top-normy

Ochrana soukromí spotřebitele v digitálním světě

(priority z hlediska spotřebitelů)

Editace: LIBOR DUPAL



ÚNMZ

KABINET PRO STANDARDIZACI
... top-normy .cz

SČS
SDRUŽENÍ ČESKÝCH SPOTŘEBITELŮ, Z. Ú.
CZECH CONSUMER ASSOCIATION
www.konzument.cz

ÚVOD - PŘEDMLUVA

Téma ochrany osobních údajů při elektronických operacích, které spotřebitel realizuje při nákupu výrobků a služeb, zejména prostřednictvím internetu, jsou velmi citlivým tématem současnosti. Jsou také předmětem určitých připravovaných, respektive již probíhajících regulativních kroků Evropské komise v kombinaci se samoregulativními a normativními opatřeními.

Spotřebitelé v současné době žijí v digitální „tmavé komoře", pokud jde o kontrolu nad způsobem, jakým jsou některými společnostmi shromažďovány a zpracovávány informace včetně totožnosti osob, informací o jejich každodenním životě, společenských aktivitách, politických názorech, koníčcích, finančních údajích a zdravotních záznamech. Probíhající reforma zastaralé a zejména ne vždy účinné evropské regulace je proto nanejvýš potřebná.

Sdružení českých spotřebitelů a Kabinet pro standardizaci působí na několika platformách, národních a zejména evropských, které se tématem digitálního světa a zejména ochrany soukromí spotřebitele zabývají. Zmíníme alespoň Konzultativní skupinu evropských spotřebitelů, což je pracovní poradenský orgán Evropské komise ustavený při Generálním ředitelství pro spravedlnost a spotřebitele, nebo ANEC, což je Evropské sdružení pro koordinaci účasti spotřebitelů na normalizaci. V obou těchto subjektech zastupuje české spotřebitele zástupce SČS.

V publikaci, kterou zájemcům nyní nabízíme, se pokoušíme podat informaci o existujících i připravovaných regulativních a normativních iniciativách, s analýzou z pohledu priorit spotřebitele, které by ve vztahu k ochraně spotřebitelského soukromí měly být řešeny. Tyto informace jsou prvotně potřebné pro zástupce organizací, které zastupují spotřebitelské zájmy v normotvorných aktivitách. Nepochybujeme však, že mohou být užitečné i pro jiné zainteresované strany včetně státní správy, aby samy lépe vnímaly potřeby spotřebitele. Užitečné informace v ní najdou i samotní spotřebitelé.

Jsme rádi, že toto téma oslovilo i Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, který podpořil vydání této publikace a zařadil ji jako úkol do Strategické vize pro evropské normy na rok 2015.

Ing. Libor Dupal, ředitel Sdružení českých spotřebitelů a ředitel Kabinetu pro standardizaci

OCHRANA SOUKROMÍ SPOTŘEBITELE V DIGITÁLNÍM SVĚTĚ (priority z hlediska spotřebitelů)

OBSAH

Publikace vznikla za podpory ÚNMZ za účelem naplňování „Strategické vize pro evropské normy".

Základem pro tuto publikaci jsou dokumenty ANEC , zejména ANEC edition Consumer Representatives Guidance Domestic Privacy and the Privacy of Digitally Connected Devices, určené k použití při zastupování zájmů spotřebitelů v technických normalizačních komisích. Podklady byly edičně upraveny z důvodu přizpůsobení našemu záměru a nutného omezení rozsahu naší publikace. Obsah byl konzultován s více odborníky včetně odborníky z ÚNMZ a dalšími autoritami, zodpovědnost za věcný obsah této tiskoviny je však plně na vydavateli.

1. ÚVOD DO OCHRANY SOUKROMÍ

1.1. Východiska regulace ochrany soukromí

Základem současné celosvětové právní úpravy v oblasti ochrany osobních údajů jsou zásady stanovené na mezinárodních platformách v roce 1980, kdy digitální přítomnost výrobků a služeb v životě spotřebitelů byla minimální. Přítomnost propojených digitálních zařízení v domácnostech a v každodenním životě spotřebitelů postupně narůstala, až dospěla k současnému stadiu, kdy lze digitální technologie bez přehánění považovat za všudypřítomné. Rozšířenost digitálních technologií neustále roste a lze předpokládat, že s příchodem inteligentních měst a internetu věcí bude dále významně narůstat.

Evropská legislativa i technická normalizace na tento vývoj logicky reagovaly a již v polovině 90. let byla vytvořena příslušná regulace. Nová Evropská komise si dala jako jednu z hlavních svých priorit úkol reformy ochrany soukromí v digitálním světě. Je to výzva i pro technickou normalizaci a její zapojení do tohoto procesu.

Cílem této publikace je přiblížit, jak ve vztahu k ochraně svého soukromí v digitálním světě vnímají své priority spotřebitelé. Publikace proto může sloužit i jako pomůcka pro zástupce spotřebitelů zapojených do normalizačních činností a podpořit tak rozvoj ochrany soukromí již od návrhu technické normy či předpisu. Navíc může být východiskem pro správnou praxi v oblasti ochrany soukromí na digitálním trhu, tedy s využitím pro výrobce a hlavně poskytovatele služeb. Tato publikace se v principu soustřeďuje na ochranu soukromí spotřebitele v domácím prostředí, jak bude dále blíže vysvětleno. Soukromí spotřebitele je nejlépe zabezpečeno, pokud je tento aspekt zohledněn již od samého počátku navrhování provedení výrobků a služeb.

1.2. Prostředí soukromí spotřebitelů

Co lze očekávat od spotřebitele?

Je třeba podotknout, že spotřebitelé jsou laici a vždy tomu tak vesměs bude. Spotřebitelé používají v každodenním životě více než 700 výrobků a služeb a protože musí vést normální život, nemají ani čas ani odborné znalosti ke zvládnutí technických detailů u všech těchto výrobků a služeb.

Pokud jde o inteligentní zařízení, musíme mít na paměti, že dochází k situacím, kdy spotřebitelé nepochopí správně všechny informace, dopouštějí se chyb, zapomínají informace a přijímají opatření, která jim připadají evidentní a která mohou, ale nemusí nutně spadat k opatřením předpokládaným v rámci provedení výrobku nebo služby.

Soukromí spotřebitelů je v reálném anebo virtuálním **domácím prostředí.** Příklady reálného prostředí jsou dům a domácnost, zahrada, auto, vnější prostředí a veřejné prostředí jako například ulice, nákupní střediska nebo tržiště a veřejné budovy. Příkladem virtuálního prostředí je přímý přístup k internetu, internetové nakupování, internetové bankovnictví, hry pro více hráčů (multiplayer games), osobní elektronická pošta, „virtuální místa setkání" a sociálně sdílené oblasti jako Facebook či blogy.

Praktické aspekty ochrany soukromí v domácím prostředí je třeba zaměřit na digitálně propojená zařízení spotřebitelů, jejichž prostřednictvím jsou generovány, shromažďovány a předávány ostatním údaje o domácím životě.

Ochrana soukromí spotřebitelů **mimo domácí prostředí** zahrnuje oblasti, ve kterých ostatní subjekty, jako jsou např. obchodníci, státní a veřejná správa nebo organizace poskytující na dobrovolné bázi neziskové služby, shromažďují od jednotlivců osobní údaje a poté je zpracovávají pro řadu různých účelů.

Tato publikace se prioritně soustřeďuje na ochranu soukromí spotřebitele v domácím prostředí.

1.3. Vymezení pojmu osobní údaje

Význam a obsah pojmu osobní údaje není dosud jednoznačně ustálen, zejména v praktických interpretacích pak dochází k neshodám.

Podle našeho národního právního předpisu[1] je *osobním údajem jakákoli informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.* Definice je ve shodě s evropskou legislativou, která pochází již z roku 1995[2].

Mezinárodní organizace pro normalizaci (ISO) přispěla s cílem napomoci při řešení této otázky vhodnou definicí osobních údajů[3]. *Osobně identifikovatelné informace (PII- personally identifiable information) jsou jakékoliv informace, které (a) mohou být použity k identifikaci subjektu PII, kterého se tato informace týká, nebo (b) mohou být přímo nebo nepřímo spojené se subjektem PII.* (Subjekt PII je definován takto: *fyzická osoba, které se osobně identifikovatelné informace (PII) týkají.*)

Digitálně propojená zařízení zpracovávají nebo shromažďují celou řadu údajů od jednotlivců, které mohou poté být využity pro osobní zpracování, nebo mohou být jinými osobami shromažďovány k jiným účelům.

Výchozím bodem k pochopení úplného rozsahu údajů představujících osobně identifikovatelné informace (PII) jsou jednotlivé typy osobních informací, které byly identifikovány v evropské normě[4], podle které mezi hlavní typy osobních údajů patří:

- osobní identifikátory – např. údaje o totožnosti (jméno, adresa), údaje potvrzující totožnost (rodné číslo), charakteristické identifikační údaje (věk, krevní skupina) či referenční údaje pro účely služeb (číslo účtu, číslo pasu).
- osobní behaviorální údaje – např. dlouhodobé chování (sexuální orientace, náboženské vyznání, členství v organizacích, politické názory), využití údajů o domácích službách (účty za inteligentní služby, výpisy z bankovních účtů, použití kreditní

[1] Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, v platném znění.

[2] Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně jednotlivců v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

[3] ČSN ISO/IEC 29100:2015 Informační technologie – Bezpečnostní techniky – Rámec soukromí

[4] ČSN EN 16571:2014 Informační technologie – Postup posouzení ochrany osobních údajů v RFID.

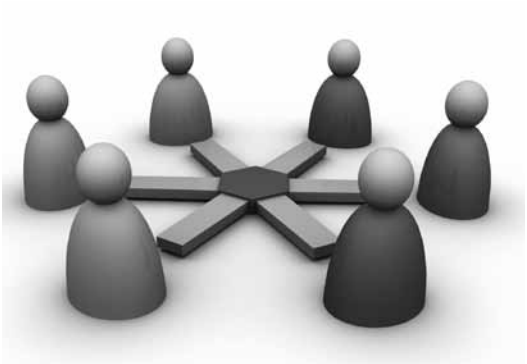
a debetní karty), údaje o odborných službách (zdravotní záznamy, záznamy o platu a mzdě) nebo údaje o komunikaci (navštívené internetové stránky, volaná telefonní čísla) atd.,
- identifikátory technologie a hardware,
- identifikátory identity věcí,
- zbytková hodnota rizika,
- časové údaje/údaje o poloze,
- údaje z čidel.

Mezi osobní identifikátory náleží údaje o totožnosti (jméno, adresa), údaje potvrzující totožnost (rodné číslo), charakteristické identifikační údaje (věk, krevní skupina) či referenční údaje pro účely služeb (číslo účtu, číslo pasu). Příkladem osobních behaviorálních údajů jsou dlouhodobé chování (sexuální orientace, náboženské vyznání, členství v organizacích, politické názory), využití údajů o domácích službách (účty za inteligentní služby, výpisy z bankovních účtů, použití kreditní a debetní karty), údaje o odborných službách (zdravotní záznamy, záznamy o platu a mzdě) nebo údaje o komunikaci (navštívené internetové stránky, volaná telefonní čísla) atd.

1.4. Sítě využívané digitálními zařízeními a účel zpracování údajů

Domácí prostředí pro zpracování údajů je technicky složité a obvykle je tvořeno propojenými digitálními zařízeními připojenými jak na domácí sítě, tak na veřejné sítě.

Všechna digitálně propojená zařízení provádějí určitou formu interního zpracování a právě návrh softwaru použitého k zajištění nebo doplnění funkcí takového zařízení určuje, kde zpracování probíhá. Je docela možné, aby jednoduše vyhlížející domácí aplikace využívaly software spuštěný na domácím zařízení propojeném přes veřejnou síť, tudíž částečně předávaný v rámci infrastruktury informačních a komunikačních technologií organizace s tím, že samotné zpracování je částečně zajišťováno službami „cloud“[5] nebo podobnými službami. Jednoduše řečeno z pohledu spotřebitele, tj. z pohledu bez odborných znalostí, by mohlo domácí zpracování údajů probíhat kdekoliv.



V domácím prostředí využívají spotřebitelé zařízení, která pracují za použití digitálního zpracování údajů vedoucího k vytvoření osobních digitálních údajů. Tato zařízení využívají spotřebitelé ze dvou hlavních důvodů, a to:

a) věnovat se něčemu, co je součástí jejich domácího života (například používání fitness aplikací na chytrém telefonu, zpracování rodinného rozpočtu v internetových tabulkových procesorech, sdílení fotografií s rodinou a přáteli);
b) komunikace s organizací za účelem získání zboží a služeb, a to od poskytovatelů jak z veřejného, tak soukromého sektoru (např. nákup v internetovém obchodě, data o občanech shromážděná obecním úřadem /například sociálního odboru/, daňové informace finančního úřadu).

Někdy může být důvodem pro konkrétní způsob zpracování údajů kombinace výše uvedeného.

V případě a) určuje účel zpracování spotřebitel, zatímco v případě b) tento účel stanovuje organizace. Právní předpisy a normy na ochranu soukromí určují, kdo je považován v daném případě za „správce“ zpracování.

1.5. Principy ochrany soukromí

Zásady ochrany údajů se vztahují k ochraně soukromí jednotlivců. Pokud jde o údaje, které jsou o spotřebitelích shromažďovány organizacemi, ochrana soukromí se zaměřuje na domácnost a domácí prostředí a na přesné stanovení vlastností technologií digitálně propojených zařízení. To bylo podnětem k formulaci sedmi principů ochrany digitálních zařízení, jež by měly být východiskem pro správné praxe, pro technické normy a konečně pro regulaci.[6]

1. ZABEZPEČENÍ DOMÁCÍCH DIGITÁLNÍCH ZAŘÍZENÍ
   Zabezpečení domácích digitálních zařízení je pro ochranu domácího soukromí nezbytné a zásadní.
2. KONTROLA SPOTŘEBITELŮ NAD VLASTNÍM SOUKROMÍM
   Spotřebitelé by měli mít v rámci domácího prostředí úplnou kontrolu nad svým soukromím.
3. KONTROLA NAD SOCIÁLNĚ SDÍLENÝMI INFORMACEMI
   Pokud jsou shromažďovány údaje od spotřebitelů, je pak třeba kontrolu přizpůsobit osobním potřebám spotřebitelů tak, aby mohli kdykoliv vyjádřit, co má v rámci ochrany jejich osobního soukromí přednost, a kdykoliv tyto preference změnit.
4. SOUKROMÍ A OBTĚŽUJÍCÍ OBSAH
   Z pohledu spotřebitele obsahují obtěžující obsah nevyžádaná pošta (SPAM), vyskakovací reklamy při připojení na internet, porno, online šikana, obtěžující telefonické volání a další. Je třeba vytvářet nástroje k jejich zamezování.
5. KONTROLA SOUKROMÍ V PŘÍPADĚ SHROMAŽĎOVÁNÍ ÚDAJŮ
   Jsou-li osobní údaje předávány ostatním, je třeba zajistit transparentnost sdílení údajů. Procesy analýzy osobních údajů by měly být navrženy způsobem umožňujícím ochranu soukromí jednotlivců.
6. SOUKROMÍ NA VEŘEJNÝCH MÍSTECH
   Anonymita na veřejných doménách by měla být nezbytným pravidlem.
7. PRINCIP ODPOVĚDNOSTI ZA PROHLÁŠENÍ A STANOVISKA ZVEŘEJNĚNÁ NA INTERNETU
   I přes právo na svobodu projevu by jednotlivci měli nést odpovědnost za prohlášení a názory prezentované ve veřejných digitálních prostředích.

Podrobně jsou tyto principy vysvětleny a komentovány v dalších kapitolách (2–8) této publikace. Kapitola 9 pak naznačuje principy posouzení dopadů na soukromí.

[5] Cloud computing je na internetu založený model vývoje a používání počítačových technologií. Lze ho charakterizovat jako poskytování služeb či programů uložených na serverech na internetu s tím, že uživatelé k nim mohou přistupovat například pomocí webového prohlížeče nebo klienta dané aplikace a používat je prakticky odkudkoliv. Uživatelé neplatí (za předpokladu, že je služba placená) za vlastní software, ale za jeho užití. Nabídka aplikací se pohybuje od kancelářských aplikací přes systémy pro distribuované výpočty až operační systémy provozované v prohlížečích, jako jsou například eyeOS, Cloud či iCloud. (Wikipedie)

[6] Autorem zásad/principů je ANEC, který je publikoval v r. 2015 v pokynu ANEC-ICT-2015-G-064, viz přehled informačních zdrojů v závěru publikace.

2. ZABEZPEČENÍ DOMÁCÍCH DIGITÁLNÍCH ZAŘÍZENÍ

2.1. Úvod

Dobré zabezpečení znemožňuje neoprávněným osobám přístup k osobním informacím. V případě digitálně propojených zařízení využívaných spotřebiteli tato zásada ovlivňuje:

a) zabezpečení platforem pro zpracování údajů využívaných spotřebiteli, jako jsou chytré telefony a tablety a také domácí sítě;
b) zachování zabezpečení platforem pro zpracování údajů o spotřebitelích s ohledem na neustálé kybernetické útoky;
c) roli spotřebitelů při zachování vlastní bezpečnosti a jejich podíl na systémovém zabezpečení veřejných sítí a soukromých organizací. *Například jak se vyvarovat stažení škodlivého softwaru (malware) a jeho dalšímu rozšíření a také jak odstranit škodlivý software zabudovaný v domácí infrastruktuře informačních a komunikačních technologií;*
d) běžné nastavení zabezpečení digitálních zařízení a součástí sítě v domácnosti, což vyžaduje dosažení rovnováhy mezi snadným používáním a ochranou přístupu k údajům.

2.2. Nejnaléhavější otázky v oblasti zabezpečení

Každá organizace by měla mít zájem na nalezení správné rovnováhy mezi důvěrou, transparentností a soukromím (CISCO, 2014). Přitom tři faktory – větší prostor pro útoky, nárůst a propracovanost typů útoků a složitost hrozeb a řešení – stále více komplikují snahy pracovníků provádějících zabezpečení dosažení výše uvedené rovnováhy.

Organizace uvádějí jako hlavní problém zejména „napadení" webových stránek a vnitřních procesů anebo infrastruktury internetových serverů.

Ze strany jednotlivců jsou hlavními problémy nevyžádané e-maily (SPAM), stahování škodlivého softwaru (malware) a obecně nedostatečná ochrana mobilních telefonů a tabletů pro osobní použití.

Aktuálně se otázkami zabezpečení, které se dají přiřadit k opatřením ve vztahu k organizacím, zabývají bezpečnostní normy ISO/IEC z řady ISO/IEC 27000[7]. Je však třeba výrazně intenzivnější normalizační činnosti v oblastech, kde je snaha o odstranění slabých stránek zabezpečení ve vztahu k jednotlivcům. Jedná se zejména o případy, kdy jednotlivci jsou právě spotřebitelé.

Životy spotřebitelů jsou již značně propojeny prostřednictvím digitálních zařízení a brzy se v našich životech objeví i internet věcí[8]. Použití chytrých telefonů s přibližně dvěma biliony chytrých telefonů v provozu v globálním měřítku již dospělo. Chytré telefony a tablety jsou pravděpodobně nejdůležitějšími, nikoliv však jedinými zařízeními používanými pro aplikace shromažďující údaje z čidel, poskytujícími spotřebitelům užitečný rozsah funkcí a kontrolu v domácím prostředí, což snižuje množství hrozeb pro jejich soukromí. Je nezbytně nutné mít k dispozici stabilní a účinný proces aktualizace softwaru operačního systému chytrého telefonu, který odhalí zranitelná místa před tím, než tak učiní někdo se špatnými úmysly; proces, který podchytí zranitelná místa, a pak spustí aktualizaci výsledného softwaru u všech postižených majitelů chytrých telefonů před tím, než je slabé místo široce zneužito. Nicméně v současnosti představuje pro majitele chytrých telefonů největší bezpečnostní riziko hrozba ztráty nebo krádeže tohoto zařízení.

Svět digitálních aplikací nabízí spotřebitelům důležité funkcionality v následujících oblastech:

- domácí péče,
- bezpečnost dětí,
- nákupy přes internet,
- kontrola domácího prostředí,
- domácí inteligentní spotřebiče ad.

Úložiště mobilních aplikací jsou důležitou součástí ekosystému chytrého telefonu a jsou hlavním distribučním bodem pro mobilní aplikace. Spotřebitelé ovšem nepřebírají osobní odpovědnost za zabezpečení svých chytrých telefonů a spoléhají se na to, že sami operátoři mobilních sítí budou vyvíjet iniciativu, pokud jde o zabezpečení zařízení a zajištění bezpečného přenosu informací prostřednictvím rádiových sítí.

Jaká jsou tedy hlavní rizika a prostředky k jejich eliminaci?

2.3. Aktuálnost ochrany spotřebitelů

S ohledem na neustálé kybernetické útoky a ohrožení zabezpečení digitálně propojených zařízení je třeba zajistit, aby byl každý prvek zařízení a sítí, ke kterým jsou tato zařízení připojena, navržen způsobem umožňujícím aktualizovat bezpečnostní software. Toho mělo být dosaženo s využitím již zmíněné řady norem ISO/IEC 27000 s podporou sledování bezpečnosti a prováděním opatření přizpůsobených spotřebitelům.

Schopnost aktualizace bezpečnostního softwaru a procesy s tím související by měly být pro uživatele (spotřebitele) snadno pochopitelné a měly by zahrnovat následující aspekty:

- bezpečnostní poplašné signály;
- automatická aktualizace softwaru, pokud možno bez přerušení provozu zařízení;
- informace poskytované spotřebitelům by měly v případě, že je vyžadován ze strany spotřebitele zásah, určovat jednotlivá zranitelná místa a rizika útoku, aby byl spotřebitel všude, kde je to možné, k provedení zásahu motivován;
- důvěryhodnost a verifikace zdrojů aktualizace zabezpečení jsou naprosto nezbytné;
- zabezpečení by nemělo být provedeno způsobem, který by omezoval možnost volby spotřebitele, pokud jde o další výrobky a služby;
- bezpečnostní opatření by měla zahrnovat možnost stažení výrobku v případě, že by otázky související se zabezpečením, například bezpečnost výrobku, vyvolaly bezpečnostní rizika vyplývající z hardwaru a možnosti zneužití, které jsou závažné a je nemožné je podchytit při aktualizaci softwaru;
- žádný negativní dopad na spotřebitele, pokud jde o výkonnost nebo funkčnost – například by nemělo být nezbytné, aby uživatel musel přeprogramovat regulátor centrálního vytápění v souladu s harmonogramem vytápění proto, že při aktualizaci zabezpečení bylo smazáno původní nastavení.

[7] Např. ČSN ISO/IEC 270002014 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník.

[8] Internet věcí (anglicky Internet of Things, zkratka IoT) je v informatice označení pro propojení vestavěných zařízení s internetem. Propojení zařízení by mělo být zejména bezdrátové a mělo by přinést nové možnosti vzájemné interakce nejen mezi jednotlivými systémy, ale též přinést nové možnosti jejich ovládání, sledování a zajištění pokročilých služeb. Problémem ovšem jsou různé existující standardy pro komunikaci různých skupin výrobců. (Wikipedia)

2.4. Důvěryhodnost programů a aplikací

Software, který si mohou spotřebitelé koupit nebo který mohou používat na svých digitálních zařízeních, by měl pocházet od ověřených dodavatelů a software i jeho zdroje by měly podléhat přísné bezpečnostní kontrole a hodnocení bezpečnosti.
Digitální zařízení používané spotřebiteli by mělo automaticky kontrolovat, zda jakýkoliv stahovaný software pochází ze spolehlivých a důvěryhodných zdrojů.

2.5. Ztráta mobilních digitálních zařízení

Zařízení používaná spotřebiteli, u kterých se dá oprávněně očekávat, že budou mobilní nebo přenosná, by měla pokud možno obsahovat prvky zabezpečení, které zajistí, že lze:

- zařízení v případě ztráty zablokovat;
- ochránit základní údaje o spotřebiteli obsažené v zařízení;
- zařízení lokalizovat a získat je tak zpět.

2.6. Bezpečnost a informovanost během celého životního cyklu výrobku

Bezpečnostní provedení a procesy aktualizace by měly zajistit, že zabezpečení zařízení používaného spotřebitelem zůstane zachováno po celou dobu životního cyklu výrobku, tj. od ověření provedení prvními uživateli po dobu plného provozu, aktivního používání až po stažení výrobku od uživatele k likvidaci.
V rámci neustálé kontroly zabezpečení a ochrany soukromí by měli být spotřebitelé informováni:

- o zbytkových bezpečnostních rizicích (a rizicích ve vztahu k soukromí) a o stupni závažnosti takových rizik;
- o jakýchkoliv opatřeních ke zmírnění rizik, která může spotřebitel podle svého uvážení přijmout, aniž by mu tím vznikly jakékoliv náklady.

Všude, kde je to možné, by posouzení rizik mělo zohledňovat konkrétní problémy spotřebitele a jako takové být prezentováno.
Detailní technické informace by s ohledem na zabezpečení měly zůstat snadno pochopitelné a opatření k vyřešení potíží snadno proveditelná.

3. KONTROLA SPOTŘEBITELŮ NAD VLASTNÍM SOUKROMÍM

3.1. Úvod

Spotřebitelé by měli mít v domácím prostředí nad svým soukromím úplnou kontrolu.
Propojení zařízení a sítí využívaných k poskytování programů a aplikací, které jsou využívány spotřebiteli v jejich osobních životech, by mělo zajistit, že každý jednotlivec využívající program nebo aplikaci může v reálném čase kontrolovat, kdo na sociálních sítích a v rodině má přístup k osobním údajům z programu nebo aplikace, které se k němu vztahují.
Existující evropská právní úprava[9] je považována za zastaralou – vždyť pochází z r. 1995 – a prochází zásadní reformou. V tomto rychle se měnícím prostředí si musí jednotlivci zachovat účinnou kontrolu nad svými osobními údaji. Podle Evropské unie se jedná o základní právo každého jednotlivce v EU a musí být zajištěno.
Právo na ochranu osobních údajů by nemělo být narušováno nebo oslabováno jenom z toho důvodu, že je snadnější nebo výnosnější jej v digitálním prostředí porušit.
Sdružení dvaadvaceti skupin zabývajících se v USA ochranou soukromí navrhlo šest požadavků do zprávy Bílého domu týkající se dat o velkém objemu a budoucnosti soukromí *(White house's report on Big Data and the Future of Privacy)*. Jednou ze šesti prioritních oblastí byla kontrola spotřebitelů nad svými údaji: „Jednotlivci by měli mít možnost kontrolovat údaje, které vytvářejí nebo která se jich týkají, a rozhodovat, zda tyto údaje budou shromažďovány a pokud ano, jakým způsobem budou využívány."

3.2. Princip kontroly spotřebitelů nad vlastním soukromím

V domácím prostředí by mělo být zpracování údajů (k usnadnění průběhu a organizace jejich života a zapojení do společenského života) prováděné jednotlivci zabezpečeno a jednotlivci by nad ním měli mít kontrolu všude, kde je zpracování prováděno v rámci globální architektury informačních a komunikačních technologií, například fitness aplikace, kontrola nad domácím prostředím (řízení teploty v bytě pomocí mobilního telefonu aj.), plánování cest atd.
Tento princip se dotýká například následujících aplikací:

- domácí sítě a propojená zařízení;
- služby „cloud computing" pro spotřebitele a využití „cloud computing" aplikacemi;
- internet věcí, inteligentní přístroje včetně inteligentních automobilů;
- rodičovský dohled a kontrola;
- kontrola nad sociálně sdílenými údaji;
- kontrola nad rušivým obsahem včetně nevyžádaných e-mailů (SPAM), porna, online šikany.

Existují tři hlavní kroky, které by měly společnosti podniknout za účelem zvýšení soukromí a bezpečnosti spotřebitelů a vybudování důvěry spotřebitelů k zařízením internetu věcí:

1) převzít přístup „bezpečnost již od návrhu";
2) zabývat se minimalizací údajů ke zpracování;
3) zvýšit transparentnost a v případě neočekávaného použití údajů spotřebitele upozornit a poskytnout jim možnost volby.

3.3. Priority ochrany soukromí a požadavky na kontrolu

Kontrola priorit ochrany soukromí poskytovaná digitálně propojenými zařízeními by měla zahrnovat možnost spotřebitele provádět kontrolu nad níže uvedeným v reálném čase:

- Jaké položky s osobními údaji mohou být zpřístupněny ostatním?

[9] Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně jednotlivců v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

- Kdo může mít přístup k osobním údajům a koho se tyto osobní údaje budou týkat?
- Kdy mohou být osobní údaje zpřístupněny?
- Kde mohou být osobní údaje zpřístupněny?
- Jakým způsobem mohou být osobní údaje zpřístupněny?
- Z jakého důvodu mohou být osobní údaje zpřístupněny?

Detaily zajištění takové kontroly soukromí zařízeními se budou odvíjet od rozhodnutí ohledně detailního umístění v rámci domácích prvků sítě a hardwaru, operačních systémů a souvisejících softwarových aplikací. Vzhledem k tomu, že většina sítí v domácnostech a domácím prostředí zahrnuje vybavení od řady různých dodavatelů a v případě aplikačních softwarů od mnoha různých firem, bude zřejmě nezbytné z praktických důvodů zpracovat pro požadavky na zajištění vysoké úrovně kontroly priorit ochrany soukromí normy pro interoperabilitu.

Kromě toho, jak už bylo zmíněno dříve, detailní návrh provedení určuje, kde přesně probíhá domácí zpracování údajů, a to obvykle způsobem, který si spotřebitel neuvědomuje. V takových případech by měla být kontrola v reálném čase rozšířena na celou infrastrukturu informačních a komunikačních technologií zapojených do zpracování osobních údajů bez ohledu na to, kde zpracování probíhá.

„Cloud computing" je jedním z hlavních příkladů rozděleného zpracování údajů zmíněného již dříve. V takových případech je „cloud computing" využíván k dokončení zpracování údajů vyžadovaného pro využití programů nebo aplikací spotřebiteli pro domácí činnosti.

Vzhledem k tomu, že stovky tisíc aplikací jsou spotřebitelům poskytovány třetími stranami bez přímého smluvního vztahu mezi spotřebitelem a poskytovateli „cloud" služeb, je nezbytné posílit pravidla, která zajistí, že prvky kontroly ochrany soukromí pro domácí použití digitálních zařízení budou rozšířeny na průběh zpracování prováděného v rámci „cloud".

Šíření **internetu věcí, inteligentních přístrojů** v domácím prostředí a rozšiřování tohoto domácího prostředí i v rámci inteligentních automobilů apod. má před sebou mnoho možností.

Zmíníme zde dva aspekty takovýchto rozvíjejících se trhů, a to:

- použití dálkového ovládání zařízení v domácnosti a domácím prostředí za účelem „vydání příkazu" objektům k vykonání určitých činností;
- starost průmyslu nad tím, že obavy o soukromí spotřebitelů zpomalí možné tempo inovací.

Zabezpečený přístup k zařízením na **dálkové ovládání** by měl podléhat kontrole spotřebitele v reálném čase tak, aby byl přístup k dálkovému ovládání umožněn pouze těm, kterým k tomu spotřebitel dal souhlas. V sociálním kontextu by příkladem mohlo být udělení souhlasu se sledováním domu a vypnutím falešných poplachů přátelům v době, kdy je spotřebitel na dovolené. Pokud výrobek nebo služba umožňují samy o sobě jiným osobám dálkové ovládání, měl by pak spotřebitel mít v reálném čase úplnou kontrolu nad jakýmikoliv kontrolními příkazy vydanými těmito osobami zařízením spotřebitele. Příkladem z komerční oblasti mohou být příkazy inteligentních sítí k vypnutí zařízení v domácnosti za účelem hospodaření s energií, kdy by hlavní kontrolu nad tím, která zařízení budou vypnuta, měl mít spotřebitel, a ne společnost dodávající elektrickou energii.

3.4. Sdílená ochrana soukromí

Existuje několik zásadních situací týkajících se spotřebitele, kdy by mohla být **do kontroly ochrany soukromí zapojena odpovědná třetí strana.** Příkladem jsou rodiče nebo opatrovníci dětí a ti, jejichž odpovědností je dohled nad osobami, které případně nemají nebo ztratily schopnost se v této oblasti rozhodovat. Zejména je třeba zdůraznit nutnost možností technické sdílené kontroly s cílem umožnit sdílení kontroly ochrany soukromí mezi osobami, o jejichž soukromí se jedná (subjekt PII) a těmi, které byly uznány jako oprávněné k jejich výchově nebo péči o ně.

Související rizika a nebezpečí online připojení:

- nevhodný obsah, včetně pornografie,
- nerespektování věkového omezení,
- přátelství a komunikace s neznámými osobami,
- grooming a sexuální zneužívání,
- sdílení osobních informací,
- gambling nebo zadlužení.

Co se týče vlastního přístupu, odborné organizace doporučují těsnou a pravidelnou komunikaci s dětmi o uvedených rizicích.

Pro tuto citlivou oblast je nutné mít k dispozici normalizovaná pravidla a zajistit, že procesy spojené s poskytováním možnosti sdílet kontrolu nad ochranou soukromí prostřednictvím digitálně propojených zařízení jsou řízeny správným způsobem. Takové požadavky by měly zahrnovat následující:

- Osoby, k nimž se údaje vztahují, by měly poskytnout souhlas někomu jinému, kdo má kontrolu nad jejich soukromím a shromažďováním údajů. Rodiči nebo třetí straně, na které byla převedena zevrubná kontrola, by měla být poskytnuta stejná úroveň ochrany soukromí, jaká je obvykle poskytována spotřebitelům.
- Osoba, k níž se údaje vztahují, by měla mít možnost odvolat souhlas se sdílenou kontrolou soukromí.
- Vzhledem k tomu, že schopnost lidí rozhodovat v čase se mění, mělo by řízení celého procesu sdílené kontroly nad soukromím umožňovat této osobě (subjekt PII) učinit rozhodnutí na stávající úrovni. Například malé děti vyrostou a přeberou více odpovědnosti za své vlastní životy, zatímco starší osoby se během času mohou stát méně způsobilými.
- Rodiče by měly mít možnost prostřednictvím technického zařízení sledovat, jakým způsobem jejich děti využívají aplikace a online služby, a to ne pouze na základě celkové dohody a souhlasu dítěte, ale s přihlédnutím k jeho vývoji a rozumovým schopnostem.

4. KONTROLA NAD SOCIÁLNĚ SDÍLENÝMI INFORMACEMI

4.1. Úvod

Je užitečné si vyjasnit, že v rámci sdílení je spotřebitelům přiřazeno několik odlišných rolí. Jsou to:

- poskytovatelé sdílených informací;
- příjemci sdílených informací;
- ostatní osoby, které nejsou ani poskytovateli informací ani jejich příjemci, ale jejichž osobní údaje sdílené informace obsahují.

Uvádí se dvě hlavní oblasti, které v případě sociálního sdílení informací vzbuzují obavy:

a) „Příliš mnoho uživatelů se domnívá, že to, co uvádějí na internetu, je soukromé, a to mezi nimi a příjemcem. Realitou však je, že jakmile je prohlášení napsáno, může být zkopírováno, uloženo a předáno. Kromě toho uživatel už dále není vlastníkem informací umístěných na sociální sítě…" *(Obavy a Obama – 2009)*.

b) „Trendem je vzájemné nakukování do soukromí a anonymity ostatních prostřednictvím videa a multimediálních záznamů způsoby, které poškozují ty, kterých se tyto digitální záznamy týkají. Neexistují žádná pravidla nebo předpisy na ochranu jednotlivců před náhodně pořízenými fotografiemi nebo videi jejich osoby a před jejich umístěním na web ke zhlédnutí ostatními. Zatímco autorské právo se ukázalo jako nesmírně účinné při ochraně vlastnických práv online, těm, kteří usilují o ochranu vlastního soukromí, je poskytována malá pomoc." *(Lipton – 2009:4)*

Toto jsou i mementa pro změnu chování spotřebitelů. Napomoci ale musí i normy a regulace.

4.2. Požadavky na sdílení údajů

Za současného stavu věcí (v kontextu písmene a) výše) obvykle sdílené systémy nekontrolují, kdo může sdílené informace přijmout, a tak mohou být přijaté sdílené informace zpřístupněny (v rámci sociálních sítí) nebo předány (v rámci systémů elektronické pošty) ostatním, se kterými původce informací rozhodně nehodlá tyto informace sdílet.

S cílem vyřešit takovou nedostatečnou kontrolu ze strany spotřebitele jako poskytovatele osobních informací (subjekt PII) nad sdílenými informacemi, by měly normy zahrnovat schopnost systémů umožnit osobní kontrolu nad tím, kdo a jaké informace sdílí, kdy a jakým způsobem je sdílí.

V závislosti na stupni kontroly individuálních přání jednotlivce takovou kontrolu provádět se může jednat o:

- distribuční seznamy pro elektronickou poštu a sociální sítě, které omezují distribuci pouze na ty, kteří jsou stanoveni subjektem PII, tj. odstranění možnosti předávání informací nebo dalších sdílení zařízení;
- kontroly poskytovatelů informací, které neumožní kopírování jejich informací v okamžiku, kdy jsou sdíleny;
- oznámení poskytovateli o tom, kdo další může nahlížet nebo mít přístup ke sdíleným informacím předávaným ostatním;
- možnost pro ty, kdo přijímají sdílené informace, požádat poskytovatele subjektu PII o povolení k dalšímu sdílení informací nad stávající omezení;
- subjekt PII by měl mít možnost udělit povolení pro širší sdílení, než vyplývá z počátečních omezení pro sdílení;
- subjekt PII nebo odpovědná třetí strana by měly mít možnost odvolat nebo omezit prvotní povolení s přístupem k dříve odstraněným sdíleným informacím pro ty, kteří byli vyloučeni změnou povolení, a to s cílem vypořádat se, zejména v případě dětí, s „nadsdílením" (oversharing).

4.3. Požadavky na příjemce sdílených osobních informací

Pokud sdílené informace od jednoho jedince obsahují osobní informace týkající se ostatních (v kontextu písmene b) výše), měly by normy zahrnovat schopnost systému umožnit:

- jednotlivci, kterého se osobní informace týkají, zaslat původnímu subjektu PII sdílejícímu údaje, upozornění, aby odstranil, skryl nebo omezil dostupnost takového obsahu;
- nastavení různé úrovně procesů pro případ, že by požadavky nebyly odeslány od subjektů sdílejících informace, zatímco ti, kteří požádali o určité omezení viditelnosti informací, které se jich týkají, si mohou vyžádat u poskytovatele služby opatření k odstranění, skrytí nebo omezení dostupnosti informací, které obsahují jejich osobně identifikovatelné informace (PII);
- řádnou správu procesů s cílem zajistit, že taková opatření k odstranění, skrytí či omezení dostupnosti souvisejících osobně identifikovatelných informací (PII) jednotlivce budou provedeny pouze na základě jasně pochopitelných a transparentních kritérií.

4.4. Identifikace jednotlivce

Otázka identifikace jednotlivce na základě údajů sdílených jinými osobami (rovněž v kontextu písmene b) výše) se týká digitálních obrázků, videí a multimediálního obsahu zahrnujících informace o jednotlivcích, kteří byli digitálně zaznamenáni ostatními; osoby, které záznam pořídily, pak tento obsah dále sdílejí.

Každý spotřebitel, který získal takové záznamy, by měl být instruován, jak postupovat, pokud jde o požadavky od „zachycených" jednotlivců na odstranění nebo zakrytí těchto záznamů v rámci sdílených údajů.

Bylo by vhodné zpracovat instrukce pro spotřebitele, kteří získali takové záznamy, jak se zachovat, pokud jde o ochranu soukromí „zachycených" jednotlivců v rámci sdílených údajů (např. odstranit nebo zakrýt části záznamů).

K tomu, aby byla nalezena technologická řešení pro osoby, které pořizují snímky jiných osob, když to není žádoucí, by bylo zapotřebí vyvinout v oblasti vývoje těchto zařízení mnohem více úsilí, než jak je tomu v současné době. Jako příklad pro ilustraci technických přístupů, které by mohly být zohledněny, lze uvést následující:

- Mobilní telefony by mohly být vybaveny schopností zachytit jiné mobilní telefony

v blízkém okolí a osobní nastavení jejich majitelů za účelem sledování, a pak by kamera, je-li namířena tím směrem, pořídila záznam.
- Drony a jejich kontrolní aplikace by mohly být vybaveny údaji z map znázorňujících obydlené oblasti, které by mohly být spojeny s GPS na palubě a směrovými čidly k vypnutí kamery v případě přeletu nad obytnými budovami.

Takovéto „myšlenkové experimentování" představuje významné zvýšení současných možností ve fázi návrhu a vyžadovalo by zpracování nové sady norem, aby mohly být takové možnosti běžně využívány.

5. SOUKROMÍ A OBTĚŽUJÍCÍ OBSAH

5.1. Úvod

Z pohledu spotřebitele obsahují obtěžující obsah nevyžádaná pošta (SPAM), vyskakovací reklamy při připojení na internet, porno, online šikana (viz také část 8), obtěžující telefonické volání a další. K takovému obtěžování může docházet prostřednictvím přímé komunikace s jednotlivcem, ale také s využitím dalších mechanismů, jako jsou například sociální média. Mnoho z typů obtěžujícího obsahu zastihne spotřebitele skrytým způsobem (nebo přinejmenším to není zcela očividné).

V případě mnoha typů obtěžujícího obsahu mohou pouze ti, kteří jsou na konci řetězce, identifikovat, zda se jedná o nežádoucí a tedy obtěžující obsah.

5.2. Požadavky na soukromí v případě obtěžujícího obsahu

Tvorba norem by se proto měla zaměřovat v obecné rovině na technické prostředky, které zabrání, aby obtěžující obsah dostihl spotřebitele, a umožní, aby soukromí jednotlivého spotřebitele bylo chráněno.

Například aplikace vyhledávající a odstraňující stránky s porno obsahem z globálních vyhledávačů, které jako porno stránky nevypadají, dokud se na ně nevstoupí, anebo zamezení šíření nežádoucích vyskakovacích reklam a dalších reklamních obsahů, které snižují význam a hodnotu informací vyhledávaných uživatelem.

Soukromí je dále třeba podporovat normami, které mohou stanovit pravidla a postupy, jak uvědomit poskytovatele služeb o tom, že konkrétní přijaté sdělení bylo obtěžující nebo nežádoucí.

- Takovéto oznámení by mělo být v maximální možné míře automatizované prostřednictvím digitálního procesu podporovaného digitálně propojenými zařízeními, která přijímají obtěžující obsah.
- Pokud existuje taková možnost, pak by takové údaje měly být automaticky předávány poskytovateli služeb včetně zprávy o narušení.
  Poznámka: V ideálním případě je původcem obsahu příslušný poskytovatel služby. V případě, že jde o zprostředkujícího poskytovatele digitální služby, jako je například poskytovatel internetových služeb nebo stránek sociálních médií, kdy jsou identita a umístění původce skryté, je potřeba další průzkum.

Technické normy by měly dále řešit a upravovat:

- zablokování doručení dalšího obtěžujícího obsahu jednotlivci od poskytovatele služeb, jakmile je zdroj tohoto obsahu identifikován. Příkladem jsou seznamy pornografických stránek interně využívané poskytovateli internetových služeb, které jsou poskytovatelem aktivovány jako filtr v rámci rodičovské kontroly;
- zablokování nebo odklonění obtěžujícího obsahu identifikovaného jednotlivcem na digitálně připojeném zařízení. Příkladem jsou filtry nevyžádané pošty (SPAM) v systémech elektronické pošty.

5.3. Ochrana před nežádoucími (chybnými) příkazy

V první obranné linii proti nežádoucím kontrolním a řídicím příkazům přicházejícím z vnějšku domácího prostředí za účelem kontroly přístrojů v domácnosti a automobilech, jako součásti internetu věcí, musí být kontrola zabezpečeného přístupu, a zejména aktualizace bezpečnostního softwaru zabudovaného do digitálně propojených zařízení (viz též kap. 2 a 3).

6. KONTROLA SOUKROMÍ V PŘÍPADĚ SHROMAŽĎOVÁNÍ ÚDAJŮ

6.1. Úvod

Pokud jsou od spotřebitelů shromažďovány údaje, měla by být kontrola přizpůsobena jejich osobním potřebám a umožňovat jim kdykoliv stanovit a změnit priority ochrany soukromí. To znamená, že souhlasí-li spotřebitelé se shromažďováním údajů v rámci jejich vlastních domácích činností, je pak nutná kontrola nad jejich prioritami ochrany soukromí v reálném čase.

Tento princip se vztahuje na shromažďování údajů pro účely:

a) objednávek prostřednictvím e-shopů a poskytovatelů služeb,
b) domácí zdravotní péče,
c) kontroly domácího prostředí (topení, větrání),
d) inteligentních měřičů a sítí,
e) dopravních a navigačních systémů,
f) inteligentních měst,
g) dat o „velkém objemu",
h) internetu věcí ad.

6.2. Ochrana údajů a minimalizace zpracování údajů

Příkladem popisu aktuální situace v oblasti shromažďování údajů o spotřebitelích je dokument z USA[10]: „Zprostředkovatelé údajů shromažďují a uchovávají obrovské množství údajů o téměř každé domácnosti ve Spojených státech a o obchodních transakcích. Databáze jednoho z devíti zprostředkovatelů údajů obsahuje informace o 1,4 bilionech spotřebitelských transakcí a více než 700 bilionů souhrnných informačních údajů; databáze dalšího zprostředkovatele údajů zahrnuje spotřebitelské transakce o objemu jednoho trilionu; a ještě další zprostředkovatel údajů doplňuje do svých databází tři biliony nových záznamů měsíčně. A co je důležitější, zprostředkovatelé údajů uchovávají obrovskou spoustu informací o jednotlivých spotřebitelích. Například jeden z devíti zprostředkovatelů údajů má 3000 datových segmentů týkajících se téměř každého spotřebitele ve Spojených státech." Principiálně je situace na evropském digitálním trhu podobná.

I když tedy máme právo na ochranu údajů, včetně minimalizace sbíraných údajů, skutečnost je taková, že:

- mnozí spotřebitelé si neuvědomují, když

[10] Data Brokers – A Call for Transparency and Accountability

udělí počáteční souhlas, jaké údaje jsou shromažďovány, anebo význam tohoto kroku pro jejich soukromí;
- mnoho organizací má v praxi potíže s minimalizací sběru údajů;
- v současné době je shromažďování údajů mimo kontrolu spotřebitelů v důsledku souhlasu zakotveného v podmínkách, které musí být odsouhlaseny před tím, než lze výrobky nebo služby získat.

6.3. Dopady na služby

Možný dopad „minimalizace" sběru dat je velmi podobný jako v případě principu „kontrola spotřebitelů nad vlastním soukromím" (viz kapitola 3), při jehož uplatnění by měla být zajištěna úplná kontrola soukromí.

Kdyby se spotřebitelé rozhodli omezit shromažďování údajů prostřednictvím kontroly priorit soukromí, pak by toto omezené shromažďování údajů mohlo mít vliv na úroveň služeb, které jsou spotřebitelům poskytovány. Existují tři kategorie možného omezení služeb, které je třeba zohlednit:

a) **Okrajové** omezení z pohledu dodávky služby

Okrajové omezení znamená, že hlavní služba může být poskytována, aniž by byly shromažďovány údaje. Jako příklad by se daly uvést podrobné údaje o nákupu potravin na věrnostní kartě supermarketu. Pokud spotřebitel z důvodu ochrany soukromí znemožní shromažďování příslušných údajů, což může představovat dočasné odvolání souhlasu, lze očekávat, že to ovlivní rozsah „poskytovaných výhod" vázaných na věrnostní kartu.

Kontrola soukromí může být dočasná nebo dlouhodobá a její vliv na okrajové výhody se může měnit s délkou doby, po kterou je na základě iniciace spotřebitelem příslušné organizaci znemožněno údaje shromažďovat.

b) **Významné** omezení z pohledu dodávky služby

Významné omezení znamená, že se může pokračovat v poskytování služby, ale s určitým omezením, pokud jde o charakteristiky a vybavení služby v období, kdy kontrola soukromí znemožňuje shromažďování údajů.

Například domácí bezpečnostní systém může detekovat narušitele a přenášet video. Znemožnění přenosu videozáznamu z důvodu ochrany soukromí povede k tomu, že systém bude pracovat, ale s omezenými funkcemi.

c) **Zásadní** omezení z pohledu dodávky služby

Zásadní omezení znamená, že hlavní služba nemůže být poskytována a spotřebitel musí vzít na vědomí, že služba nebude dostupná, pokud bude zablokován prvek shromažďování jednotlivých údajů. Příkladem by mohlo být využití kontroly soukromí k zablokování shromažďování údajů o poloze pro aplikaci „najít místo, kde se lze najíst".

Soukromí spotřebitelů a vzájemné působení služeb

V případě, že by kontrola soukromí ovlivňovala úroveň přijímané služby, měly by normy popisující osvědčené postupy zahrnovat zpětné mechanismy pro spotřebitele, které by spotřebiteli umožňovaly přezkoumat a potvrdit nebo zrušit stanovené priority ochrany soukromí.

7. SOUKROMÍ NA VEŘEJNÝCH MÍSTECH

Jsou-li informace o spotřebiteli umístěny na veřejných doménách, měla by být běžným pravidlem **anonymita,** tj. jednotlivce lze identifikovat pouze digitálně, pokud některé z jejich osobních údajů (PII) byly shromážděny a zpracovány (analyzovány) za účelem jejich identifikace. Hlavním aspektem v tomto ohledu je potřeba transparentního a spravedlivého řízení procesu identifikace a analýzy.

Ve veřejném prostředí – a to jak v reálném, ve kterém jsou používána čidla (včetně kamer), tak ve virtuálním, jako jsou hry pro více hráčů nebo při používání internetu, by jednotlivci měli mít možnost předpokládat, že jejich identifikovatelnost bude omezena na osoby, které znají, nebo na případy, kdy souhlasili s tím, že budou identifikováni. Jinak by měla být anonymita pravidlem, pokud ji právní předpisy přímo nevyžadují.

Například Electronic Freedom Federation k tomu uvádí: „Nikdo nesmí být vystaven svévolnému zasahování do soukromého života, do rodiny, domova nebo korespondence ani útokům na svou čest a pověst. Každý má právo na zákonnou ochranu proti takovým zásahům nebo útokům."

Anonymita má mnoho pozitivních účinků, pokud jednotlivec čelí represivním praktikám významných společností či státu, ale stejně tak může anonymita chránit ty, kteří se chovají zločinně.

Tématu se týká přístup popsaný v kapitole 5, pokud jsou čidla využívána organizacemi, respektive v kapitole 4, pokud soukromé osoby zaznamenali prostřednictvím kamery nebo čidel údaje týkající se někoho jiného.

8. ODPOVĚDNOST ZA OBSAH ŠÍŘENÝCH INFORMACÍ

Ve veřejném, sociálně sdíleném a osobním prostředí by měli jednotlivci očekávat, že ponesou v souladu s národními právními předpisy právní odpovědnost za jakékoliv škody způsobené někomu jinému a za správnost svých veřejných prohlášení.

Tento princip má vliv na níže uvedené:

a) svoboda vyjádřit osobní názor, kterou je třeba zachovat;
b) svoboda organizovat se, kterou je třeba zachovat;
c) kybernetická šikana;
d) otázky související s křivým nařčením a pomluvou na internetu;
e) podněcování k nenávisti;
f) anonymní účastníci na Twitteru (Twitter trool) a jiné.

Tento aspekt ochrany soukromí a jiné vlivy jednotlivců na soukromí spotřebitelů jsou zohledněny v rámci kapitoly 5, pomocí níž můžeme identifikovat obsah, který považujeme za obtěžující.

9. POSOUZENÍ DOPADŮ NA SOUKROMÍ

9.1. Zapojení spotřebitelů do vývoje

Existuje mnoho dobrých důvodů pro přímé zapojení spotřebitelů do vývoje nových výrobků a služeb.

Proces inovace a vývoje by měl zahrnovat zapojení prvních uživatelů a zpětnou vazbu, a to s cílem omezit množství faktorů, které mohou negativně ovlivnit soukromí, již na samém začátku návrhu. Zapojení prvních uživatelů by mělo odhalit řadu otázek souvisejících s provozem a provedením, a to včetně jakýchkoliv otázek týkajících se ochrany soukromí.

9.2. Principy posouzení dopadů na soukromí

Přístup „bezpečnost již od návrhu" by měl využívat posouzení dopadů na soukromí provedené v rámci procesu návrhu pro výrobky nebo služby, které jsou tvořeny digitálními spotřebitelskými zařízeními nebo je obsahují. Posouzení dopadů na soukromí by se mělo v rámci procesu vývoje opakovat s cílem zajistit, že ochrana soukromí a jeho kontrola budou součástí provedení.

V posledních fázích návrhu by mělo být posouzení dopadů na soukromí využito k poskytnutí základních informací, které jsou pro spotřebitele nezbytné, jakmile jsou výrobek nebo služba uvedeny na trh. K těmto informacím patří informace o jakékoliv úrovni zbytkového rizika pro soukromí a také o jakémkoliv zmírňujícím opatření, které musí uživatel přijmout, aby se dosáhlo této úrovně zbytkového rizika.

Protože posouzení dopadů na soukromí je zdrojem klíčových informací o soukromí spotřebitelů, je důležité, aby se k posouzení dopadů na soukromí všech digitálně propojených spotřebitelských zařízení přistupovalo důsledně. To by usnadnilo spotřebitelům volbu a umožnilo by vytvoření rovných podmínek pro všechny podniky působící na spotřebitelských trzích.

Za tímto účelem je třeba využít všude, kde je to možné, stejný rámec pro posouzení dopadů na soukromí vytvořený v rámci EU pro periferní technologie. V současné době platí evropská norma EN 16571[11], do které je začleněn rámec pro hodnocení rizika přejatý z metodiky posouzení bezpečnostního rizika z ISO/IEC 2700[12].

Do tohoto přístupu k dosažení posouzení dopadů na soukromí je doplněno hodnocení tří faktorů, které dohromady tvoří celkový výsledek. Jedná se o níže uvedené:

- hodnocení citlivosti osobních údajů, která by mohla představovat riziko – hodnocené od 0 do 4;
- hodnocení ohrožení soukromí zranitelnými místy návrhu – hodnocené od 0 do 3;
- hodnocení pravděpodobnosti, že zranitelné místo bude zneužito – hodnocené od 0 do 3.

Tyto faktory vyvolávají neustávající debaty, z nichž nejkontroverznější je debata o třetím faktoru, tj. o pravděpodobnosti, že zranitelná místa ochrany soukromí budou zneužita.

[11] ČSN EN 16571:2014 Informační technologie – Postup posouzení ochrany osobních údajů v RFID

[12] ČSN ISO/IEC 27005: 2013 Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací

Uvedená norma přijala užitečný přístup k posouzení dopadů na soukromí, který je založen na hodnocení pravděpodobnosti rizika pro ochranu soukromí ve čtyřech stupních 0–3:

0 = žádné zneužití, které je reálně možné v rámci návrhu, a tudíž ani žádné teoretické riziko
1 = teoretické riziko, které bylo popsáno ve studiích ze seriózních zdrojů
2 = ověření konceptu (tj. praktická ukázka), které bylo demonstrováno uznávanými výzkumnými pracovníky v oblasti bezpečnosti a soukromí
3 = prolomení soukromí/zabezpečení, ke kterému došlo v praxi na trhu

Tato problematika ovšem vyžaduje podrobnější rozklad, pro který zde nemáme místo, ale můžeme odkázat na dokument ANEC *Key Principles for Digital Device Privacy Impact Assessment*.

10. ZÁVĚR

Spotřebitelé by měli v podstatně větší míře vnímat osobní odpovědnost za ochranu svého soukromí v digitálním světě.

I když máme právo na ochranu údajů, včetně minimalizace sbíraných údajů, skutečnost je taková, že při internetových nákupech a dalších službách poskytovaných prostřednictvím internetu a operátory mobilních sítí:

- mnozí spotřebitelé si neuvědomují, když udělí počáteční souhlas, jaké údaje jsou shromažďovány anebo význam tohoto kroku pro jejich soukromí;
- mnoho organizací má v praxi potíže s minimalizací sběru údajů;
- shromažďování údajů je mnohdy mimo kontrolu spotřebitelů v důsledku souhlasu zakotveného v podmínkách, které musí být odsouhlaseny před tím, než lze výrobky nebo služby získat.
- spotřebitelé místo řádného zabezpečení svých mobilních zařízení se často spoléhají na to, že sami operátoři mobilních sítí budou vyvíjet iniciativu, pokud jde jak o zabezpečení zařízení, tak o zajištění bezpečného přenosu informací prostřednictvím rádiových sítí.

Je třeba dbát, aby software, který si kupujeme pro svá digitální zařízení, pocházel od ověřených dodavatelů a software i jeho zdroje byly pod přísnou bezpečnostní kontrolou a hodnocením bezpečnosti. Je zásadní si uvědomit potřeby aktualizací bezpečnostního softwaru a procesů s tím souvisejících, přičemž tyto by měly být pro uživatele snadno pochopitelné. Spotřebitel musí sledovat informace, kdy je vyžadován z jeho strany zásah, odhadovat jednotlivá zranitelná místa a rizika útoku. Důvěryhodnost a verifikace zdrojů aktualizace zabezpečení jsou naprosto nezbytné.

Propojení zařízení a sítí využívaných k poskytování programů a aplikací, které jsou využívány spotřebiteli v jejich osobních životech, by mělo zajistit, že každý jednotlivec využívající program nebo aplikaci může v reálném čase kontrolovat, kdo na sociálních sítích a v rodině může mít přístup k osobním údajům z programu nebo aplikace, které se k němu vztahují. Každý musíme mít možnost kontrolovat údaje, které vytváříme nebo které se nás týkají, a rozhodovat, zda tyto údaje budou shromažďovány a pokud ano, jakým způsobem budou využívány.

Rodiče by měli mít možnost (a také zájem)

prostřednictvím technického zařízení sledovat, jakým způsobem jejich děti využívají aplikace a online služby, a to nikoli pouze na základě celkové dohody a souhlasu dítěte, ale s přihlédnutím k vývoji a rozumovým schopnostem dítěte.

Ve veřejném, sociálně sdíleném a osobním prostředí by měli jednotlivci očekávat, že ponesou v souladu s národními právními předpisy právní odpovědnost za jakékoliv škody způsobené někomu jinému, a za správnost svých veřejných prohlášení. Tento princip zahrnuje různé aspekty a strany problému, například svobodu vyjádřit osobní názor, kterou je třeba zachovat; svobodu organizovat se, kterou je třeba zachovat; kybernetickou šikanu; otázky související s křivým nařčením a pomluvou na internetu; podněcování k nenávisti apod.

Není pochyb, že obezřetnost a sebeuvědomění vlastní odpovědnosti každého spotřebitele by mělo být podpořeno srozumitelným a efektivním právním prostředím, důslednými technickými normami a dalšími samoregulativními nástroji, dodržovanými poskytovateli digitálních služeb.

ZDROJE

▶ **Právní předpisy ČR a EU**

- Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění účinném od 1. ledna 2015
- Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně jednotlivců v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů

▶ **Technické normy**

- ČSN ISO/IEC 29100:2015 Informační technologie – Bezpečnostní techniky – Rámec soukromí
- ČSN EN 16571:2014 Informační technologie – Postup posouzení ochrany osobních údajů v RFID
- ČSN ISO/IEC 27000:2014 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník; a další normy této řady
- ČSN ISO/IEC 27005:2013 Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací

▶ **Dokumenty ANEC**

- ANEC-ICT-2015-G-064 - May 2015, ANEC Pocket Guide, Consumer Representatives Guidance Domestic Privacy and the Privacy of Digitally Connected Devices
- Key Principles for Digital Device Privacy Impact Assessment http://www.anec.eu/attachments/ANEC-ICT-2015-G-008.pdf
- Využití údajů o spotřebitelích – Pokyny pro zástupce spotřebitelů týkající se soukromí (Using Consumer Data – Consumer Representatives Guides on Privacy) http://www.anec.eu/attachments/ANEC-ICT-2015-G-009.pdf

▶ **Jiné zdroje, odkazy na internet**

- How does the data protection reform strenghthen citizens' rights? http://ec.europa.eu/justice/data-protection/index_en.htm
- EU Data Protection Day – Key Message http://www.beuc.org/publications/2013-00056-01-e.pdf
- White house's report on Big Data and the Future of Privacy http://www.consumerwatchdog.org/newsrelease/consumer-watchdog-tells-white-house-team-people-have-right-control-data
- http://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety
- Obavy a Obama (2009), Lipton (2009:4 – http://social-networks-privacy.wikidot.com/
- Data Brokers – A Call for Transparency and Accountability – http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf
- Electronic Freedom Federation" – http://www.eff.org/files/filenode/unspecial-rapporteurfoe2011-final_3.pdf

O NÁS

Sdružení českých spotřebitelů, z. ú. (SČS) *si klade za cíl hájit oprávněné zájmy a práva spotřebitelů na vnitřním trhu EU a ČR, přičemž zdůrazňuje preventivní stránku ochrany zájmů spotřebitelů: „Jen poučený spotřebitel se dokáže účinně hájit". SČS působí v řadě oblastí – pokrývají odbornosti ve vztahu ke kvalitě a bezpečnosti výrobků včetně potravin, technické normalizaci a standardizaci, kvalitě a bezpečnosti služeb včetně služeb finančního trhu aj.*

Pod Altánem 99/103
100 00 Praha 10 – Strašnice
TEL.: +420 261 263 574
e-mail: spotrebitel@regio.cz
www.konzument.cz

Kabinet pro standardizaci, o. p. s. (KaStan) *je nezávislou obecně prospěšnou společností založenou Sdružením českých spotřebitelů. Cílem je zvyšování bezpečnosti a kvality výrobků a služeb vytvářením a podporou funkce nástrojů zajišťujících účinné zapojení spotřebitelů do standardizačních procesů (technická normalizace, certifikace a posuzování shody, akreditace, dozor nad trhem), včetně uplatňování technických předpisů a norem.*

Pod Altánem 99/103,
100 00 Praha 10 – Strašnice
TEL.: +420 261 263 574
e-mail: normy@regio.cz
www.top-normy.cz

ANEC – *The European Association for the Co-ordination of Consumer Representation in Standardisation (Evropské sdružení pro koordinaci účasti spotřebitelů na normalizaci) je mluvčím evropských spotřebitelů v oblasti normalizace, který hájí zájmy spotřebitelů v procesu technické normalizace a posuzování shody stejně jako v tvorbě související legislativy a ve veřejných záležitostech. ANEC je financován Evropskou unií a EFTA s příspěním národních spotřebitelských organizací formou věcného plnění. Sekretariát sídlí v Bruselu.*

e-mail: anec@anec.eu
www.anec.eu

PUBLIKACE SDRUŽENÍ ČESKÝCH SPOTŘEBITELŮ, z. ú.,
vydáno ve spolupráci a pro potřeby KABINETU PRO STANDARDIZACI, o. p. s.

OCHRANA SOUKROMÍ SPOTŘEBITELE V DIGITÁLNÍM SVĚTĚ (priority z hlediska spotřebitelů)

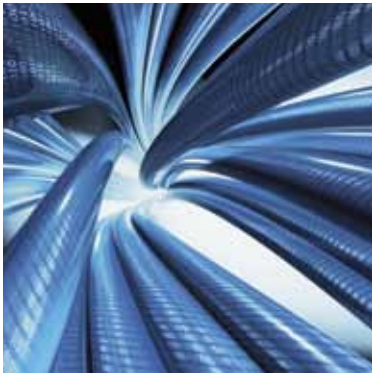
edice: top-normy, svazek č. 3, 1. vydání, pro tisk připravil a editoval

Obálka a grafická úprava Kateřina Tomášková – ktdesign.
Vytiskla tiskárna Garamon Hradec Králové.

ISBN 978-80-87719-32-9 (Sdružení českých spotřebitelů, z. ú.)

KABINET
PRO STANDARDIZACI
... top-normy .cz

SČS
SDRUŽENÍ ČESKÝCH SPOTŘEBITELŮ, Z. Ú.
CZECH CONSUMER ASSOCIATION
www.konzument.cz


Děkujeme za aktivní spolupráci zejména
v moravských regionech ELIM OPAVA o.p.s.
www.elimopava.cz

ELIM opava