARUČENIE INFORMOVANÉHO SÚHLASU S DORUČOVANÍM REKLÁM

92. Poskytovatelia sietí používajú tzv. *cookies* a iné zariadenia na sledovanie správania jednotlivých užívateľov, keď surfujú po internete s cieľom získať prehľad o ich záujmoch a vybudovať profily. Tieto informácie sa potom využívajú na to, aby sa im mohli posielať cielené reklamy ([4]).

VII.1. Zostávajúce výzvy a riziká v rámci súčasného právneho rámca na ochranu údajov/súkromia

93. Na toto spracovanie údajov sa vzťahuje smernica o ochrane údajov (ak ide o osobné údaje) a aj článok 5 ods. 3 smernice o elektronickom súkromí. V tomto článku sa konkrétne vyžaduje, aby užívateľ bol informovaný a mal možnosť reagovať formou súhlasu alebo odmietnutia, pokiaľ ide o ukladanie prostriedkov, akými sú *cookies* a pod., na jeho počítač alebo iné zariadenie ([5]).

94. Prevádzkovatelia reklamných sietí sa doteraz opierajú o nastavenia prehliadačov a politiky ochrany súkromia, ktoré umožňujú informovať užívateľov a poskytujú im

([1]) Viviane Reding, členka Európskej komisie zodpovedná za informačnú spoločnosť a médiá, Premysli si, čo zverejníš! Ako dosiahnuť väčšiu bezpečnosť lokalít sociálnych sietí pre deti a tínedžerov? Deň bezpečnejšieho internetu, Štrasburg, 9. februára 2010.

([2]) Stanovisko Európskeho hospodárskeho a sociálneho výboru o vplyve na lokality sociálnych sietí na občanov/spotrebiteľov, 4 november 2009.

([3]) Vysvetlené tiež v bode 33 tohto dokumentu.

([4]) Stopovacie *cookies* sú malé textové súbory obsahujúce jedinečný identifikátor. Poskytovateľ reklamnej siete obvykle (ako aj prevádzkovatelia webových lokalít alebo vydavatelia) umiestňujú cookies na hard disk návštevníkov, najmä do prehliadača užívateľov internetu, keď užívatelia prvýkrát navštívia webové lokality prinášajúce reklamy, ktoré sú súčasťou ich siete. *Cookie* umožní poskytovateľovi reklamnej siete spoznať bývalého návštevníka, ktorý sa vráti na túto webovú lokalitu alebo navštívi ktorúkoľvek webovú stránku, ktoré je partnerom reklamnej siete. Takéto opakované návštevy umožnia poskytovateľovi reklamnej siete vytvoriť profil návštevníka.

([5]) Článok 5 ods. 3 smernice o elektronickom súkromí bol nedávno zmenený a doplnený na zvýšenie ochrany pred zachytením komunikácie užívateľov na základe používania, napríklad *spyware* a *cookies* ukladaných v počítači užívateľa alebo inom prístroji. Podľa novej smernice by sa užívateľom mali ponúknuť lepšie informácie a jednoduchšie spôsoby na kontrolu, či ukladať *cookies* vo svojom koncovom zariadení.

možnosť, aby súhlasili s *cookies* alebo ich odmietli. V politikách vydavateľov na ochranu súkromia vysvetľujú, ako zrušiť (*opt-out*) prijímanie *cookies* úplne alebo ako ich prijímať v jednotlivých prípadoch. Pri tomto mali v úmysle splniť svoju povinnosť a ponúknuť užívateľom právo odmietnuť *cookies*.

95. Kým teoreticky touto metódou (cez prehliadač) by sa skutočne mohol účinne poskytovať zmysluplný informovaný súhlas, realita je však veľmi odlišná. Vo všeobecnosti užívatelia nerozumejú dobre zberu akýchkoľvek údajov a ešte menej od tretích strán, hodnote týchto údajov, ich využívaniu, ani tomu, ako táto technológia funguje a najmä nevedia, ako a kde to môžu zrušiť. Kroky, ktoré užívatelia musia podniknúť na zrušenie sa zdajú nielen zložité, ale aj prehnané (najprv si musí nastaviť svoj prehliadač, aby akceptoval cookies a potom uskutočnil voľbu „opt-out").

96. Výsledkom je, že v praxi len veľmi málo ľudí si zvolí možnosť „opt-out", nie preto, že sa informovane rozhodli prijímať reklamy zasielané na základe ich správania (angl.: *behavioural advertisement*), ale skôr preto, že si neuvedomujú, že pokiaľ nezvolia možnosť „opt out" (deaktivovať), v skutočnosti zvolia možnosť prijímať.

97. Preto zatiaľ čo z právneho hľadiska článok 5 ods. 3 smernice o elektronickom súkromí ustanovuje účinnú právnu ochranu, v praxi sa usudzuje, že užívatelia internetu súhlasia so sledovaním na účely zasielania reklám na základe svojho správania, i keď v skutočnosti v mnohých prípadoch, ak nie vo väčšine, si vôbec neuvedomujú, že dochádza k takémuto sledovaniu.

98. Pracovná skupina zriadená podľa článku 29 pripravuje stanovisko, ktorého cieľom je vysvetliť právne požiadavky na zapojenie sa do reklám na základe svojho správania, čo je vítané. Výklad však sám o sebe nemusí byť dostatočný na vyriešenie tejto situácie a môže byť potrebné, aby Európska únia prijala ďalšie opatrenia.

VII.2. **Potreba ďalších opatrení, najmä poskytovanie povinných štandardných nastavení ochrany súkromia**

99. Ako je uvedené vyššie, webové prehliadače bežne umožňujú úroveň kontroly nad určitými druhmi tzv. *cookies*. V súčasnosti štandardné nastavenia väčšiny webových prehliadačov prijímajú všetky *cookies*. Inými slovami, štandardne sú prehliadače nastavené tak, aby prijmali všetky *cookies*, nezávisle od toho, na aké účely. Užívateľ nebude prijímať *cookies* iba vtedy, ak zmení nastavenie svojho prehliadača na odmietnutie *cookies*, čo, ako už bolo uvedené, len veľmi málo užívateľov urobí. Navyše, neexistuje sprievodca v oblasti súkromia v prípade prvej inštalácie alebo aktualizácie prehliadačových aplikácií.

100. Uvedený problém by sa dal zmierniť, keby sa prehliadače poskytovali so štandardným nastavením ochrany súkromia. Inými slovami, keby sa poskytovali s nastavením „neprijímať *cookies* tretích strán". Na doplnenie a zvýšenie účinnosti by prehliadače mali požadovať, aby užívatelia pri prvej inštalácii alebo aktualizácii prehliadača preštudovali sprievodcu v oblasti ochrany súkromia. Potrebné sú podrobnejšie a jasnejšie informácie o typoch *cookies* a užitočnosti niektorých z nich. Užívatelia, ktorí chcú byť sledovaní na účely prijímania reklamy, budú riadne informovaní a budú potrebovať zmeniť nastavenia prehliadača. To by im poskytlo lepšiu kontrolu nad svojimi osobnými údajmi a ochranou súkromia. Toto by bol podľa názoru európskeho dozorného úradníka pre ochranu údajov účinný spôsob, ako rešpektovať a zachovať súhlas užívateľa ([1]).

101. Na jednej strane vzhľadom na častý výskyt tohto problému, inými slovami, počet užívateľov internetu v súčasnosti sledovaných na základe iluzórneho súhlasu a na strane druhej vzhľadom na mieru záujmu je potreba dodatočných bezpečnostných opatrení čoraz naliehavejšia. Zavedenie zásady ochrany súkromia od štádia návrhu systému do webových prehliadačových aplikácií by mohlo dramaticky zmeniť poskytovanie kontroly jednotlivcom nad praktikami zberu údajov používaných na reklamné účely.

102. Z týchto dôvodov európsky dozorný úradník pre ochranu údajov žiada Komisiu, aby zvážila legislatívne opatrenia vyžadujúce povinné nastavenia ochrany súkromia v prehliadačoch a poskytovanie relevantných informácií.

VIII. **ĎALŠIE ZÁSADY ZAMERANÉ NA OCHRANU SÚKROMIA/ÚDAJOV JEDNOTLIVCOV**

103. Aj keď zásada ochrany súkromia od štádia návrhu systému má veľký potenciál pre zlepšenie ochrany osobných údajov a súkromia jednotlivcov, na zabezpečenie dôvery spotrebiteľov v IKT je potrebné navrhnúť a zahrnúť do práva dodatočné zásady. V tejto súvislosti sa európsky dozorný úradník pre ochranu údajov zameriava na zásadu zodpovednosti a dokončenie povinného rámca na ochranu pred narušením bezpečnosti platného v jednotlivých sektoroch.

VIII.1. **Zásada zodpovednosti na zabezpečenie dodržiavania zásady ochrany súkromia už od štádia návrhu systému**

104. V dokumente pracovnej skupiny zriadenej podľa článku 29 s názvom „Budúcnosť súkromia" ([2]) sa odporučilo zahrnúť zásadu zodpovednosti do smernice o ochrane

([1]) Zároveň si európsky dozorný úradník pre ochranu údajov uvedomuje, že týmto by sa problém úplne nevyriešil, pokým existujú cookies, ktoré nemožno kontrolovať cez prehliadač, ako napríklad prípad s tzv. flash cookies. Z tohto dôvodu by bolo potrebné, aby pracovníci vyvíjajúci prehliadače pri uvádzaní na trh nových prehliadačov štandardne zabudovali do svojich kontrol *cookies* tzv. flash kontroly.

([2]) Stanovisko 168 pracovnej skupiny zriadenej podľa článku 29 o budúcnosti súkromia, Spoločný príspevok ku konzultáciám Európskej komisie o právnom rámci pre základné právo na ochranu osobných údajov, prijaté 1. decembra 2009.

údajov. Táto zásada uznaná v niektorých medzinárodných nástrojoch ochrany údajov ([1]) vyžaduje, aby organizácie zaviedli procesy na dodržiavanie existujúcich právnych predpisov a aby stanovili metódy hodnotenia a preukazovania súladu s právnymi predpismi a inými záväznými nástrojmi.

105. Európsky dozorný úradník pre ochranu údajov plne podporuje odporúčania pracovnej skupiny zriadenej podľa článku 29. Podľa jeho názoru bude táto zásada veľmi dôležitá na podporu účinného uplatňovania zásad a povinností ochrany údajov. Zodpovednosť si bude vyžadovať, aby prevádzkovatelia údajov preukázali, že zaviedli mechanizmus potrebný na dodržiavanie platných právnych predpisov na ochranu údajov. Je pravdepodobné, že prispejú k účinnému zavádzaniu ochrany súkromia od štádia návrhu systému do technológií IKT ako obzvlášť vhodného prvku na preukázanie zodpovednosti.

106. Na meranie a preukázanie zodpovednosti by prevádzkovatelia údajov mohli využívať interné postupy a tretie strany, ktoré môžu vykonávať audity alebo iné typy kontrol a overovaní, ktoré môžu na základe nich udeliť potvrdenia alebo pokuty. V tejto súvislosti európsky dozorný úradník pre ochranu údajov vyzýva Komisiu, aby zvážila, či okrem zásady všeobecnej zodpovednosti môže byť užitočné vyžadovať podľa zákona osobitné opatrenia súvisiace so zodpovednosťou, ako napríklad potrebu vyhotovovať hodnotenia vplyvu na ochranu súkromia a údajov a za akých okolností.

VIII.2. **Narušenie bezpečnosti: dokončenie právneho rámca**

107. Minuloročnými zmenami a doplneniami smernice o elektronickom súkromí sa zaviedla povinnosť oznamovať porušenia ochrany údajov postihnutým osobám a tiež aj príslušným orgánom. Porušenie ochrany údajov je všeobecne vymedzené ako akékoľvek porušenie, ktoré vedie k zničeniu, strate, zverejneniu osobných údajov prenášaných, uchovávaných alebo iným spôsobom spracovávaným v spojení so službou. Oznámenie jednotlivcom sa bude vyžadovať v prípade, ak by porušenie ochrany údajov mohlo mať nepriaznivý vplyv na ich osobné údaje alebo súkromie. Môže k tomu dôjsť vtedy, keby porušenie mohlo viesť ku krádeži identity alebo závažnému zneváženiu alebo poškodeniu povesti. Oznámenia príslušným orgánom sa budú vyžadovať v prípade každého porušenia ochrany údajov bez ohľadu na ohrozenie jednotlivca.

Uplatňovanie povinností v oblasti narušenia bezpečnosti v jednotlivých sektoroch

108. Žiaľ, táto povinnosť sa vzťahuje len na poskytovateľov verejne dostupných elektronických komunikačných služieb, ako napr. telefónnych spoločností, poskytovateľov prístupu k internetu, poskytovateľov služby webmail a pod. Európsky dozorný úradník pre ochranu údajov naliehavo vyzýva Komisiu, aby predložila návrhy v súvislosti s narušením bezpečnosti, ktoré budú platiť v jednotlivých sektoroch. Čo sa týka obsahu tohto rámca, európsky dozorný úradník pre ochranu údajov zastáva názor, že právnym rámcom týkajúcim sa narušenia bezpečnosti prijatým v smernici o elektronickom súkromí sa našla zlatá stredná cesta medzi ochranou práv jednotlivcov vrátane ich práv na ochranu osobných údajov a súkromia a povinnosťami uloženými subjektom, na ktoré sa vzťahuje. Zároveň ide o rámec so skutočnými „zubami“, pretože sa opiera o zmysluplné ustanovenia na presadzovanie, ktoré orgánom poskytujú dostatočné právomoci na vyšetrovanie a sankcie v prípade ich nedodržiavania.

109. Európsky dozorný úradník pre ochranu údajov preto žiada Komisiu, aby prijala legislatívny návrh na uplatnenie tohto rámca v jednotlivých sektoroch, v prípade potreby s príslušnými úpravami. Navyše by sa tým zabezpečilo uplatňovanie rovnakých noriem a postupov v jednotlivých sektoroch.

Dokončenie právneho rámca zakotveného v smernici o elektronickom súkromí prostredníctvom komitologického postupu

110. Revidovaná smernica o súkromí splnomocňuje Komisiu, aby prijala technické vykonávacie opatrenia, t. j. podrobné opatrenia týkajúce sa oznamovania narušenia bezpečnosti prostredníctvom komitologického postupu ([2]). Toto splnomocnenie je odôvodnené, aby sa zabezpečilo dôsledné vykonávanie a uplatňovanie právneho rámca týkajúceho sa porušenia ochrany bezpečnosti. Dôsledná realizácia prác na zabezpečenie, aby jednotlivci v rámci Spoločenstva mali rovnako vysokú úroveň ochrany a aby zahrnuté subjekty neboli zaťažené rozdielnymi požiadavkami na oznámenie.

111. Smernica o elektronickom súkromí bola prijatá v novembri 2009. Podľa všetkého nie je žiadny dôvod oprávňujúci odloženie začatia prác smerujúcich k prijatiu technických vykonávacích opatrení. Európsky dozorný úradník pre ochranu údajov usporiadal dva semináre zamerané na výmenu a zhromažďovanie skúseností o porušovaní ochrany údajov. Rád by sa podelil o výsledky z tejto činnosti a teší sa na spoluprácu s Komisiou a ostatnými zainteresovanými stranami pri dolaďovaní právneho rámca týkajúceho porušovania ochrany bezpečnosti.

112. Európsky dozorný úradník pre ochranu údajov naliehavo vyzýva Komisiu, aby v krátkom čase prijala potrebné opatrenia. Pred prijatím technických vykonávacích opatrení sa Komisia musí zapojiť do rozsiahlych konzultácií, v rámci ktorých je potrebné konzultovať s agentúrou ENISA, európskym dozorným úradníkom pre ochranu údajov a pracovnou skupinou zriadenou podľa článku 29. Okrem toho sa do konzultácií musia zapojiť aj iné „príslušné zainteresované strany“, a to najmä s cieľom informovať o najlepších dostupných technických a ekonomických prostriedkov na realizáciu.

([1]) 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data; Madrid Privacy Declaration on Global Privacy Standards for a Global World *(Pokyny OECD z roku 1980 o ochrane súkromia a cezhraničných tokov osobných údajov; Madridská deklarácia o súkromí – Globálne normy súkromia pre globálny svet)*, z 3. novembra 2009.

([2]) Komitológia zahŕňa prijatie technických vykonávacích opatrení prostredníctvom výboru zástupcov členských štátov, ktorému predsedá Komisia. V prípade smernice o elektronickom súkromí sa uplatňuje tzv. regulačný postup s kontrolou, čo znamená, že Európsky parlament a tiež aj Rada môžu namietať proti opatreniam, ktoré navrhla Komisia. Viac informácií nájdete na: http://europa.eu/scadplus/glossary/comitology_en.htm

IX. **ZÁVERY**

113. Zistilo sa, že dôvera a či skôr jej nedostatok je hlavným problémom pri vývoji a úspešnom zavádzaní informačných a komunikačných technológií. Ak ľudia nebudú dôverovať IKT , je pravdepodobné, že tieto technológie zlyhajú. Dôvera v IKT závisí od rôznych faktorov a jedným z kľúčových faktorov je zabezpečenie toho, aby tieto technológie neporušovali základné práva jednotlivcov na súkromie a ochranu osobných údajov.

114. Na ďalšie posilnenie právneho rámca v oblasti ochrany údajov/súkromia, ktorého zásady sa celkovo naďalej uplatňujú v informačnej spoločnosti, európsky dozorný úradník pre ochranu informácií navrhuje Komisii, aby ochranu súkromia už od štádia návrhu systému začlenila do rôznych úrovní tvorby práva a politiky.

115. Odporúča Komisii, aby sledovala štyri smery činnosti, a síce aby:

a) navrhla zahrnúť všeobecné ustanovenie o ochrane súkromia už od štádia návrhu systému do právneho rámca v oblasti ochrany údajov. Toto ustanovenie by malo byť neutrálne z hľadiska technológie a dodržiavanie uvedenej zásady by malo byť v jednotlivých štádiách povinné;

b) ďalej rozpracovať toto všeobecné ustanovenie v osobitných ustanoveniach po navrhnutí konkrétnych právnych nástrojov v jednotlivých sektoroch. Tieto osobitné ustanovenia by sa mohli už teraz zahrnúť do právnych nástrojov; na základe článku 17 smernice o ochrane údajov (a iných existujúcich právnych predpisov);

c) zahrnula ochranu súkromia už od štádia návrhu systému ako prvoradú zásadu do digitálneho programu Európy;

d) zaviedla ochranu súkromia už od štádia návrhu systému ako zásadu do ďalších iniciatív EÚ (hlavne nelegislatívnych).

116. V troch určených oblastiach IKT európsky dozorný úradník pre ochranu údajov odporúča Komisii, aby posúdila potrebu predložiť návrhy na zavedenie zásady ochrany súkromia už od štádia návrhu systému konkrétnymi spôsobmi:

a) aby v súvislosti s RFID navrhla legislatívne opatrenia upravujúce hlavné problémy používania RFID v prípade, ak zlyhá účinné uplatňovanie existujúceho právneho rámca na základe samoregulácie. A najmä, aby ustanovila zásadu predchádzajúceho súhlasu (opt-in) v mieste predaja, podľa ktorej by sa všetky štítky RFID pripojené k spotrebnému tovaru štandardne deaktivovali v mieste predaja;

b) aby v súvislosti so sociálnymi sieťami pripravila právne predpisy, ktoré by obsahovali prinajmenšom všeobecnú povinnosť vyžadujúcu povinné nastavenia ochrany súkromia spolu s presnejšími požiadavkami v oblasti obmedzenia prístupu k profilom užívateľov pre kontakty vybrané samotným užívateľom a za predpokladu, že vyhradené prístupové profily sa nebudú dať identifikovať pomocou interných/externých vyhľadávačov;

c) aby v súvislosti s cielenou reklamou zvážila právne predpisy predpisujúce, aby nastavenia prehliadačov štandardne neprijímali tzv. cookies tretích strán a vyžadujúce, aby si užívatelia pri prvej inštalácii alebo aktualizácii prehliadača preštudovali sprievodcu v oblasti ochrany súkromia.

117. Napokon európsky dozorný úradník pre ochranu údajov navrhuje Komisii, aby:

a) zvážila zavedenie zásady zodpovednosti do existujúcej smernice na ochranu údajov a

b) vypracovala rámec pravidiel a postupov na vykonávanie ustanovení o oznamovaní narušenia bezpečnosti smernice o elektronickom súkromí a rozšírila ich, aby sa uplatňovali všeobecne na všetkých prevádzkovateľov údajov.

V Bruseli 18. marca 2010

Peter HUSTINX

Európsky dozorný úradník pre ochranu údajov