I

(Usnesení, doporučení a stanoviska)

STANOVISKA

EVROPSKÝ INSPEKTOR OCHRANY ÚDAJŮ

Stanovisko evropského inspektora ochrany údajů k podpoře důvěry v informační společnost prostřednictvím posílení ochrany údajů a soukromí

(2010/C 280/01)

EVROPSKÝ INSPEKTOR OCHRANY ÚDAJŮ,

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

s ohledem na Listinu základních práv Evropské unie, a zejména na články 7 a 8 této listiny,

s ohledem na směrnici Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů ([1]),

s ohledem na směrnici Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací ([2]),

s ohledem na nařízení Evropského parlamentu a Rady (ES) č. 45/2001 ze dne 18. prosince 2000 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů, a zejména na článek 41 tohoto nařízení ([3]),

PŘIJAL TOTO STANOVISKO:

I. ÚVOD

1. Informační a komunikační technologie (IKT) nabízejí obrovské možnosti prakticky ve všech ohledech našich životů – ovlivňují to, jak pracujeme, bavíme se, navazujeme vztahy a jak se vzděláváme. Jsou zásadní pro dnešní informační ekonomiku a obecně pro společnost.

2. Evropská unie je globální silou v pokročilých IKT a je rozhodnuta být jí i nadále. V rámci splnění tohoto úkolu se očekává, že Evropská komise brzy přijme evropskou digitální agendu, o které komisařka Kroesová potvrdila, že je její prioritou ([4]).

3. Evropský inspektor ochrany údajů uznává přínosy IKT a souhlasí, že by Evropská unie měla dělat co nejvíce pro posílení jejich rozvoje a rozsáhlého zavádění. Rovněž plně podporuje názor komisařek Kroesové a Redingové, že v jádru tohoto nového prostředí by měly být fyzické osoby ([5]). Fyzické osoby by měly mít možnost se spolehnout na schopnost IKT zaručit bezpečnost a kontrolu nad užíváním jejich informací a dále na skutečnost, že i v digitálním prostoru budou respektována jejich práva na ochranu soukromí a údajů. Respektování těchto práv je zásadní pro vytvoření důvěry spotřebitelů. A tato důvěra je rozhodující, mají-li občané využívat nové služby ([6]).

([1]) Úř. věst. L 281, 23.11.1995, s. 31.
([2]) Úř. věst. L 201, 31.7.2002, s. 37.
([3]) Úř. věst. L 8, 12.1.2001, s. 1.

([4]) Odpovědi na dotazník Evropského parlamentu pro komisařku Neelie Kroesovou v souvislosti se slyšením Evropského parlamentu, které předcházelo jmenování komisařky.
([5]) Odpovědi na dotazník Evropského parlamentu pro komisařku Neelie Kroesovou v souvislosti se slyšením Evropského parlamentu, které předcházelo jmenování komisařky; projev komisařky Viviane Redingové Evropská digitální agenda pro nového digitálního spotřebitele přednesený na Fóru BEUC několika zainteresovaných stran na téma Soukromí spotřebitelů a on-line marketing: tržní trendy a perspektivy politik), v Bruselu dne 12. listopadu 2009.
([6]) Viz například zpráva Důvěra v informační společnost), zpráva poradního výboru, RISEPTIS (Výzkum a inovace v oblasti bezpečnosti, soukromí a důvěryhodnosti v informační společnosti). Dostupné na adrese http://www.think-trust.eu/general/news-events/riseptis-report.html Viz také: *J. B. Horrigan, Broadband Adoption and Use in America, FCC Omnibus Broadband Initiative, OBI Working Paper Series No 1* (J. B. Horrrigan, Přijetí a využití širokého pásma v Americe, Iniciativa pro souhrnné široké pásmo FCC, Pracovní dokument ISŠP, řada č. 1).

4. EU má silný právní rámec v oblasti ochrany údajů a soukromí, jehož zásady zůstávají v digitálním věku platné v plném rozsahu. To však nelze považovat za dostačující. V mnoha případech IKT vzbuzují nové obavy, které nejsou ve stávajícím právním rámci zohledněny. Proto je potřeba podniknout určité kroky, aby se zajistilo, že práva fyzických osob zakotvená v právu EU budou i nadále poskytovat účinnou ochranu v tomto novém prostředí.

5. Toto stanovisko pojednává o opatřeních, která by Evropská unie mohla buď podpořit, nebo přijmout, aby zaručila ochranu soukromí a údajů fyzických osob v globalizovaném světě, ve kterém technologie bude i nadále hnací silou. Pojednává o legislativních i nelegislativních nástrojích.

6. Po představení IKT jako pokroku, který vytváří příležitosti, ale také přináší rizika, se toto stanovisko zabývá potřebou zohlednit ochranu údajů a soukromí v praxi, a to od samého počátku nových informačních a komunikačních technologií (což je označováno jako zásada „soukromí coby aspekt návrhu“). Dále toto stanovisko pojednává o potřebě zohlednění této zásady v právním rámci pro ochranu osobních údajů alespoň dvěma různými způsoby. Za prvé jejím začleněním jako obecné, závazné zásady a za druhé jejím začleněním do konkrétních oblastí IKT představujících specifická rizika pro ochranu údajů a soukromí, která mohou být zmírněna pomocí přiměřené technické architektury a návrhu. Těmito oblastmi jsou identifikace na základě rádiové frekvence (RFID), aplikace sociálních sítí a aplikace prohlížečů. Závěrem stanovisko předkládá návrhy týkající se dalších nástrojů a zásad zaměřených na ochranu soukromí a údajů fyzických osob v oblasti IKT.

7. Při řešení výše uvedených otázek se stanovisko podrobněji zabývá některými body zmíněnými pracovní skupinou zřízenou podle článku 29 v jejím příspěvku k veřejné konzultaci o budoucnosti soukromí ([1]). Dále navazuje na dřívější stanoviska evropského inspektora ochrany údajů, jako je stanovisko ze dne 25. července 2007 k provádění směrnice o ochraně údajů, stanovisko ze dne 20. prosince 2007 k RFID a jeho dvě stanoviska ke směrnici o ochraně soukromí v odvětví elektronických komunikací ([2]).

II. IKT NABÍZEJÍ NOVÉ PŘÍLEŽITOSTI, ALE PŘEDSTAVUJÍ TAKÉ NOVÁ RIZIKA

8. IKT jsou srovnávány s jinými důležitými objevy minulosti, jako je elektřina. I když je možná příliš brzy na hodnocení jejich skutečného historického dopadu, vazba mezi IKT a hospodářským růstem v rozvinutých zemích je jasná. IKT přinesly zaměstnanost, hospodářské přínosy a přispěly k celkovému blahobytu. Dopad IKT je širší než čistě ekonomický, protože hraje důležitou úlohu při posilování inovace a tvořivosti.

9. IKT dále změnily způsob, jak lidé pracují, navazují vztahy a vzájemně reagují. Lidé se například stále více opírají o IKT při sociálních a hospodářských interakcích. Fyzické osoby mohou využívat široký rozsah nových aplikací IKT, jako jsou elektronické aplikace ve zdravotnictví, dopravě a státní správě (eHealth, eTransport, eGoverment), jakož i inovační interaktivní systémy pro zábavu a učení.

10. S ohledem na tyto přínosy všechny evropské instituce vyjádřily svůj závazek podporovat IKT jako nezbytný nástroj ke zlepšení konkurenceschopnosti evropského průmyslu a zrychlení hospodářského zotavení v Evropě. V srpnu 2009 Komise přijala zprávu o digitální konkurenceschopnosti Evropy ([3]) a zahájila veřejnou konzultaci o vhodných budoucích strategiích pro posílení IKT. Dne 7. prosince 2009 Rada předložila svůj příspěvek k této konzultaci nazvaný „Strategie navazující na i2010 – na cestě k otevřené, zelené a konkurenceschopné znalostní společnosti“ ([4]). Evropský

([1]) Stanovisko 168 pracovní skupiny zřízené podle článku 29 k budoucnosti soukromí, společný příspěvek ke konzultaci Evropské komise k právnímu rámci pro základní právo na ochranu osobních údajů přijaté dne 1. prosince 2009.

([2]) Stanovisko ze dne 25. července 2007 ke sdělení Komise Evropskému parlamentu a Radě o pokračování pracovního programu pro lepší provádění směrnice o ochraně osobních údajů, Úř. věst. C 255, 27.10.2007, s. 1; Stanovisko ze dne 20. prosince 2007 ke sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů o identifikaci na základě rádiové frekvence (RFID) v Evropě: kroky k rámci politiky (KOM(2007) 96), Úř. věst. C 101, 23.4.2008, s. 1; Stanovisko ze dne 10. dubna 2008 k návrhu směrnice, kterou se mění mimo jiné směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (směrnice o soukromí a elektronických komunikacích), Úř. věst. C 181, 18.7.2008, s. 1; Druhé stanovisko ze dne 9. ledna 2009 k přezkoumání směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací.

([3]) Zpráva o digitální konkurenceschopnosti Evropy – Hlavní úspěchy strategie i2010 v období 2005–2009 (SEK(2009) 1060).

([4]) Závěry Rady „Strategie navazující na i2010 – na cestě k otevřené, zelené a konkurenceschopné znalostní společnosti.“ (17107/09), přijato dne 18.12.2009.

parlament právě přijal zprávu, která má Komisi poskytnout vodítko při vymezení digitální agendy ([1]).

11. Příležitosti a přínosy, které doprovázejí rozvoj IKT, jsou spojeny s novými riziky, zejména pro soukromí a ochranu osobních údajů fyzických osob. IKT často vedou k nárůstu množství informací, které jsou shromažďovány, tříděny, filtrovány, přenášeny nebo jinak uchovávány (a to způsoby, které jsou velmi často mimo dohled fyzických osob), a rizika pro takové údaje se proto násobí.

12. Například na (některých) spotřebních výrobcích jsou čárové kódy nahrazovány čipy RFID. Díky zlepšení informačního toku v dodavatelském řetězci (a v důsledku toho omezení potřeby disponovat „bezpečnostními" zásobami, poskytováním přesnějších výhledů atd.) má nový systém znamenat přínosy pro podnik i spotřebitele. Současně to však vede ke znepokojující možnosti sledovatelnosti prostřednictvím označeného osobního majetku, a to pro různé účely a ze strany různých subjektů.

13. Dalším příkladem je „cloud computing", v zásadě poskytování internetových služeb spotřebitelských a jiných než spotřebitelských úložných aplikací. Jejich rozsah se pohybuje od fotografických alb, kalendářů, internetových poštovních databází a databází spotřebitelů po složitější služby související s podnikáním. Přínosy pro podniky i fyzické osoby jsou jasné; snížení nákladů (náklady skokově rostou), omezení vazby na místo (snadný přístup k informacím kdekoli na světě), automatizace (není potřeba mít zvláštní zdroje pro informační technologie a údržbu aktuálního softwaru) atd. Současně však existují rizika poruch zabezpečení a hackerství, která jsou velmi reálná. Existuje také obava, že může dojít ke ztrátě přístupu k vlastním údajům a kontrole nad nimi.

14. Souběžná existence přínosů a rizik byla prokázána v dalších oblastech, kde dochází k využívání aplikací IKT. Vezměme si elektronickou aplikaci pro zdravotnictví (eHealth), která může zvýšit účinnost, snížit náklady, zvýšit přístupnost a obecně zlepšit kvalitu služeb zdravotní péče. Aplikace eHealth však často vede k otázce oprávněnosti sekundárního využití informací, které jsou v ní obsaženy, což vyžaduje pečlivou analýzu účelů potenciálního sekundárního využití ([2]). Navíc s rozsáhlejším využíváním elektronických zdravotních záznamů došlo ke skandálům u samotných systémů, které odhalily mnoho případů hackerství v oblasti elektronických zdravotních záznamů.

15. Celkem vzato je pravděpodobné, že bude přetrvávat určitý stupeň zbytkového rizika i po provedení správného vyhodnocení a přijetí nezbytných opatření. Situace nulového rizika by byla nerealistická. Jak je však uvedeno dále, lze a musí být provedena opatření ke snížení takového rizika na přiměřenou úroveň.

III. SOUKROMÍ COBY ASPEKT NÁVRHU JAKO KLÍČOVÝ NÁSTROJ PRO VYTVOŘENÍ DŮVĚRY FYZICKÝCH OSOB V IKT

16. Potenciální přínosy IKT lze v praxi využívat pouze, pokud jsou schopny vytvořit důvěru, jinými slovy, jestliže mohou zajistit ochotu uživatele být závislým na IKT kvůli jejich charakteristikám a přínosu. Taková důvěra se vytvoří pouze, pokud jsou IKT spolehlivé, bezpečné, pod kontrolou fyzických osob a pokud je zaručena ochrana jejich osobních údajů a soukromí.

17. Rozsáhlá rizika a selhání jako ta, která byla popsána výše, zejména pokud vedou ke zneužití nebo prolomení osobních údajů a odhalení soukromí fyzických osob, pravděpodobně naruší důvěru uživatele v informační společnost. To by mohlo vážně ohrozit rozvoj IKT a přínosy, které by mohly znamenat.

18. Řešením těchto rizik pro ochranu soukromí a údajů však nemůže být zrušení, vyloučení nebo odmítnutí využívání nebo podpory IKT. To by nebylo ani proveditelné, ani realistické; zabránilo by to fyzickým osobám využívat přínosy IKT a vážně by to omezilo celkové výhody, které lze získat.

19. Evropský inspektor ochrany údajů má za to, že pozitivnějším řešením je navrhovat a rozvíjet IKT způsobem, který bere ohled na ochranu soukromí a údajů. Proto je rozhodující, aby ochrana soukromí a údajů byla zapracována do celého cyklu životnosti technologie od velmi brzké etapy návrhu až do jejího zavedení a konečného odstranění. To se obvykle nazývá „soukromí coby aspekt návrhu" a o tomto konceptu je dále pojednáno níže.

20. Soukromí coby aspekt návrhu může zahrnovat různé kroky v závislosti na konkrétním případu nebo aplikaci. V některých případech může například vyžadovat odstranění či omezení osobních údajů nebo zabránění zbytečnému a/nebo nežádoucímu zpracování. V jiných případech může soukromí coby aspekt návrhu zahrnovat nabídku nástrojů pro posílení kontroly fyzické osoby nad jejími osobními údaji. Taková opatření by měla být zvažována při definování norem anebo osvědčených

([1]) Zpráva o vymezení nové digitální agendy pro Evropu: od i2010 po digital.eu (2009/2225 (INI)), přijatá dne 18.3.2010.

([2]) Například prodej nebo využití zdravotních informací shromážděných za účelem poskytování léčby nesmí být prováděno pro volbu míst satelitních klinik, pro zřizování středisek ambulantních ordinací ani jinak za účelem plánování budoucích činností s finančními dopady, což by vyžadovalo pečlivé zkoumání.

postupů. Tato opatření také mohou být zapracována do architektury informačních a komunikačních systémů nebo do organizačních struktur subjektů, které zpracovávají osobní údaje.

III.1 **Zásada soukromí coby aspekt návrhu použitelná v různých prostředích IKT a jejich dopad**

21. Potřebu zásady soukromí coby aspekt návrhu lze nalézt v mnoha různých prostředích IKT. Odvětví zdravotnictví se například stále více opírá o infrastrukturu IKT, což často znamená centralizované uložení zdravotních informací pacientů. Uplatnění zásady soukromí coby aspekt návrhu v odvětví zdravotnictví by vyžadovalo hodnocení vhodnosti různých opatření, jako je možnost minimalizace centrálně ukládaných údajů nebo jejich omezení na seznam, používání šifrovacích nástrojů, omezené přidělování přístupových práv na „základě potřeby vědět", anonymizace údajů, jakmile se již nepotřebují atd.

22. Podobně i dopravní systémy jsou stále více standardně dodávány s pokročilými aplikacemi IKT, které pro různé účely a funkce interagují s vozem a jeho prostředím. Například automobily jsou stále více vybavovány novými funkcemi IKT (GPS, GSM, síť čidel atd.), které v reálném čase informují nejen o jejich místě, ale i o jejich technických podmínkách. Tyto informace by se mohly použít například pro náhradu stávajícího systému silniční daně silničním poplatkem závislým na míře využívání. Uplatnění zásady soukromí coby aspekt návrhu v návrhu architektury takových systémů by mělo podpořit zpracovávání a další předávání co možná nejmenšího množství osobních údajů ([1]). V souladu s touto zásadou by před centralizovanými architekturami byly upřednostněny decentralizované nebo semidecentralizované architektury, které by omezovaly poskytování údajů o místě do centrálního bodu.

23. Výše uvedené příklady ukazují, že když jsou informační a komunikační technologie vytvářeny podle zásady soukromí coby aspekt návrhu, mohou být významně minimalizována rizika pro ochranu soukromí a údajů.

III.2 **Nedostačující zavádění IKT uplatňujících zásadu soukromí coby aspekt návrhu**

24. Důležitou otázkou je, zda hospodářské subjekty, výrobci/poskytovatelé IKT a správci údajů mají zájem podporovat a uplatňovat zásadu soukromí coby aspekt návrhu u IKT. V této souvislosti je také důležité zhodnotit poptávku uživatelů.

25. V roce 2007 Komise vydala sdělení, kterým vyzývá podniky, aby využily svoji inovační kapacitu pro tvorbu a provádění technologií zvyšujících ochranu soukromí (PET) jako způsobu zlepšení ochrany soukromí a osobních údajů od samého počátku vývojového cyklu ([2]).

26. Dostupné důkazy však ukazují, že ani výrobci IKT, ani správci údajů (v soukromém i veřejném sektoru) dosud nebyli schopni důsledně uplatňovat nebo obchodně prosazovat soukromí coby aspekt návrhu. Byly uváděny různé důvody, včetně chybějících ekonomických stimulů nebo institucionální podpory, nedostatečné poptávky atd ([3]).

27. Současně poptávka ze strany uživatelů po soukromí coby aspektu návrhu byla poměrně nízká. Uživatelé produktů a služeb IKT možná oprávněně předpokládají, že jejich soukromí a osobní údaje jsou *de facto* chráněny, zatímco v mnoha případech nejsou. V některých případech prostě nemohou učinit bezpečnostní opatření nutná pro ochranu buď svých vlastních osobních údajů, nebo osobních údajů jiných osob. V mnoha případech je to proto, že nemají úplné nebo dokonce ani částečné znalosti o těchto rizicích. Například obecně platí, že mládež přehlíží rizika pro soukromí spojená se zobrazováním osobních informací na sociálních sítích a často ignoruje nastavení pro ochranu soukromí. Další uživatelé mají povědomí o rizicích, ale možná nemají nezbytnou technickou odbornost pro zavádění bezpečnostních technologií pro ochranu jejich připojení na internet nebo změnu nastavení prohlížeče pro minimalizaci tvorby profilů na základě sledování jejich činnosti na internetu.

28. Rizika pro ochranu soukromí a údajů jsou velmi reálná. Pokud není ochrana soukromí a údajů zohledněna od samého počátku, je často příliš pozdě a příliš ekonomicky

([1]) Viz Stanovisko evropského inspektora ochrany údajů ze dne 22. července 2009 ke sdělení Komise o akčním plánu zavádění inteligentních dopravních systémů v Evropě a k souvisejícímu návrhu směrnice Evropského parlamentu a Rady, kterou se stanoví rámec pro zavedení inteligentních dopravních systémů v silniční dopravě a jejich styčné body s jinými druhy dopravy, dostupné na adrese: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2009/09-07-22_Intelligent_Transport_Systems_CS.pdf

([2]) Sdělení Komise Evropskému parlamentu a Radě ze dne 2.5.2007, KOM(2007) 228 v konečném znění, o podpoře ochrany osobních údajů prostřednictvím technologií zvyšujících ochranu soukromí (PET).

([3]) Studie o ekonomických přínosech technologií zvyšujících ochranu soukromí (PETS) jls/2008/D4/036.

obtížné zavedené systémy korigovat rovněž jako je příliš pozdě na nápravu již vzniklé škody. Narůstající počet případů narušení údajů v nedávné minulosti tento problém dokonale odhaluje a prohlubuje potřebu soukromí coby aspektu návrhu.

29. Výše uvedené jasně naznačuje, že výrobci a poskytovatelé IKT určených ke zpracování osobních údajů by měli mít spolu se správci údajů odpovědnost za jejich návrh se zabudovanou ochranou údajů a ochranou soukromí. V mnoha případech by to znamenalo, že by měly být navrženy s ochranou soukromí jako standardním nastavením.

30. V této souvislosti musíme zvážit, jaké kroky by měli učinit tvůrci politik pro podporu zásady soukromí coby aspekt návrhu při rozvoji IKT. První otázkou je, zda stávající právní rámec ochrany údajů obsahuje odpovídající ustanovení pro zajištění provádění zásady soukromí coby aspekt návrhu ze strany správců údajů i výrobců či vývojářů. Druhou otázkou je, co by se mělo udělat s ohledem na evropskou digitální agendu pro zajištění, aby odvětví IKT vzbuzovalo důvěru spotřebitelů.

IV. ZAPRACOVÁNÍ ZÁSADY SOUKROMÍ COBY ASPEKT NÁVRHU DO PRÁVA A POLITIK EU

IV.1 Současný právní rámec ochrany údajů a soukromí

31. EU má silný právní rámec v oblasti ochrany údajů a soukromí obsažený ve směrnici 95/46/ES ([1]), směrnici 2002/58/ES ([2]) a judikatuře Evropského soudu pro lidská práva ([3]) a Soudního dvora.

32. Směrnice o ochraně údajů se vztahuje na „jakýkoli úkon nebo soubor úkonů s osobními údaji“ (shromažďování, uchovávání, sdělení atd.). Ukládá nutnost vyhovění určitým zásadám a povinnostem ze strany těch, kteří zpracovávají osobní údaje („správci údajů“). Stanoví práva fyzických osob, jako je právo na přístup k osobním údajům. Směrnice o soukromí a elektronických komunikacích se konkrétně zabývá ochranou soukromí v odvětví elektronických komunikací ([4]).

33. Stávající směrnice o ochraně údajů neobsahuje výslovný požadavek na soukromí coby aspekt návrhu. Obsahuje však ustanovení, která mohou v různých situacích nepřímo vyžadovat provedení zásady soukromí coby aspekt návrhu. Zvláště článek 17 vyžaduje, aby správci údajů přijali vhodná technická a organizační opatření, aby zabránili nedovolenému zpracování údajů ([5]). Zásada soukromí coby aspekt návrhu je proto zahrnuta velmi obecným způsobem. Ustanovení směrnice se navíc obrací hlavně na správce údajů a jejich zpracování osobních informací. Výslovně nevyžadují, aby informační a komunikační technologie vyhovovaly ochraně soukromí a údajů, což vyžaduje oslovení návrhářů a výrobců IKT i zahrnutí činností vykonávaných v etapě normalizace.

34. Směrnice o soukromí a elektronických komunikacích je jednoznačnější. Čl. 14 odst. 3 uvádí, že „V případě potřeby lze přijmout opatření, aby bylo zajištěno, že koncové zařízení je sestrojeno tak, že odpovídá právu uživatelů na ochranu a kontrolu využití jejich osobních údajů v souladu se směrnicí 1999/5/ES a rozhodnutím Rady 87/95/EHS ze dne 22. prosince 1986 o normalizaci v oblasti informačních technologií a telekomunikací“. Toto ustanovení však nikdy nebylo použito ([6]).

35. Zatímco výše uvedená ustanovení těchto dvou směrnic napomáhají podpoře zásady soukromí coby aspektu návrhu, v praxi tato zásada nebyla dostačující pro zajištění zohlednění ochrany soukromí v odvětví IKT.

36. V důsledku této situace platné právní předpisy dostatečně přesným způsobem nevyžadují, aby IKT byly navrhovány v souladu se zásadou soukromí coby aspekt návrhu.

([1]) Směrnice Evropského parlamentu a Rady 95/46/ES (dále: směrnice o ochraně údajů).

([2]) Směrnice Evropského parlamentu a Rady 2002/58/ES (dále: směrnice o soukromí a elektronických komunikacích).

([3]) Interpretace hlavních prvků a podmínek stanovených v článku 8 Úmluvy o ochraně lidských práv a základních svobod (EÚLP) přijaté v Římě dne 4. listopadu 1950, které se uplatňují u různých.

([4]) Lisabonská smlouva takovou ochranu posílila tím, že v článku 7 a 8 Listiny základních práv Evropské unie uznala úctu k soukromému životu a ochranu osobních údajů jako samostatná základní práva. Listina základních práv Evropské unie se stala závaznou, když vstoupila v platnost Lisabonská smlouva.

([5]) Článek 17 má toto znění: „Členské státy stanoví, že správce musí přijmout vhodná technická a organizační opatření na ochranu osobních údajů proti náhodnému nebo nedovolenému zničení, náhodné ztrátě, úpravám, neoprávněnému sdělování nebo přístupu, zejména pokud zpracování zahrnuje předávání údajů v síti, jakož i proti jakékoli jiné podobě nedovoleného zpracování.“ Bod odůvodnění 46 to doplňuje tím, že uvádí „Vzhledem k tomu, že ochrana práv a svobod subjektů údajů v souvislosti se zpracováním osobních údajů vyžaduje, aby byla přijata příslušná technická a organizační opatření jak při přípravě systému zpracování, tak v průběhu vlastního zpracování, s cílem zajistit především bezpečnost a tím také zabránit jakémukoli neoprávněnému zpracování“.

([6]) Komise ohlásila plány aktualizovat směrnici 1999/5/ES koncem roku 2010.

Úřady na ochranu údajů také nemají dostatek pravomocí pro zajištění zapracování této zásady, což vede k její neúčinnosti. Například úřady na ochranu údajů mohou uložit sankce, když nedojde k odpovědi na žádost o přístup ze strany fyzických osob, a budou mít kompetence na to, aby vyžadovaly provedení určitých opatření pro zabránění nedovoleného zpracování údajů. Přesto není vždy dostatečně jasné, zda se jejich pravomoci vztahují na to, aby požadovaly, že systém má být navržen tak, aby usnadňoval uplatňování prá fyzických osob na ochranu údajů ([1]). Například na základě stávajících právních ustanovení není jasné, zda by mohlo být požadováno, aby architektura informačního systému byla navržena tak, aby usnadňovala reakci společností na žádosti o přístup ze strany fyzických osob způsobem, který by znamenal automatické a rychlejší zpracování těchto žádostí. Navíc pozdější pokusy o změnu technologie poté, co byla vytvořena nebo zavedena, mohou vést k nedokonalým řešením, která kromě ekonomické nevýhodnosti nemusí být plně funkční.

37. Podle názoru evropského inspektora ochrany údajů, který sdílí s pracovní skupinou zřízenou podle článku 29 ([2]), současný právní rámec ponechává prostor pro jednoznačnější podporu zásady soukromí coby aspekt návrhu.

IV.2 **Zapracování zásady soukromí coby aspekt návrhu na různých úrovních**

38. Ve světle výše uvedeného evropský inspektor ochrany údajů doporučuje Komisi, aby provedla čtyři kroky:

a) navrhla zahrnout obecné ustanovení o soukromí coby aspektu návrhu do právního rámce pro ochranu údajů;

b) podrobně popsala toto obecné ustanovení ve specifických ustanoveních, až budou navrženy konkrétní právní nástroje v různých odvětvích. Tato specifická ustanovení by již nyní mohla být zahrnuta do právních nástrojů, a to na základě článku 17 směrnice o ochraně údajů (a dalších stávajících právních předpisů);

c) zahrnula soukromí coby aspekt návrhu jako vedoucí zásadu do evropské digitální agendy;

d) zavedla soukromí coby aspekt návrhu jako zásadu do dalších iniciativ EU (zejm. nelegislativní povahy).

Obecné ustanovení o soukromí coby aspektu návrhu

39. Evropský inspektor ochrany údajů navrhuje jednoznačně a výslovně zahrnout zásadu soukromí coby aspekt návrhu do stávajícího právního rámce ochrany údajů. To by zajistilo, že tato zásada bude silnější, zřetelnější a že si kromě zajištění větší oprávněnosti donucovacích orgánů vyžadovat její *de facto* uplatňování v praxi vynutí účinné provádění. To je zejména nutné s ohledem na výše popsané skutečnosti, nejen kvůli důležitosti samotné zásady jako nástroje podpory důvěry, ale také jako stimulu pro zainteresované strany, aby prováděly zásadu soukromí coby aspekt návrhu a prohloubily záruky, které jsou již obsaženy ve stávajícím právním rámci.

40. Tento návrh navazuje na doporučení pracovní skupiny zřízené podle článku 29 zavést zásadu „soukromí coby aspekt návrhu“ jako obecnou zásadu do právního rámce ochrany údajů, a to zejména směrnice o ochraně údajů. Jak uvádí pracovní skupina zřízená podle článku 29: „Tato zásada by měla být závazná pro návrháře a výrobce technologií i pro správce údajů, kteří musí rozhodovat o pořízení a využívání IKT. Měli by mít povinnost zohlednit technologickou ochranu údajů již v etapě plánování informačních a technologických postupů a systémů. Poskytovatelé takových systémů nebo služeb i správci by měli prokázat, že přijali všechna opatření vyžadovaná pro vyhovění těmto požadavkům“.

41. Evropský inspektor ochrany údajů také vítá podporu zásady soukromí coby aspekt návrhu ze strany komisařky Viviane Redingové vyjádřenou v souvislosti s oznámením o přezkoumání směrnice o ochraně údajů ([3]).

42. Tím se dostáváme k obsahu takové regulace. Prvním a nejdůležitějším ohledem je, že zásada soukromí coby aspekt návrhu by měla být nezávislá na technologii. Tato zásada by neměla regulovat technologii, tedy neměla by předepisovat konkrétní technická řešení. Místo toho by

([1]) Viz zpráva úřadu komisaře Spojeného království pod názvem: „Privacy by Design“ (Soukromí coby aspekt návrhu), zveřejněná v listopadu 2008.

([2]) Viz Stanovisko 168 pracovní skupiny zřízené podle článku 29 k budoucnosti soukromí, společný příspěvek ke konzultaci Evropské komise k právnímu rámci pro základní právo na ochranu osobních údajů přijaté dne 1. prosince 2009.

([3]) „Soukromí coby aspekt návrhu je zásada, která je v zájmu občanů i podniků. Soukromí coby aspekt návrhu povede k lepší ochraně pro fyzické osoby i k důvěře v nové služby a výrobky, která zase povede ke kladnému dopadu na hospodářství. Existují některé povzbudivé příklady, ale je třeba udělat ještě daleko více“) Hlavní projev v Den ochrany osobních údajů, 28. ledna 2010, Evropský parlament, Brusel.

měla nařizovat, aby stávající zásady ochrany soukromí a údajů byly začleněny do informačních a komunikačních systémů a řešení. To by umožnilo zainteresovaným stranám, výrobcům, správcům údajů a úřadům na ochranu údajů vykládat význam této zásady v každém jednotlivém případě. Za druhé by vyhovění této zásadě bylo povinné v různých etapách, od vytvoření norem a návrhu architektury po jejich provedení ze strany správce údajů.

Ustanovení ve specifických právních předpisech

43. Zásadu soukromí coby aspekt návrhu bude nutno začlenit do stávajících i budoucích právních předpisů, a to na základě současného právního rámce a – po jeho přijetí – na základě výše zmíněného obecného ustanovení. Například podle současných iniciativ týkajících se inteligentních dopravních systémů Komise bude mít konkrétní počáteční odpovědnost při vymezení opatření, normalizačních iniciativ, postupů a osvědčené praxe. Při provádění těchto úkolů by zásada soukromí coby aspekt návrhu měla být vedoucí zásadou.

44. Evropský inspektor ochrany údajů dále poznamenává, že zásada soukromí coby aspekt návrhu má také specifický význam v oblasti svobody, bezpečnosti a práva, zejména ve vztahu k cílům strategie pro správu informací, jak se předpokládají ve Stockholmském programu [1]. Ve svém stanovisku týkajícím se Stockholmského programu evropský inspektor ochrany údajů zdůraznil, že architektura pro výměnu informací by měla být založena na „soukromí coby aspektu návrhu“ [2]: „Konkrétněji to znamená, že by informační systémy, které jsou navrhovány za účelem veřejné bezpečnosti, měly být vždy vytvářeny v souladu se zásadou soukromí coby aspekt návrhu“.

45. Stanovisko pracovní skupiny zřízené podle článku 29 k budoucnosti soukromí [3] ještě přesněji zdůrazňuje, že v oblasti svobody, bezpečnosti a práva, kde jsou hlavními aktéry veřejné orgány a kde opatření ke zvýšení dohledu mají přímý dopad na základní práva na ochranu soukromí a údajů, by požadavky soukromí coby aspektu návrhu měly být povinné. Zavedením těchto požadavků do informačních systémů by vlády také podpořily soukromí coby aspekt návrhu jako první zákazníci.

[1] Stockholmský program – Otevřená a bezpečná Evropa, která slouží občanům a chrání je, schválený Evropskou radou v prosinci 2009.

[2] Stanovisko ze dne 10. července 2009 ke sdělení Komise Evropskému parlamentu a Radě o prostoru svobody, bezpečnosti a práva ve službách občanům, Úř. věst. C 276, 17.11.2009, s. 8, bod 60.

[3] Stanovisko 168 pracovní skupiny zřízené podle článku 29 k budoucnosti soukromí, společný příspěvek ke konzultaci Evropské komise k právnímu rámci pro základní právo na ochranu osobních údajů, přijaté dne 1. prosince 2009.

Soukromí coby aspekt návrhu jako vedoucí zásada v evropské digitální agendě

46. Informační a komunikační technologie jsou stále složitější a nesou s sebou větší rizika pro ochranu soukromí a údajů. Obecně platí, že digitalizované informace, ke kterým lze snadněji přistupovat, kopírovat je a předávat, jsou vystaveny daleko větším rizikům než informace na papíru. Na cestě k sítím vzájemně propojených objektů se tato rizika budou zvyšovat. Čím větší jsou rizika pro ochranu soukromí a údajů, tím větší bude poptávka po vylepšených zárukách ochrany údajů a soukromí. Proto je ospravedlnění potřeby provádění soukromí coby aspektu návrhu závažnější v odvětví IKT. Kromě toho, jak bylo uvedeno výše, důvěra jednotlivců v IKT je zásadní, pokud mají občané přijmout tyto nové služby, a klíčovými prvky této důvěry je ochrana soukromí a údajů.

47. Výše uvedené zdůrazňuje, že strategie pro rozvoj IKT musí potvrdit nutnost, aby tyto technologie byly navrhovány se začleněným prvkem ochrany soukromí a údajů, tedy při zohlednění zásady soukromí coby aspekt návrhu.

48. Proto by evropská digitální agenda měla výslovně schválit zásadu soukromí coby aspekt návrhu jako nezbytný prvek pro zajištění důvěry občanů v IKT a on-line služby. Měla by uznat, že soukromí a důvěra jdou ruku v ruce a že soukromí coby aspekt návrhu by mělo být vedoucím faktorem při rozvoji důvěryhodného odvětví IKT.

Soukromí coby aspekt návrhu jako zásada v dalších iniciativách EU

49. Komise by měla zajistit, aby soukromí coby aspekt návrhu bylo vedoucí zásadou při provádění politik, činností a iniciativ ve specifických odvětvích IKT, včetně elektronických aplikací pro zdravotnictví, zadávání veřejných zakázek, sociálního zabezpečení, učení (eHealth, eProcurement, eSocial Security, eLearning) atd. Mnohé z těchto iniciativ budou prováděny v rámci evropské digitální agendy.

50. To například znamená, že iniciativy k zajištění efektivnějších a modernějších aplikací státní správy umožňující vzájemnou komunikaci s fyzickými osobami by měly zahrnovat potřebu jejich navrhování a provozu v souladu se zásadou soukromí coby aspekt návrhu. Totéž platí pro politiky a činnosti Komise, které se zabývají rychlejším internetem, digitálním obsahem nebo celkovou podporou pevné či bezdrátové komunikace a přenosu údajů.

51. Výše uvedené také zahrnuje oblasti, kde je Komise odpovědná za rozsáhlé systémy informační technologie, jako je SIS a VIS, i ty případy, kdy je odpovědnost Komise omezena na rozvoj a údržbu společné infrastruktury takového systému, jako je Evropský informační systém rejstříků trestů (ECRIS).

52. Jak přesně bude rozvinuta zásada soukromí coby aspekt návrhu, bude záviset na každém konkrétním odvětví a situaci. Pokud například iniciativy Komise doprovází návrhy právních předpisů v konkrétním odvětví IKT, bude v mnoha případech vhodné zahrnout výslovný odkaz na tuto zásadu do návrhu konkrétní aplikace nebo systému IKT. Rovněž navržené akční plány pro specifickou oblast by měly systematicky zajišťovat uplatňování právního rámce a konkrétněji zaručit, aby příslušná IKT byla vytvořena při zohlednění zásady soukromí coby aspektu návrhu.

53. Pokud se týká výzkumu, sedmý rámcový program a následující programy by se měly používat jako nástroj pro podporu projektů majících za cíl analýzu norem, IKT a architektury, které lépe slouží ochraně soukromí, a zejm. zásadě soukromí coby aspektu návrhu. Navíc by tato zásada měla také být nezbytným prvkem, který je třeba brát v úvahu u širších projektů IKT, jejichž cílem je zpracovávání osobních údajů fyzických osob.

Oblasti, které vyžadují zvláštní pozornost

54. V důsledku zvláštních rizik pro ochranu soukromí a údajů fyzických osob nebo v důsledku dalších faktorů (jako např. nevůle výrobců poskytovat produkty vycházející ze zásady soukromí coby aspekt návrhu, poptávka spotřebitelů atd.) může být v některých případech nutné vymezit konkrétnější a specifická opatření pro soukromí coby aspekt návrhu, která musí být zapracována do daného typu informačního a komunikačního produktu nebo technologie, a to v legislativních či jiných nástrojích.

55. Evropský inspektor ochrany údajů určil různé oblasti (RFID, aplikace tvorby sociálních sítí a prohlížečů), které si podle jeho názoru v této etapě zasluhují pečlivé zvážení ze strany Komise a praktický přístup nastíněný výše. O těchto třech oblastech je dále pojednáno v následujícím textu.

V. **IDENTIFIKACE NA ZÁKLADĚ RÁDIOVÉ FREKVENCE – RFID**

56. Štítky RFID mohou být použity u předmětů, zvířat a lidí. Mohou se používat pro sběr a ukládání osobních údajů, jako jsou lékařské záznamy, ke sledování pohybů lidí nebo tvorbě profilu jejich chování pro různé účely. To vše lze provádět, aniž by o tom fyzická osoba věděla ([1]).

57. Pro důvěru veřejnosti v RFID a budoucí internet věcí jsou rozhodující účinné záruky týkající se ochrany údajů, soukromí a všech souvisejících etických aspektů. Pouze pak bude tato technologie schopná přinášet četné ekonomické a společenské přínosy.

V.1 **Mezery v použitelném právním rámci ochrany údajů**

58. Směrnice o ochraně údajů a směrnice o soukromí a elektronických komunikacích se vztahuje na shromažďování údajů prováděné prostřednictvím aplikací RFID ([2]). Mezi jiným vyžadují, aby byly zavedeny vhodné záruky ochrany soukromí při provozu aplikací RFID ([3]).

59. Tento právní rámec se však nezabývá všemi oblastmi vzbuzujícími obavy v oblasti ochrany údajů a soukromí a které přináší tato technologie. Je to tím, že směrnice nejsou dostatečně podrobné, pokud jde o typ ochranných

([1]) RFID je zkratkou pro identifikaci na základě rádiové frekvence. Hlavními složkami technologie *nebo* infrastruktury identifikace na základě rádiové frekvence je *štítek* (tj. mikročip), čtečka a aplikace spojená se štítky a čtečkami prostřednictvím integračního softwaru (middleware) a zpracování generovaných údajů. Štítek se skládá z elektronického obvodu, který ukládá údaje, a antény, která předává údaje prostřednictvím rádiových vln. Čtečka má anténu a demodulátor, který převádí příchozí analogové informace z rádiového spojení na digitální údaje. Tyto informace lze pak zasílat přes sítě do databází a na servery za účelem počítačového zpracování.

([2]) Směrnice o soukromí a elektronických komunikacích odkazuje na RFID v článku 3: „Tato směrnice se vztahuje na zpracování osobních údajů ve spojení s poskytováním veřejně dostupných služeb elektronických komunikací ve veřejných komunikačních sítích ve Společenství, včetně veřejných komunikačních sítí podporujících zařízení pro shromažďování a identifikaci údajů". To je doplněno bodem odůvodnění 56: „Technologický pokrok umožňuje vývoj nových aplikací na bázi zařízení pro shromažďování a identifikaci údajů, což mohou být bezkontaktní zařízení využívající rádiové frekvence. Například rádiová identifikační zařízení (RFID) využívají rádiové frekvence na zachycení údajů z jedinečně označených štítků, které lze poté přenášet přes stávající komunikační sítě. Široké využívání těchto technologií může přinést značné hospodářské a společenské výhody, a významně tak přispět k vnitřnímu trhu, je-li jejich používání pro občany přijatelné. Aby toho bylo dosaženo, je třeba zajistit ochranu základních práv jednotlivců, a zejména práva na soukromí a ochranu údajů. Jsou-li tato zařízení připojena k veřejně přístupným sítím elektronických komunikací nebo využívají-li služby elektronických komunikací jako základní infrastrukturu, měla by se použít příslušná ustanovení směrnice 2002/58/ES (směrnice o soukromí a elektronických komunikacích), včetně ustanovení o bezpečnosti, provozních a lokalizačních údajích a důvěrnosti".

([3]) Například článek 17 směrnice o ochraně údajů ukládá povinnost přijmout vhodná technická a organizační opatření na ochranu osobních údajů proti náhodnému nebo nedovolenému zničení nebo neoprávněnému sdělování.

opatření, které by měly být zavedeny u aplikací RFID. Stávající pravidla je třeba doplnit dalšími, která by ukládala konkrétní opatření, a to zejména povinnost zapracovat technická řešení (soukromí coby aspekt návrhu) do RFID technologie. To platí pro štítky, které ukládají osobní informace, jež by měly obsahovat příkazy ke zničení, a pro používání šifrování u štítků, které uchovávají určité typy osobních informací.

V.2 **Samoregulace jako první krok**

60. V březnu 2007 Komise přijala sdělení ([1]), kterým mimo jiné uznala potřebu nezbytných pokynů k praktickému provádění RFID a vhodnost přijetí konstrukčních kritérií pro zamezení rizikům pro soukromí a bezpečnost.

61. Pro dosažení těchto cílů Komise v květnu 2009 přijala doporučení o zavedení zásad ochrany soukromí a údajů v RFID aplikacích ([2]). U maloobchodně prodávaných RFID aplikací to vyžaduje deaktivaci štítků v místě prodeje, pokud fyzické osoby neudělily souhlas k jejich používání. Toto pravidlo platí v případě že, zhodnocení dopadu na ochranu soukromí a údajů neprokáže, že štítky pravděpodobně nepředstavují hrozbu pro soukromí nebo ochranu osobních údajů, V takovém případě by štítky zůstaly aktivní s tím, že by se fyzické osoby mohly rozhodnout pro bezplatnou deaktivaci.

62. Evropský inspektor ochrany údajů souhlasí s přístupem Komise použít samoregulační nástroje. Jak je však popsáno níže, lze si představit, že samoregulace nepřinese očekávané výsledky, proto vyzývá Komisi, aby byla připravena přijmout alternativní opatření.

V.3 **Problematické oblasti a případná další opatření, pokud samoregulace selže**

63. Evropský inspektor ochrany údajů má obavy, že organizace provozující RFID aplikace v maloobchodě mohou přehlédnout možnost, že RFID štítky jsou sledovány nežádoucími třetími stranami. Při takovém sledování může dojít k vyzrazení případných osobních údajů uložených na štítku, ale mohlo by také umožnit třetí straně, aby sledovala nebo časem identifikovala určitou osobu na základě pouhého využití jedinečných identifikátorů obsažených v jednom nebo několika štítcích, které fyzická osoba má při sobě, a to dokonce v prostředí, které je mimo provozní okruh RFID aplikace. Dále má obavy, že provozovatelé RFID aplikací mohou mít tendenci spoléhat se bez řádného důvodu na výše zmíněnou výjimku, a ponechávat tak provozuschopné štítky i za místem prodeje.

64. Pokud k tomu dojde, může být příliš pozdě na zmírnění rizik pro ochranu údajů a soukromí fyzických osob, které již mohly být postiženy. Navíc když vezmeme v úvahu povahu samoregulace, vnitrostátní donucovací orgány mohou mít slabší postavení, když vyžadují, aby organizace provozující RFID aplikace uplatňovaly konkrétní opatření týkající se soukromí coby aspektu návrhu.

65. Ve světle výše uvedeného evropský inspektor ochrany údajů vyzývá Komisi, aby byla připravena navrhnout právní předpisy regulující hlavní problémy použití RFID v případě, že selže účinné provádění stávajícího právního rámce. Hodnocení Komise by nemělo být bez řádného důvodu odkládáno; odkládání by ohrozilo fyzické osoby a bylo by také kontraproduktivní pro průmysl, protože právní nejistota je příliš vysoká a související problémy by mohly být komplikovanější a jejich náprava nákladnější.

66. V rámci opatření, která bude možná nezbytné navrhnout, evropský inspektor ochrany údajů doporučuje stanovit zásadu rozhodnutí pro deaktivaci v místě prodeje, podle které by všechny RFID štítky, které jsou připojeny ke spotřebním výrobkům, byly standardně deaktivovány v místě prodeje. Nemusí být nutné nebo vhodné, aby Komise stanovila konkrétní technologii, která by měla být použita. Místo toho musí právo Unie stanovit právní povinnost získat souhlas k ponechání aktivace, čímž by se provozovatelům poskytl prostor pro rozhodnutí, jak tomuto požadavku vyhovět.

V.4 **Další otázky ke zvážení: Správa internetu věcí**

67. Informace generované RFID štítky – například informace o výrobku – mohou být nakonec propojeny do globální sítě komunikační infrastruktury. Tomu se obvykle říká „internet věcí". S ním vyvstávají otázky ochrany údajů/soukromí, protože předměty reálného světa lze identifikovat pomocí RFID štítků, které kromě informací o výrobku mohou zahrnovat osobní údaje.

68. Existuje mnoho otevřených otázek o tom, kdo bude řídit ukládání informací týkajících se položek opatřených štítky. Jak budou uspořádány? Kdo k nim bude mít přístup? V červnu 2009 Komise přijala sdělení o internetu věcí ([3]), které výslovně zmínilo potenciální problémy ochrany údajů a soukromí spojené s tímto jevem.

([1]) Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů ze dne 15.3.2007 o identifikaci na základě rádiové frekvence (RFID) v Evropě: kroky k rámci politiky, KOM(2007) 96 v konečném znění.

([2]) Doporučení Komise ze dne 12.5.2009 o zavedení zásad ochrany soukromí a údajů v aplikacích podporovaných identifikací na základě rádiové frekvence (C(2009) 3200 v konečném znění).

([3]) Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů: Internet věcí – akční plán pro Evropu, 18.6.2009, KOM(2009) 278 v konečném znění.

69. Evropský inspektor ochrany údajů by rád zdůraznil některé z otázek zmíněných v tomto sdělení, které si podle jeho názoru s rozvojem internetu věcí zasluhují zvýšenou pozornost. Za prvé potřeba decentralizované architektury může být nápomocná z hlediska odpovědnosti a vynutitelnosti právního rámce EU. Za druhé by mělo být v co největší možné míře zachováno právo fyzické osoby na to, aby sledována. Jinými slovy, měly by existovat jen velmi omezené případy, kdy dochází ke sledování fyzických osob prostřednictvím RFID štítků bez jejich souhlasu. Takový souhlas by měl být výslovný. To se obvykle nazývá „mlčení čipů" a právo na nerušený soukromý život. A konečně při navrhování internetu věcí by měla být vedoucí zásadou zásada soukromí coby aspekt návrhu. To by například vyžadovalo, aby konkrétní RFID aplikace, které mají zabudované mechanismy pro poskytnutí kontroly uživatelům, byly konstruovány se standardním nastavením ochrany soukromí.

70. Evropský inspektor ochrany údajů očekává, že bude konzultován, jakmile bude Komise zavádět opatření zmíněná v tomto sdělení, a to zejména ohledně návrhu sdělení o soukromí a důvěře ve všudypřítomnou informační společnost.

VI. **SOCIÁLNÍ SÍTĚ A POTŘEBA IMPLICITNÍHO NASTAVENÍ SOUKROMÍ**

71. Sociální sítě jsou trendem poslední doby, přičemž se zdá, že překonaly popularitu e-mailu. Spojují lidi navzájem na základě podobných zájmů či aktivit. Lidé mohou mít své profily na internetu a sdílet mediální soubory, jako jsou videa, fotografie, hudba, i své profesní profily.

72. Mládež rychle přijala tvorbu sociálních sítí a tento trend pokračuje. Průměrný věk uživatele internetu v Evropě v několika posledních letech poklesl: mladí ve věku 9–10 let se nyní připojují několikrát týdně; mladí ve věku 12–14 let jsou on-line každý den, často po dobu jedné až tří hodin.

VI.1 **Sociální sítě a použitelný právní rámec pro ochranu údajů a soukromí**

73. Rozvoj sociálních sítí umožnil uživatelům nahrávat na internet informace o nich samotných a o třetích stranách. Přitom podle pracovní skupiny zřízené podle článku 29 [1] uživatelé internetu ve vztahu údajům, které nahrávají [2], vystupují jako správci údajů podle čl. 2 písm. d) směrnice o ochraně údajů. Ve většině případů však takové zpracování patří do výjimky pro domácí činnosti podle čl. 3 odst. 2 směrnice. Současně jsou služby tvorby sociálních sítí považovány za správce údajů, pokud poskytují prostředky pro zpracování údajů uživatelů a všechny základní služby týkající se správy uživatelů (např. registraci a vymazání účtů).

74. V právním smyslu to znamená, že uživatelé internetu a služby tvorby sociálních sítí sdílejí společnou odpovědnost za zpracování osobních údajů jako „správci údajů" ve smyslu čl. 2 písm. d) směrnice, třebaže do různého stupně a při odlišných povinnostech.

75. Podobně by uživatelé měli vědět a chápat, že na základě zpracovávání svých osobních údajů i osobních údajů dalších osob se na ně vztahují ustanovení právních předpisů EU týkající se ochrany údajů, která mimo jiné vyžadují získání informovaného souhlasu osob, jejichž informace jsou nahrávány, a poskytnutí práv na opravu, námitku atp. Také služby tvorby sociálních sítí musí mezi jiným přijmout vhodná technická a organizační opatření pro zabránění nedovoleného zpracování při zohlednění rizik spojených se zpracováním a s povahou údajů. To zase znamená, že služby tvorby sociálních sítí by měly zajistit standardní nastavení, které umožňuje ochranu soukromí, včetně nastavení, které omezuje přístup k profilu na kontakty, které si uživatel sám zvolil. Před tím, než by byl jakýkoli profil přístupný pro jiné třetí strany, by nastavení také vyžadovalo potvrzující souhlas uživatele a profily se zakázaným přístupem by nemělo být možné vyhledat vnitřními vyhledávači.

76. Bohužel sama existence výše zmíněných právními požadavky nestačí k zajištění jejich dodržování. Přestože jsou uživatelé internetu z právního hlediska považováni za správce údajů a jsou vázáni právním rámcem EU pro ochranu údajů a soukromí, ve skutečnosti často nemají o této úloze žádné povědomí. Obecně nedostatečně rozumí skutečnosti, že zpracovávají osobní údaje a že se zveřejňováním takových informací jsou spojena rizika pro ochranu soukromí a údajů. Zejména mládež zveřejňuje obsah on-line a podceňuje přitom důsledky pro sebe i pro jiné, například v souvislosti s následným studiem nebo žádostmi o pracovní místo.

---

[1] Viz Stanovisko 163, 5/2009 pracovní skupiny zřízené podle článku 29 k tvorbě internetových sociálních sítí přijaté dne 12. června 2009.

[2] „Správcem" se rozumí fyzická či právnická osoba, veřejný orgán, agentura nebo jakýkoli jiný orgán, který sám nebo společně s jinými rozhoduje o účelech a prostředcích zpracování osobních údajů; kde účely a prostředky zpracování stanoví vnitrostátní zákony nebo předpisy nebo zákony či předpisy Společenství, může být správce nebo specifická kritéria pro jeho jmenování stanoveny vnitrostátním právem nebo právem Společenství.

77. Poskytovatelé sociální sítě současně často předem zavádějí standardní nastavení na základě možnosti netrvat na ochraně soukromí a tím napomáhají poskytování osobních informací. Někteří umožňují, aby profily byly přístupné pro běžné vyhledávače. To vede k otázkám, zda fyzické osoby skutečně souhlasily s poskytnutím údajů i zda sociální sítě vyhověly článku 17 směrnice (popsanému výše), který po nich vyžaduje, aby přijaly vhodná technická a organizační opatření pro zabránění nedovolenému zpracování.

VI.2 **Rizika generovaná sociálními sítěmi a navrhované kroky k jejich řešení**

78. Výše uvedené vede ke zvýšenému riziku pro ochranu soukromí a údajů fyzické osoby. Vystavuje uživatele internetu a osoby, jejichž údaje byly nahrány, zřejmým porušením jejich ochrany soukromí a údajů.

79. V této souvislosti je otázkou, kterou by se Komise měla zabývat, co by mělo a mohlo být uděláno pro řešení této situace. Toto stanovisko neposkytuje vyčerpávající odpověď na tuto otázku, místo toho předkládá řadu návrhů k dalšímu zvážení.

Investování do vzdělání uživatelů internetu

80. Prvním návrhem je investovat do vzdělání uživatelů. V tomto ohledu by instituce EU a vnitrostátní orgány měly investovat do vzdělávání a zvyšování povědomí o hrozbách, které představují internetové stránky tvorby sociálních sítí. Například generální ředitelství pro informační společnost a média provádí program bezpečnějšího internetu, který má posílit a chránit děti a mládež například prostřednictvím činností ke zvyšování povědomí ([1]). Instituce EU nedávno zahájily kampaň „Mysli, než něco dáš na net!“ ke zvýšení povědomí o rizicích sdílení osobních informací s cizími lidmi.

81. Evropský inspektor ochrany údajů vyzývá Komisi, aby i nadále podporovala tento typ činnosti. Samotní poskytovatelé sociálních sítí by však také měli hrát aktivní úlohu, protože mají právní a sociální odpovědnost za vzdělávání uživatelů o tom, jak využívat jejich služby bezpečně a při zajištění soukromí.

82. Jak bylo popsáno výše, když jsou informace zveřejňovány na sociálních sítích, mohou být tyto informace implicitně zpřístupněny řadou různých způsobů. Například informace mohou být přístupné pro širokou veřejnost, včetně vyhledávačů, které je mohou opatřit indexy a poskytovat tak na ně přímé odkazy. Na druhé straně informace mohou být omezeny na „vybrané přátele“ nebo mohou být uchovávány jako zcela soukromé. Je jasné, že povolení profilů a používaná terminologie se liší podle dané sítě.

83. Jak však bylo popsáno výše, velmi málo uživatelů služeb tvorby sociálních sítí má povědomí o tom, jak ovládat přístup na informace, které zveřejňují, tím méně jak měnit standardní nastavení ochrany soukromí. Toto nastavení obvykle zůstává beze změny, protože uživatelé nemají povědomí o jeho dopadech nebo nevědí, jak to udělat. Nezměněné nastavení ochrany soukromí tedy velmi často neznamená, že by fyzické osoby učinily informované rozhodnutí přijmout sdílení informací. V této souvislosti je zejména důležité, aby třetí strany jako vyhledávače neodkazovaly na jednotlivé profily na základě předpokladu, že uživatelé implicitně souhlasili (tím, že nezměnili nastavení soukromí) s neomezeným zpřístupněním informací.

84. I když vzdělání uživatelů může pomoci řešit tuto situaci, nebude fungovat samo o sobě. Jak doporučuje pracovní skupina zřízená podle článku 29 ve svém stanovisku k sociálním sítím, poskytovatelé sociálních sítí by měli standardně a bezplatně nabízet taková nastavení, která zajišťují ochranu soukromí. To by zajistilo větší povědomí uživatelů a umožnilo jim lépe se rozhodovat o tom, zda chtějí sdílet informace a s kým.

Úloha pro samoregulaci

85. Komise uzavřela dohodu s dvaceti poskytovateli sociálních sítí pod názvem Bezpečnější zásady tvorby sociálních sítí pro EU ([2]). Cílem této dohody je zlepšit bezpečnost nezletilých při používání internetových stránek pro tvorbu sociálních sítí v Evropě. Tyto zásady zahrnují mnoho požadavků odvozených z uplatňování právního rámce ochrany údajů popsaného výše. Zahrnují například požadavek posílit postavení uživatelů pomocí technologie s cílem zajistit kontrolu nad využitím a šířením jejich osobních informací. Dohoda zahrnuje také potřebu poskytování standardního nastavení ochrany soukromí.

86. Na začátku ledna 2010 Komise zpřístupnila zprávu hodnotící provádění těchto zásad ([3]). Evropský inspektor ochrany údajů má obavy, že tato zpráva ukazuje, že

([1]) Informace o tomto programu jsou dostupné na adrese: http://ec.europa.eu/information_society/activities/sip/index_en.htm

([2]) Tato dohoda je dostupná na adrese: http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf

([3]) Zpráva o hodnocení provádění Bezpečnějších zásad tvorby sociálních sítí pro EU, dostupné na adrese: http://ec.europa.eu/information_society/activities/social_networking/docs/final_report/first_part.pdf

zatímco některé kroky byly učiněny, mnoho dalších nebylo. Například zpráva zjistila problémy se sdělováním bezpečnostních opatření a nástrojů, které jsou dostupné na internetových stránkách. Zjistila také, že méně než polovina signatářů dohody omezuje přístup k profilům nezletilých pouze na jejich přátele.

Potřeba povinného stqndardního nastavení ochrany soukromí

87. V této souvislosti je klíčovou otázkou, zda jsou nezbytná další politická opatření, aby se zajistilo, že služby sociálních sítí budou obsahovat standardní nastavení ochrany soukromí. Tento problém zmínila bývalá komisařka pro informační společnost, Viviane Redingová, která zdůraznila, že může dojít k nutnosti regulace ([1]). Podobně i Evropský hospodářský a sociální výbor uvedl, že spolu se samoregulací by měly být minimální normy ochrany uloženy závazným právním předpisem ([2]).

88. Jak bylo poznamenáno výše, povinnost poskytovatelů sociálních sítí zavádět standardní nastavení soukromí lze nepřímo odvodit z článku 17 směrnice o ochraně údajů ([3]), která ukládá správcům údajů přijmout vhodná technická a organizační opatření („jak při přípravě systému zpracování, tak v průběhu vlastního zpracování") s cílem zajistit bezpečnost a zabránit neoprávněnému zpracování při zohlednění rizik, která představují zpracování a povaha údajů.

89. Tento článek je však příliš obecný a také v této souvislosti postrádá specifičnost. Neuvádí jasně, co je míněno vhodnými technickými a organizačními opatřeními v souvislosti se sociálními sítěmi. Současná situace je tak situací právní nejistoty, což způsobuje problémy pro regulační orgány i fyzické osoby, jejichž soukromí a ochrana údajů nejsou plně chráněny.

90. S ohledem na výše uvedené evropský inspektor ochrany údajů vyzývá Komisi, aby navrhla právní předpisy, které by jako minimum upravovaly obecnou povinnost vyžadující povinné nastavení soukromí spolu s přesnějšími požadavky:

a) na poskytování nastavení omezujícího přístup k profilům uživatelů na vlastní kontakty zvolené uživatelem. Toto nastavení by také vyžadovalo potvrzující souhlas uživatele před tím, než by byl jakýkoli profil přístupný pro třetí strany;

b) na zajištění, aby profily s omezeným přístupem nemohly být nalezeny vnitřními a vnějšími vyhledávači.

91. Kromě zajištění povinného standardního nastavení ochrany soukromí zůstává otázka, zda by také nebyla vhodná další specifická opatření ochrany údajů a jiná opatření (například týkající se ochrany nezletilých). To vede k další otázce, totiž zda by bylo užitečné vytvořit specifický rámec pro tyto typy služeb, který by kromě uložení povinného nastavení soukromí reguloval další aspekty. Evropský inspektor ochrany údajů žádá Komisi, aby tuto otázku zvážila.

VII. **STANDARDNÍ NASTAVENÍ OCHRANY SOUKROMÍ U PROHLÍŽEČŮ PRO ZARUČENÍ INFORMOVANÉHO SOUHLASU PRO PŘIJÍMÁNÍ REKLAMY**

92. Poskytovatelé sítí inzerce využívají cookies a další nástroje pro sledování chování jednotlivých uživatelů, když se pohybují na internetu, s cílem vytvářet seznam jejich zájmů a profily. Tyto informace se pak používají k zasílání cílené reklamy ([4]).

VII.1 **Další výzvy a rizika v souvislosti se stávajícím právním rámcem v oblasti ochrany údajů a soukromí**

93. Toto zpracování je upraveno ve směrnici o ochraně údajů (pokud se jedná o osobní údaje) a také v čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích. Tento článek konkrétně vyžaduje, aby byl uživatel informován a dostal příležitost reagovat souhlasem nebo odmítnutím týkajícím se ukládání nástrojů, jako jsou cookies atd. na jeho počítač nebo jiná zařízení ([5]).

94. Až dosud provozovatelé reklamní sítě spoléhali na nastavení prohlížečů a na politiky soukromí, aby uživatele informovali a umožnili jim poskytnout souhlas nebo odmítnout cookies. V politikách soukromí vydavatelů

([1]) Viviane Redingová, členka Evropské komise odpovědná za informační společnost a média. Mysli, než něco dáš na net! Jak zajistit bezpečnější internetové stránky tvorby sociálních sítí pro děti a dospívající? Den pro bezpečnější internet, Štrasburk 9. února 2010.

([2]) Stanovisko Evropského hospodářského a sociálního výboru k dopadu internetových stránek sociálních sítí na občany/spotřebitele, 4. listopadu 2009.

([3]) Podrobněji popsáno také v bodu 33 tohoto dokumentu.

([4]) Cookies pro sledování jsou malé textové soubory, které obsahují jedinečný identifikátor. Poskytovatelé sítě inzerce (stejně jako provozovatelé internetových stránek nebo vydavatelé) obvykle umístí cookies na pevný disk návštěvníka, zejména do prohlížeče uživatelů internetu, když uživatelé poprvé vstoupí na internetové stránky, které nabízejí inzeráty, které jsou součástí jejich sítě. Cookie umožní poskytovateli sítě inzerce poznat dřívějšího návštěvníka, který se na tyto internetové stránky vrací nebo navštíví jakoukoli partnerskou internetovou stránku sítě inzerce. Takové opakované návštěvy umožní poskytovateli sítě inzerce vytvořit profil návštěvníka.

([5]) Čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích byl nedávno změněn, aby posílil ochranu před zachycováním komunikace uživatelů prostřednictvím použití například spywaru a cookies uložených na počítači nebo jiných zařízeních uživatele. Podle nové směrnice by měly být uživatelům nabídnuty lepší informace a snadnější způsoby, jak ovládat, zda chtějí mít cookies uloženy na svém koncovém zařízení.

vysvětlovali, jak úplně zamezit přijímání cookies nebo jak je přijímat případ od případu. Tímto způsobem měli v úmyslu vyhovět své povinnosti nabídnout uživateli právo odmítnout cookies.

95. Zatímco teoreticky by tato metoda (prostřednictvím prohlížeče) mohla skutečně účinně zajistit smysluplný informovaný souhlas, realita je velmi odlišná. Obecně platí, že uživatelé nemají základní ponětí o shromažďování jakýchkoli údajů, tím méně údajů poskytnutých třetími stranami, hodnotě takových údajů, jejich využití, fungování příslušné technologie, a zejména toho, jak a kde zabránit přijímání cookies. Zdá se, že kroky, které musí uživatelé učinit, aby přijímání zabránili, jsou nejen komplikované, ale také nepřiměřené (nejdříve musí nastavit svůj prohlížeč na přijímání cookies, pak provést volbu zabránění přijímání).

96. V důsledku toho v praxi dochází k tomu, že velmi málo lidí provádí volbu zabránění přijímání cookies, nikoli proto, že by učinili informované rozhodnutí přijímat cílenou reklamu, ale spíše proto, že si neuvědomují, že když tuto volbu neprovedou, pak vlastně poskytují souhlas.

97. Zatímco tedy z právního hlediska čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích stanoví účinnou právní ochranu, v praxi se má za to, že uživatelé internetu souhlasí se sledováním pro účely zasílání reklamy na základě jejich chování, když vlastně v mnoha, ne-li ve většině případů vůbec nevědí o tom, že dochází ke sledování.

98. Pracovní skupina zřízená podle článku 29 připravuje stanovisko s cílem upřesnit právní požadavky pro využívání cílené reklamy, což se vítá. Samotný výklad však nemusí být dostačující pro vyřešení této situace a může být nezbytné, aby Evropská unie učinila další kroky.

VII.2 **Potřeba dalšího kroku, zejména stanovení povinného standardního nastavení ochrany soukromí**

99. Jak bylo popsáno výše, internetové prohlížeče běžně umožňují určitou úroveň kontroly nad určitými druhy cookies. V současnosti je standardním nastavením většiny internetových prohlížečů přijímat všechny cookies. Jinými slovy, prohlížeče jsou implicitně nastaveny tak, aby přijímaly všechny cookies bez ohledu na účel dané cookie. Pouze pokud uživatel změní nastavení své aplikace prohlížeče tak, aby odmítla cookies, což, jak bylo výše popsáno, provede jen velmi málo uživatelů, nebude cookies přijímat. Navíc neexistuje žádný software pro ochranu soukromí při první instalaci nebo aktualizaci aplikací prohlížečů.

100. Tento problém by šlo zmírnit dodáváním prohlížečů se standardním nastavením ochrany soukromí. Jinými slovy, pokud by prohlížeče byly dodávány s nastavením „nepřijímat cookies třetích stran“. Jako doplnění a účinnější zajištění by prohlížeče měly vyžadovat, aby při první instalaci nebo aktualizaci prohlížeče uživatelé prošli softwarem pro ochranu soukromí. Existuje potřeba podrobnějších a srozumitelnějších informací o typech cookies a užitečnosti některých z nich. Uživatelé, kteří by byli ochotní být sledováni pro účely přijímání cílené reklamy, by o tom byli řádně informováni a museli by změnit nastavení svého prohlížeče. To by jim poskytlo zvýšenou kontrolu nad jejich osobními údaji a soukromím, což by podle názoru evropského inspektora ochrany údajů bylo účinným způsobem, jak respektovat a zachovat souhlas uživatelů ([1]).

101. Když vezmeme v úvahu na jedné straně rozšířenost tohoto problému, jinými slovy počet uživatelů internetu, kteří jsou v současnosti sledováni na základě zdánlivého souhlasu, a na druhé straně závažnost dotčeného zájmu, potřeba dalších ochranných opatření se stává ještě naléhavější. Provedení zásady soukromí coby aspekt návrhu u aplikací internetových prohlížečů by mohlo znamenat významný rozdíl při poskytování kontroly ve prospěch fyzických osob nad praktikami shromažďování údajů pro účely cílené.

102. Z těchto důvodů evropský inspektor ochrany údajů naléhá na Komisi, aby zvážila legislativní opatření, která by vyžadovala povinné standardní nastavení ochrany soukromí v prohlížečích a poskytování příslušných informací.

VIII. **DALŠÍ ZÁSADY ZAMĚŘENÉ NA OCHRANU SOUKROMÍ / OCHRANU ÚDAJŮ FYZICKÝCH OSOB**

103. I když má zásada soukromí coby aspekt návrhu velký potenciál pro zlepšení ochrany osobních údajů a soukromí fyzických osob, je pro zajištění důvěry spotřebitelů v IKT nezbytné zakotvení doplňujících zásad v příslušných právních předpisech. V této souvislosti se evropský inspektor ochrany údajů zabývá zásadou odpovědnosti a dokončením právního rámce týkajícího se narušení bezpečnosti, který bude použitelný napříč odvětvími.

VIII.1 **Zásada odpovědnosti pro zajištění vyhovění zásadě soukromí coby aspekt návrhu**

104. Dokument pracovní skupiny zřízené podle článku 29 pod názvem Budoucnost soukromí ([2]) doporučil, aby byla zásada odpovědnosti zahrnuta do směrnice o ochraně

([1]) Evropský inspektor ochrany údajů si současně uvědomuje, že by to tento problém úplně nevyřešilo, protože existují cookies, které nelze ovládat prostřednictvím prohlížeče, jako v případě tak zvaných flash cookies. Pro ně by bylo nutné, aby vývojáři při vydávání nových prohlížečů implicitně začlenili ovládání typu flash do jejich ovládání cookies.

([2]) Stanovisko 168 pracovní skupiny zřízené podle článku 29 k budoucnosti soukromí, společný příspěvek ke konzultaci Evropské komise k právnímu rámci pro základní právo na ochranu osobních údajů přijaté dne 1. prosince 2009.

údajů. Tato zásada, která je uznávána v některých nadnárodních nástrojích v oblasti ochrany údajů ([1]), vyžaduje, aby organizace přijaly postupy směřující k respektování stávajících právních předpisů a vytvořily metody pro jejich hodnocení a prokázání.

105. Evropský inspektor ochrany údajů plně podporuje doporučení pracovní skupiny zřízené podle článku 29. Má za to, že tato zásada bude vysoce významná pro podporu účinného uplatňování zásad a povinností týkajících se ochrany údajů. Odpovědnost bude vyžadovat, aby správci údajů prokázali, že zavedli nezbytné mechanismy za účelem zaručení souladu s platnými právními předpisy v oblasti ochrany údajů. To pravděpodobně přispěje k účinnému provádění zásady soukromí coby aspekt návrhu u IKT jako zvláště vhodného prvku pro prokázání odpovědnosti.

106. Pro stanovení a prokázání odpovědnosti by správci údajů mohli využívat vnitřní postupy a třetí strany, které mohou provádět audity nebo jiné typy kontrol a ověření a které by pak na jejich základě mohly udělovat pečetě nebo ceny. V této souvislosti evropský inspektor ochrany údajů vyzývá Komisi, aby zvážila, zda by kromě obecné zásady odpovědnosti bylo užitečné, aby byla stanovena konkrétní opatření jako je potřeba vytvářet hodnocení dopadu ochrany soukromí a údajů a za jakých podmínek.

VIII.2 **Narušení bezpečnosti: dokončení právního rámce**

107. Loňské změny směrnice o soukromí a elektronických komunikacích zavedly požadavek oznamovat narušení údajů dotčeným fyzickým osobám a také příslušným orgánům. Narušení údajů je široce definováno jako jakékoli narušení, které vede ke zničení, ztrátě, vyzrazení atd. osobních údajů přenášených, uchovávaných nebo jinak zpracovávaných v souvislosti se službou. Oznamování fyzickým osobám se bude vyžadovat, pokud by narušení údajů pravděpodobně nepříznivě ovlivnilo jejich osobní údaje nebo soukromí. To by mohlo nastat, jestliže by narušení mohlo vést ke krádeži totožnosti nebo významnému ponížení či poškození pověsti. Oznamování příslušným orgánům bude vyžadováno u každého narušení údajů bez ohledu, zda existuje riziko pro fyzické osoby.

Uplatňování povinností týkajících se narušení bezpečnosti napříč odvětvími

108. Tato povinnost se bohužel vztahuje pouze na poskytovatele veřejně přístupných služeb elektronických komunikací, jako jsou telefonní společnosti, poskytovatelé přístupu na internet, poskytovatelé internetových stránek atd. Evropský inspektor ochrany údajů vyzývá Komisi, aby předložila návrhy týkající se narušení bezpečnosti, které by se uplatňovaly napříč odvětvími. Pokud se jedná o obsah takového rámce, evropský inspektor ochrany údajů má za to, že právní rámec týkající se narušení bezpečnosti přijatý ve směrnici o soukromí a elektronických komunikacích nalézá vhodnou rovnováhu mezi ochranou práv fyzických osob, včetně jejich práv na ochranu osobních údajů a soukromí, a povinnostmi, které se ukládají výše zmíněným subjektům. Současně se jedná o efektivní právní rámec, protože se opírá o smysluplná donucovací ustanovení, která poskytují orgánům dostatečné pravomoci provádět šetření a ukládat sankce.

109. Evropský inspektor ochrany údajů také vyzývá Komisi, aby přijala návrh právního předpisu, který by podle potřeby s vhodnými úpravami uplatňoval tento rámec napříč odvětvími. Navíc by to zajistilo, že jsou napříč odvětvími uplatňovány stejné normy a postupy.

Dokončení právního rámce obsaženého ve směrnici o soukromí a elektronických komunikacích prostřednictvím projednávání ve výboru

110. Revidovaná směrnice o soukromí a elektronických komunikacích zmocňuje Komisi, aby přijala technická prováděcí opatření, tj. podrobná opatření týkající se oznamování narušení bezpečnosti prostřednictvím postupu projednávání ve výboru ([2]). Toto zmocnění je odůvodněno nutností zajistit jednotné provádění a uplatňování příslušného právního rámce. Jednotné provádění má za cíl zajistit, aby fyzické osoby v celém Společenství měly stejně vysokou úroveň ochrany a aby výše zmíněné subjekty nebyly zatěžovány odlišnými požadavky na oznamování.

111. Směrnice o soukromí a elektronických komunikacích byla přijata v listopadu 2009. Zdá se, že neexistuje žádný důvod, který by ospravedlňoval odkládání zahájení činnosti směřující k přijetí technických prováděcích opatření. Evropský inspektor ochrany údajů uspořádal dva semináře zaměřené na sdílení a sběr zkušeností o oznamování při narušení údajů. Rád by se podělil o výsledky těchto akcí a těší se na spolupráci s Komisí a dalšími zainteresovanými stranami při vylaďování celkového právního rámce týkajícího se narušení údajů.

112. Evropský inspektor ochrany údajů vyzývá Komisi, aby v krátkém časovém horizontu učinila nezbytné kroky. Před přijetím technických prováděcích opatření se Komise musí zapojit do širokých konzultací zahrnujících ENISA, evropského inspektora ochrany údajů a pracovní skupinu zřízenou podle článku 29. Tyto konzultace musí dále zapojovat další „příslušné zainteresované strany“, zejména s cílem získání informací o nejlepších dostupných technických a ekonomických prostředcích provedení.

([1]) Pokyny OHSR z roku 1980 k ochraně soukromí a přeshraničním tokům osobních údajů; Madridská deklarace o soukromí: Globální normy soukromí pro globální svět ze dne 3. listopadu 2009.

([2]) Projednávání ve výboru zahrnuje přijetí technických prováděcích opatření prostřednictvím výboru zástupců členských států, kterému předsedá Komise. Na směrnici o soukromí a elektronických komunikacích se vztahuje tak zvaný regulativní postup s kontrolou, což znamená, že Evropský parlament i Rada se mohou postavit proti opatřením navrženým Komisí. Další podrobnosti naleznete na adrese: http://europa.eu/scadplus/glossary/comitology_en.htm

IX. **ZÁVĚRY**

113. Důvěra nebo spíše její nedostatek byl určen jako základní problém pro vznik a úspěšné zavádění informačních a komunikačních technologií. Pokud by lidé neměli důvěru v IKT, tyto technologie by selhaly. Důvěra v IKT závisí na různých faktorech, přičemž klíčovým faktorem je zajištění, že tyto technologie nebudou poškozovat základní práva fyzických osob na soukromí a ochranu osobních údajů.

114. Aby došlo k dalšímu posílení právního rámce ochrany údajů a soukromí jako zásad, které zůstávají v informační společnosti zcela platné, evropský inspektor ochrany údajů navrhuje Komisi, aby na různých úrovních tvorby právních předpisů a politiky začlenila zásadu soukromí coby aspekt návrhu.

115. Evropský inspektor ochrany údajů navrhuje Komisi provést čtyři následující kroky:

a) navrhnout zahrnutí obecného ustanovení o soukromí coby aspektu návrhu do právního rámce ochrany údajů. Toto ustanovení by mělo být neutrální z hlediska technologie a jeho respektování by mělo být povinné v různých etapách;

b) podrobně rozpracovat toto obecné ustanovení ve specifických ustanoveních, až budou navrženy konkrétní právní nástroje v různých odvětvích. Tato specifická ustanovení by již nyní mohla být zahrnuta do právních nástrojů, a to na základě článku 17 směrnice o ochraně údajů (a dalších právních předpisů);

c) zahrnout soukromí coby aspekt návrhu jako vedoucí zásadu do evropské digitální agendy;

d) zavést soukromí coby aspekt návrhu jako zásadu do dalších iniciativ EU (hlavně jiné než legislativní povahy).

116. U tří určených oblastí IKT evropský inspektor ochrany údajů doporučuje Komisi, aby zhodnotila potřebu předložit návrhy, které by prováděly zásadu soukromí coby aspekt návrhu konkrétními způsoby:

a) ve vztahu k RFID navrhnout právní opatření regulující hlavní problémy použití RFID v případě, že selže účinné provádění stávajícího právního rámce prostřednictvím samoregulace. Zejména stanovit zásadu rozhodnutí pro aktivaci v místě prodeje, podle které by všechny RFID štítky, které jsou připojeny ke spotřebním výrobkům, byly standardně deaktivovány v místě prodeje;

b) ve vztahu k sociálním sítím navrhnout právní předpisy, které by jako minimum zahrnovaly širokou povinnost vyžadující povinné nastavení ochrany soukromí spolu s přesnějšími požadavky o omezení přístupu k profilům uživatelů na vlastní kontakty zvolené uživatelem a stanovení, že profily s omezeným přístupem nemohou být nalezeny vnitřními a vnějšími vyhledávači;

c) ve vztahu k cílené reklamě zvážit právní předpisy ukládajících nastavení prohlížečů, které by standardně odmítalo přijímání cookies třetích stran a vyžadovalo, aby uživatelé při první instalaci nebo aktualizaci prohlížeče prošli softwarem pro ochranu soukromí.

117. A konečně evropský inspektor ochrany údajů doporučuje Komisi, aby:

a) zvážila provedení zásady odpovědnosti ve stávající směrnici o ochraně údajů a

b) vytvořila rámec pravidel a postupů pro provedení ustanovení o oznamování narušení bezpečnosti ve směrnici o soukromí a elektronických komunikacích a rozšířila je tak, aby se vztahovala na všechny správce údajů.

V Bruselu dne 18. března 2010.

Peter HUSTINX

evropský inspektor ochrany údajů