**Ochrana osobních údajů**

**v digitální ekonomice**

**Expertní skupina pro rozvoj systému iPodpora**

Bc. Václav Procházka – metodik, ASO
Daniel Smrtka – metodik KZSP ČR
Josefína Vondrová – člen, ASO

# Obsah

[1 Definice osobních údajů – co vše lze považovat za osobní údaj 3](#_Toc475396287)

[2 Ochrana osobních údajů v minulosti 7](#_Toc475396288)

[3 Zpracování osobních údajů v moderní ekonomice 12](#_Toc475396289)

[4 Přístup k osobním údajům z pohledu státu 13](#_Toc475396290)

[5 Nebezpečí zneužití dat v digitálním světě 14](#_Toc475396291)

[6 Nutnost ochrany osobních údajů 16](#_Toc475396292)

[7 Znevýhodněné skupiny osob 18](#_Toc475396293)

[8 Nutná osvěta osob od školního věku do stáří 19](#_Toc475396294)

[9 Ochrana osobních údajů v EU a ve světě 22](#_Toc475396295)

[10 Nové nařízení Komise EU v ochraně osobních údajů 23](#_Toc475396296)

[11 Výhled do budoucna 28](#_Toc475396297)

# Definice osobních údajů – co vše lze považovat za osobní údaj

*Co vše lze považovat za osobní údaje, které si zaslouží ochranu, které je možné volně uveřejnit, definice z pohledu legislativy, z pohledu praxe a běžného života.*

Na osobní údaje můžeme, a patrně bychom i měli, nahlížet ze dvou pohledů – tím prvním musí být pohled daný platnou legislativou, v České republice tedy Zákonem o ochraně osobních údajů č. 101/2000 Sb., který byl několikrát novelizován do současné podoby a samozřejmě i pohledem druhým, spíše praktickým, který vychází z běžného života a praxe. Aby nedocházelo k záměně, případně ke špatnému výkladu některých pojmů, vymezuje česká legislativa pro celou oblast práce s osobními údaji několik pojmových definic, které je vhodné znát.

Podle závažnosti dělí údaje vztahující se k fyzické osobě na:

* anonymní údaje – což jsou jakékoliv údaje, které již při pořízení, případně jejich dalším zpracováním není možné jakýmkoliv způsobem vztáhnout na konkrétní osobu. Z hlediska zákona o ochraně osobních údajů jsou toto obecné informace, které zákon nijak speciálně neošetřuje.
* osobní údaje – již mohou být jakékoliv informace, jejichž užitím můžeme určitou konkrétní fyzickou osobu identifikovat, a to jak přímo, tak i nepřímo. Mohou to být například identifikační čísla, kódy a označení, fotografie či videozáznamy, případně i síťové identifikátory. Tato kategorie údajů je zákonem ošetřena a jejich pořizování a nakládání s nimi je určitým způsobem regulováno a porušování pravidel sankcionováno.
* citlivé údaje – jsou zvláštní podskupinou osobních údajů. Tyto údaje mohou být ze své podstaty vysoce důvěrné a v případě jejich zneužití mohou konkrétní osobě způsobit výraznou újmu. Jsou jimi například biometrické údaje umožňující přímou autentizaci osoby, údaje o zdravotním stavu, sexuálním životě, genetické údaje, rasový a etnický původ, ale například i náboženská orientace, politické postoje nebo členství v odborových organizacích. Tato nejdůvěrnější kategorie osobních údajů je zákonem zvlášť důkladně ošetřena.

Zákon nám rovněž definuje, koho se osobní údaje týkají, kdo je jejich správcem a zpracovatelem:

* subjekt údajů – je konkrétní fyzická osoba, které se dané osobní nebo citlivé údaje týkají.
* správce – je fyzická nebo právnické osoba, tedy subjekt, který osobní údaje zpracovává, určuje způsob a prostředky zpracování osobních údajů a především za zpracovávané osobní údaje odpovídá. Správce technicky nemusí osobní údaje zpracovávat sám, může k tomu zmocnit nebo delegovat jiný subjekt, který bude zpracování osobních údajů provádět z pověření. I když pro správce osobní údaje zpracovává jiný zpracovatel, správce se nezbavuje své zákonné odpovědnosti za získané osobní údaje.
* zpracovatel – je fyzická nebo právnická osoba, tedy subjekt, který byl správcem případně ze zákona pověřen pro správce osobní údaje zpracovávat. I pro zpracovatele zákon definuje konkrétní odpovědnosti a případné sankce.

 V oblasti zpracování osobních údajů se můžeme často setkávat ještě s dalšími pojmy, které je dobré zmínit:

* zpracování, shromažďování a uchovávání osobních údajů – jsou činnosti, při kterých správce nebo zpracovatel osobních údajů systematicky provádí určité operace, přičemž nezáleží, zda automatizovaně nebo ručně. Činnostmi zpracování jsou například jejich shromažďování, uchovávání, zpřístupňování, zpracování, předávání dál, ale i blokování a likvidace. Jde o systematickou, opakovanou činnost.
* likvidace údajů – zahrnuje skutečnou likvidaci uložených osobních údajů, tedy například fyzické zničení datových nosičů, trvalé smazání dat tak, aby již nemohly být nikdy použity.
Pozn.: V této souvislosti je třeba zmínit zvláštní případ, kdy správce nebo zpracovatel osobních údajů jako řádný hospodář zálohuje, popřípadě archivuje pracovní data obsahující osobní údaje, přičemž dojde k požadavku na likvidaci údajů. Například v případě zálohování na pásku jistě není technicky možné jeden konkrétní údaj smazat a zákonodárce toto ani takto striktně nepožaduje. V případě obnovy dat z takového záložního média na toto musí správce nebo zpracovatel brát ohled a případně obnovená data ihned zlikvidovat!
* souhlas subjektu údajů – je prokazatelný, nevynucený a vědomý souhlas subjektu údajů se zpracováním osobních údajů. Tento souhlas může být proveden například podpisem, zatržením políčka webového formuláře, nebo v případě kamerových systémů vstupem do monitorovaného prostoru, který však musí být označen (například na dveřích piktogramem s informací o provádění bezpečnostního záznamu).

Pozn.: Zákon o ochraně osobních údajů definuje i další pojmy, zájemce je může vyhledat přímo ve Sbírce zákonů pod číslem 101/2000 v platném znění.

Z výše stručně uvedeného je zjevné, že z pohledu zákona pod ochranu osobních údajů spadají jen takové údaje, které jsou zpracovávány systematicky, jsou ukládány, zpracovávány a může jejich prostřednictvím být identifikována konkrétní fyzická osoba.

Naproti tomu zákon na ochranu osobních údajů se nevztahuje na případy, kdy se osobní údaje zpracovávají nahodile nebo jednoúčelově (například nahodilá fotografie osoby poškozující vozidlo fotoaparátem nebo kamerou z ruky z balkónu jistě není zpracováním osobních údajů), nejsou dále zpracovávány (například kamerový systém bez záznamu), jsou využity pouze pro určitý krátký čas z technologických důvodů (například cookies identifikátory pro předávání pouze stavových informací na internetovém portále, nikoliv však trasovací cookies) nebo je jejich zpracování výlučně pro vlastní potřebu (například určité adresáře sběratelů apod., nesmí však být předmětem obchodu a nesmí být zveřejňovány).

Připomeňme, že povinnosti dané zákonem na Ochranu osobních údajů se v případě jejich zpracování vztahují jak na firmy a organizace, tak na soukromé fyzické osoby. Především soukromé osoby na toto často zapomínají, především z důvodu nevědomosti, například při provozování kamerových systémů se záznamem.

V České republice je kontrolním orgánem Úřad na ochranu osobních údajů (ÚOOÚ), který vede registr správců osobních údajů, řeší spory mezi subjekty údajů (osoby) a správci nebo zpracovateli osobních údajů, provádí dozorovou činnost, osvětu a uděluje sankce v případě porušení zákona. ÚOOÚ je také partnerem obdobným úřadům v ostatních státech a vůči EU. Adresa webu úřadu je <http://www.uoou.cz/>.

Použijeme-li pohled druhý, který je dán především prudkým rozvojem informačních systémů posledních let, jejich nebývalou dostupností a především rozvojem, či fenoménem sociálních sítí, musíme náš pohled poněkud rozšířit, jelikož pod něj bude spadat mnohem širší okruh údajů. Musíme si uvědomit, že obrovské množství uživatelů moderních informačních technologií vkládá do různých systémů obrovské množství svých privátních dat, množství osobních informací, informací o své rodině, o svém domově, mnoho informací o zaměstnání, o přátelích, zveřejňují své názory na mnoho oblastí života, vkládají fotografie své vlastní, fotografie svých dětí, přátel, včetně různých videí, leckdy i na hraně intimnosti. Toto jsou informace, které o jednotlivých uživatelích sdělí velmi mnoho, však jsou také v současnosti sociální sítě hojně využívány například personalisty, kteří si takto „lustrují“ případné zájemce o zaměstnání.

Uživatelé do těchto systémů vkládají své informace zcela svobodně a z vlastní vůle, informace jsou určeny ke zveřejnění, primárně tedy nejde z pohledu zákona o typické zpracování osobních údajů a tak je zcela na vůli provozovatele, jak s vloženými údaji naloží (pomineme registraci, kde se identifikujeme jménem, e‑mailem, bydlištěm atd., tam zjevně jde o zpracování osobních údajů). Je tedy velmi potřebné porozumět provozním podmínkám konkrétního provozovatele a vzít na vědomí, že vložená data se často stávají majetkem provozovatele, který s nimi ve své podstatě může naložit, jak sám uzná za vhodné. Je mnoho případů, kdy především mladí uživatelé po několika letech litují, že na sociální sítě či různé seznamky na internetu vkládali vlastní fotografie, přičemž fotografie z večírků jsou tou lepší variantou.

Je třeba zmínit právo na ochranu osobnosti, která s ochranou osobních údajů souvisí nepřímo, ale která zaručuje právo na soukromí, chrání morální, sociální a fyzické aspekty života, čest a vážnost jednotlivce a je upravena Občanským zákoníkem. Pozor na zveřejňování informací a fotografií ostatních osob na komunitních a sociálních sítích, videí na populárních videoportálech jako je YouTube, k tomu je vždy třeba mít souhlas dané osoby, přičemž tento souhlas může daná osoba kdykoliv odvolat!

Na osobní údaje raději nahlížejme nejen z pohledu zákona, ale používejme široký pohled a především kritické myšlení, moderní technologie nám mohou velmi dobře sloužit, ale zároveň nám mohou být zlým pánem. Internet umožnil obrovskému množství uživatelů navzájem komunikovat, nebývalou rychlostí přesouvat a zpracovávat obrovské objemy dat bez ohledu na geografické umístění. Na internetu se kromě obrovské spousty bezúhonných uživatelů pohybuje velké množství uživatelů, kteří na námi poskytnutých datech chtějí vydělávat a mohou nás v lepším případě otravovat (například cílená telefonická reklama), ale je zde i dostatečně velká skupina kriminálních živlů, které naše data mohou zneužít nebo i kriminálně proti nám samotným využít – jsou známy případy uživatelů, kteří se na sociálních sítích pochlubili domácím vybavením a informací o odjezdu na vysněnou dovolenou a zpět se vrátili do prázdného domu, nebo bytu. Známé jsou rovněž případy zcizení identity, kdy množství dostupných informací o vlastní osobě umožní podvodníkovi vydávat se za jinou osobu a podvodně odebrat zboží. Je těžké vysvětlovat dodavateli, kterého vidíte prvně v životě, že jste nic neodebrali a faktury za podvodníka platit nechcete.

Ochrana osobních údajů je v České republice a obecně v členských státech Evropské unie z pohledu zákona poměrně dobře a přísně ošetřena, této oblasti je přikládán vysoký stupeň důležitosti. Otevřené prostředí internetu a jeho celosvětový dosah z principu nemůže být zákony jedné nebo několika zemí globálně chráněno. Proto je na každém jednotlivém uživateli, aby jak se svými daty, tak s daty ostatních nakládal velmi obezřetně a uvážlivě. Platí jednoduchá, ale poměrně pravdivá poučka „Co na internet napíšeš, to už nikdy nesmažeš“.

# Ochrana osobních údajů v minulosti

*I v minulosti byly některé informace chráněny a byly považovány za důvěrné.*

Lidstvo na naší krásné planetě Zemi disponuje určitými přírodními zdroji, které se daří více či méně úspěšně zužitkovat, některé následně recyklovat, některé jsou bohužel vyčerpatelné. Za přírodní bohatství můžeme považovat i ne zcela zjevné komodity, jako například frekvenční pásma, která můžeme řadit k vyčerpatelným zdrojům (připomeňme rozšiřování frekvenčních pásem LTE datových sítí na úkor TV a tím budoucí nutnost přechodu na úspornější přenosové standardy, např. DVB-T2) nebo informace, které naopak můžeme přiřadit ke zdrojům neustále se rozšiřujícím a nevyčerpatelným. Informace lidstvo střádá od počátku věků, je to bezedný zdroj a čím úspěšněji určitá civilizace informace střádá a čím efektivněji s nimi pracuje, tím úspěšnější je i v ostatních oblastech. Proto informace můžeme považovat za určitou formu majetku, za obchodovatelnou komoditu, pro jejíž použití, uchování a obchodování je třeba stanovit určitá pravidla. Informace má svou hodnotu, má i svého vlastníka.

V minulosti, kdy neexistovaly informační technologie, byly informace dostupné omezenému okruhu uživatelů, ve své podstatě patřily určité formě společenství, státním útvarům nebo náboženským institucím. Vyhledávání a analyzování nastřádaných informací bylo v dřívějších dobách poměrně náročné, ne-li zcela nemožné, mnoho informací bylo nevědomě duplicitních, za informacemi bylo nutné cestovat, naopak mnoho informací se vůbec nesledovalo a nezaznamenávalo, nebyl jim přikládán žádný význam. Z podstaty formy jejich uložení s nimi mohl nakládat jen vlastník, leckdy stát či náboženská autorita a jimi pověřená omezená skupina osob, která zaručovala i jistou míru ochrany. Uchované informace tak byly zabezpečeny de-facto technologickými možnostmi doby a přístup k nim nebyl třeba speciálně upravovat, jejich zcizení bylo technicky těžko proveditelné.

Změna přišla až v poměrně nedávné době v minulém století s rozvojem informačních systémů, nejprve (z dnešního pohledu) poměrně jednoduchých, ale velmi rychle se rozvíjejících zařízení, s nástupem elektroniky byl rozvoj přímo raketový. Informační technologie, rozvoj telekomunikací, instalace podmořských kabelů, vypuštění komunikačních družic na oběžnou dráhu Země, vznik datových sítí a internetu, jejich nebývalý rozvoj jak z pohledu plošného rozšíření, tak jejich kapacity a rychlosti, nebývalá dostupnost obrovských úložných systémů téměř komukoli, to vše po staletí stejně fungující systém přístupu k informacím zcela změnil. Informace jsou dnes prostřednictvím elektronických médií dostupné téměř komukoliv během chvilky na druhém konci světa, některé jsou přístupné zdarma, některé se staly předmětem obchodu.

Vzhledem k možnému jednoduchému a rychlému přesunu a zpracování informací, které mohou mít i naprosto unikátní a neveřejný charakter (utajované skutečnosti, technické informace, osobní informace a další), přičemž speciálně osobní údaje jsou naprosto nezpochybnitelným vlastnictvím konkrétní osoby, kdy zneužití takových informací může člověka poškodit jak společensky, tak ekonomicky bez ohledu na jeho postavení ve společnosti, vyvstala potřeba vytvoření jasných pravidel vymezujících způsob ochrany dat.

Prvotními základy ochrany osobních dat bylo vytvoření Všeobecné deklarace lidských práv přijatou na konci roku 1948 Organizací spojených národů, pro jejíž přijetí hlasovali zástupci Afghánistánu, Argentiny, Barmy, Belgie, Bolívie, Brazílie, Číny, Dánska, Dominikánské republiky, Ekvádoru, Egypta, Etiopie, Filipín, Francie, Guatemaly, Haiti, Islandu, Indie, Iráku, Íránu, Chile, Kanady, Kolumbie, Kostariky, Kuby, Libanonu, Libérie, Lucemburska, Mexika, Nikaragui, Nizozemska, Nového Zélandu, Norska, Pákistánu Panamy, Paraguaye, Peru, Rakouska, Řecka, Salvadoru, Siamu, Spojeného království, Spojených států amerických, Sýrie, Švédska, Turecka, Uruguaye a Venezuely.
Hlasování se zdrželi zástupci Běloruska, Československa, Jihoafrické unie, Jugoslávie, Polska, Saúdské Arábie, Sovětského svazu a Ukrajiny. Musíme zmínit, že tato deklarace nebyla pro signatáře právně závazná, byla spíše vodítkem pro vytvoření národních právních dokumentů.

V článku 12 je uvedeno:

„**Nikdo nesmí být vystaven svévolnému zasahování do soukromého života, do rodiny, domova nebo korespondence, ani útokům na svou čest a pověst**.“

V roce 1950 následovala v Římě sjednaná Úmluva o ochraně lidských práv a základních svobod, která byla zprvu podepsána členy Rady Evropy, později i dalšími státy, přičemž Česká a Slovenská federativní republika se stala s drobnou výhradou signatářem na začátku roku 1991, ratifikace proběhla v březnu 1992. V tomto dokumentu byla velmi obecná deklarace z předchozí Všeobecné deklarace lidských práv rozpracována a upřesněna. Nejen že zde byla vyjmenována obecná práva a přímo stanoveno, že stát do těchto práv běžně a svévolně nemůže zasahovat, ale byly zde také prvně stanoveny určité konkrétní výjimky, kdy se ustanovení nepoužije, jako například omezení v případě ochrany národní bezpečnosti, v případě ochrany práv a svobod jiných, při předcházení zločinnosti a další výjimky. V Úmluvě stanovené výjimky však musí být zaneseny do národních zákonů, musí být konkrétně vyjmenovány, ale zároveň mohou být upravovány v případě ohrožení státu nebo v případě války.

Úmluva o ochraně lidských práv a základních svobod je do práva České republiky zakomponována prostřednictvím Ústavy a jejího článku 10, má tedy přednost před ostatním vnitrostátním právem. Na Úmluvu navazují a konkretizují ji především ustanovení v uvedená v Občanském zákoníku.

S rozvojem elektronických komunikací a vytvářením databází (zejména databází osob na státní úrovni, ale i v soukromé sféře) vyvstala potřeba konkretizovat pravidla pro nakládání s osobními daty a databázemi osobních dat. Z toho důvodu byly na půdě Rady Evropy vytvořeny první dokumenty, tzv. Resolution (73) 22 a Resolution (74) 29, které jako první stanovovaly principy ochrany soukromí osob při nakládání s elektronickými daty a to jak ve státním, tak i soukromém sektoru. Mezi prvními státy, které do svého práva zapracovaly zákony na ochranu osobních dat, bylo v roce 1973 Švédsko, v roce 1977 následovala Spolková republika Německo a následovaly další státy. Spolupráce států a praxe ukázala potřebu sjednocení pravidel a tak na tomto základě Organizace pro hospodářskou spolupráci a rozvoj (OECD) vydala v roce 1980 Doporučení pro ochranu soukromí a toky osobních údajů přes hranice. Zde již byla specifikována základní pravidla a principy, které se v podstatě užívají dodnes – princip:

* omezení sběru osobních dat
* kvalita osobních dat
* omezení užití osobních dat
* záruka bezpečnosti osobních dat
* otevřenost (povaha a účel zpracování musí být přístupné)
* účast subjektu osobních dat
* odpovědnost správce osobních dat

Teze z tohoto doporučení byly v podstatě převzaty a dopracovány do prvního uceleného mezinárodního právního dokumentu Úmluva ETS č. 108 o ochraně osob s ohledem na automatizované zpracování osobních dat přijaté na začátku roku 1981 Radou Evropy, přičemž její vysoká důležitost byla dána tím, že byla zahrnuta do sféry základních lidských práv a svobod člověka. Byly zde prvně stanoveny zásady, které by jednotlivé státy měly aplikovat do svých právních systémů a prvně definují pojmy jako například „co jsou osobní údaje“, „kdo je subjektem osobních údajů“, „co je automatizovaný soubor dat“, co je „automatizované zpracování“ a „kdo je správce osobních údajů“. Úmluva také definuje, že se aplikuje pro veřejný i soukromý sektor.

Česká republika přijala ETS č. 180 až v roce 2001 (po nabytí účinnosti zákona na ochranu osobních údajů 101/2000 Sb.).

Několik drobných nejasností však mělo za následek rozdílné přijímání Úmluvy členskými státy Rady Evropy, z toho důvodu byl v roce 2001 otevřen Dodatkový protokol k Úmluvě o ochraně osob s ohledem na automatizované zpracování osobních dat, o dozorčích orgánech a toku údajů přes hranice (ETS 181). Zde Česká republika dokument přijala a ratifikovala v podstatě ihned. Rada Evropy neustále monitoruje proces přijímání legislativy o ochraně osobních údajů a jejich uplatňování v jednotlivých státech. Na základě tohoto monitoringu pak nejen český Úřad na ochranu osobních údajů povoluje předávání osobních údajů do zahraničí mimo EU.

Paralelně s iniciativou Rady Evropy se ochrana osobních údajů řešila i na půdě Evropské unie. Již Zakládací smlouva Evropské unie se přímo odvolává na Úmluvu o lidských právech a základních svobod z roku 1950. Na ni následně navazuje Listina základních práv Evropské unie z roku 2000, která sice nemá právní závaznost, ale ochrana osobních údajů je zde zmiňována především ve spojitosti s vývojem informačních technologií.

V roce 1995 vstoupila v platnost Směrnice Evropského parlamentu a Rady č. 95/46/EC, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volném pohybu těchto údajů, která je součástí primárního práva Evropské unie podle Amsterodamské smlouvy. Směrnice Evropského parlamentu a Rady je na rozdíl od doporučení Rady Evropy pro jednotlivé členské státy závazná, v podstatě nařizuje do národních právních systémů aplikovat to, co dříve vydala Rada Evropy jako doporučení. Obdobně definuje základní pojmy, dále je upřesňuje, popisuje způsob zpracování, vymezuje povinnost vymazání neúplných nebo nepřesných dat, rozšiřuje definici citlivých údajů, nastavuje povinnost ohlášení zpracování osobních dat kontrolnímu úřadu před zahájením zpracování dat, zavádí právo podat námitku, právo požadovat náhradu škody a upřesňuje podmínky předávání osobních dat do třetích zemí.

Směrnicí byla zároveň zřízena pracovní skupina podle článku č. 29 (Working Party 29, nebo také „WP29“) složená ze zástupců každého členského státu, která má za úkol koordinovat a posuzovat stav ochrany osobních údajů v Evropské unii, zajišťuje další rozvoj ochrany osobních údajů a vydává stanoviska.

Na prudký rozvoj telekomunikací a především její digitalizace byla na konci roku 1997 přijata Směrnice 97/66/EC Evropského Parlamentu a Rady, která specifikovala zpracování osobních údajů a ochrany soukromí v telekomunikační oblasti, ta však musela být velmi rychle nahrazena inovovanou verzí - Směrnice 2002/58/EC Evropského parlamentu a Rady především z důvodu rozvoje do té doby neexistujících digitálních a mobilních sítí, vzniku nových technologií, zaváděním obsahu na přání, interaktivní TV, vzniku automatizovaných systémů volání a podobně.

V mimoevropském prostoru je situace v ochraně osobních údajů značně roztříštěná, pokus o řešení této nesourodosti mezi EU a ostatním světem byla vyřešena Rozhodnutím Komise č. 2000/520/EC o adekvátnosti ochrany poskytnuté dle principu bezpečného přístavu především s ohledem na potřeby přeshraničního předávání osobních dat do USA, které v principu centralizovaně mnoho oblastí neregulují a EU tak označuje za bezpečné z pohledu ochrany osobních údajů pouze konkrétní jednotlivé subjekty.
Pozn.: Toto rozhodnutí komise bylo později zrušeno rozhodnutím Evropského soudního dvoru (případ C-362/14 Schrems), rozhodování o povolení předávání osobních dat do třetích zemí tak spadá do pravomoci národních úřadů na ochranu osobních údajů.

Česká republika ochranu osobních údajů v ucelené formě zanesla do právního prostředí prvně v roce 1992 přijetím zákona č. 256/1992 Sb., jehož podkladem se stala výše zmíněná Úmluva ETS 108 o ochraně osob s ohledem na automatizované zpracování osobních dat. Prvně se tak v českém právu objevují termíny jako osobní údaje, dotčená osoba, provozovatel, informační služba, likvidace informace, a mnohé další do té doby českému právu neznámé pojmy. Zákon prvně definoval podmínky zpracování osobních dat, účel jejich sběru, stanovoval základní principy zaručení bezpečnosti a jistým způsobem definoval, co jsou citlivé údaje. Zákonem předpokládaný úřad dohledu nad provozováním informačních systémů ale nikdy nevznikl a nevznikly ani některé zákonem předjímané návazné právní normy, čímž Česká republika nebyla z pohledu EU státem dostatečně chránícím osobní údaje – z toho důvodu nebyly členské státy EU oprávněny předávat data do ČR.

Změna nastala až v době přístupových rozhovorů České republiky do Evropské unie, kdy se Směrnice Evropského parlamentu a Rady č. 95/46/EC, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volném pohybu těchto údajů stala jednou ze seznamu povinných právních dokumentů, které musely být implantovány do českého práva. Česká republika splnila svou povinnost přijetím zákona 101/2000 Sb. O ochraně osobních údajů a zřízením Úřadu pro ochranu osobních údajů.

# Zpracování osobních údajů v moderní ekonomice

*Moderní ekonomika přináší mnoho technologických změn, především počítačové zpracování dat, sběr informací všeho druhu, jejich vyhodnocování a párování, obchod s daty.*

Stále existuje velká skupina lidí, kteří jsou udiveni, když jim jsou na jejich osobní adresy domů doručovány nevyžádané obchodní balíčky se vzorky lákající k nákupu, že jim volá zástupce jakéhosi operátora s výhodnější nabídkou služeb, snad každému z nás do e-mailových schránek denně padá mnoho nevyžádané pošty s nabídkou všeho možného od Viagry, výhodného pojištění nebo 20ti tunového bagru. Všechny tyto aktivity jsou produktem přímého marketingu firem, jejichž jasným zájmem je nalákat co nejvíce nových zákazníků.

Nechat v televizním vysílání zobrazovat účinnou reklamu a čekat na zákazníka, který přijde do obchodu pro nový produkt, je velmi nákladné. Jednou z cest je tak získání co nejvíce a co nejpřesnějších informací o potenciálních zákaznících, o jejich zvycích a na základě těchto údajů vytipovat nejvýhodnější vzorek lidí, kteří by se mohli stát novými odběrateli zboží a služeb. Takovéto údaje, celé databáze jsou dnes velmi cenným obchodním artiklem a je s nimi čile obchodováno. Jediným problémem je, jak tato data získat. Ideálním zdrojem jsou právě konkrétní lidé, kteří poskytnou data i se souhlasem na zpracování a nejlépe zdarma. Zde nastupuje sociální inženýring. Stačí vhodně vymyslet a zrealizovat různé soutěže s pouhou možností získat drobnost nebo velké slevy, jejichž účastníci dobrovolně vyplní mnoho údajů a dají přímé svolení ke zpracování i k obchodovatelnosti s těmito daty. Dotazníky často obsahují i velice osobní dotazy, například rodinné poměry, finanční příjem, oblast zaměstnání. Často je zde také dotaz na jména a kontaktní údaje na další spřátelené osoby (jež budou následně osloveny). Je až s podivem, jak velké procento osob dobrovolně sdělí mnoho osobních i citlivých údajů neznámému člověku v případě vidiny možné výhry. Nedávno provedený test jedním z plošně působících zpravodajských portálů získal tímto způsobem osobní data od více jak 30 % oslovených osob. Najatí agenti se prezentovali jako zástupci neexistující fiktivní firmy a nabízeli za poskytnuté údaje *možnost* vyhrát zájezd s 90% slevou.

Dnes velmi populární sociální sítě jako je Facebook, Google, Microsoft, služby jako Skype ve velkém shromažďují a zpracovávají data, která jim dobrovolně a ve velkém poskytují právě jednotlivci – jejich uživatelé. Leckdy se ani nezamýšlíme nad tím, že nám tyto firmy poskytují jimi nákladně vytvořené a výborně fungující systémy zcela zdarma. Jedná se o globálně působící firmy a již dnes je zřejmé a nadmíru pravděpodobné, že v budoucnu budou mít uživateli vložené a zpravidla jimi vlastněné informace a nastřádaná data cenu zlata. Například díky případu Snowden víme, že tyto společnosti data bez problému zpřístupňují bezpečnostním složkám USA. Nyní jsme ve věku vytváření dat, „těžit“ a využívat se začne za několik let a pro mnohé osoby může být velmi nepříjemné, co vše z hlubin internetu může po mnoha letech vyjít na povrch. V prostředí internetu se nezapomíná.

Měli bychom být velmi obezřetní při předávání svých osobních a dalších dat různým osobám a firmám jen při vidině možného zisku či úspory, případně jenom pro vlastní momentální potřebu zviditelnit se. Dobrovolně tak předáváme osobní data, která se následně s naším svolením stávají obchodním artiklem a která jsou velmi cenným zbožím pro obchod v budoucnu.

# Přístup k osobním údajům z pohledu státu

*Přístup k osobním datům z pohledu komerčního subjektu zohledňuje především obchodní zájem, z pohledu státu se jedná o potřebu fungování běhu celého systému. Samostatnou kapitolou je přístup policejních složek, státních a armádních tajných služeb.*

Stát pro své fungování zpracování osobních údajů jednoznačně potřebuje, o tom patrně nikdo nepochybuje, je třeba vést databáze údajů o občanech, o sociálním pojištění, databáze katastru nemovitostí, registr firem a další nepřeberné množství informací. Otázkou pak ale je, zda o nás stát neshromažďuje příliš mnoho informací a zda by mu jich nestačilo méně. V tomto ohledu Česká republika nijak nevybočuje z průměru, spíše se zdá, že náš stát patří mezi rozvinutými ekonomikami k těm umírněnějším „sběratelům“ osobních a jiných dat. Dalo by se tedy spekulovat, že stát je obecně tím největším zpracovatelem osobních údajů. Naštěstí je způsob zpracování těchto dat v rámci EU náležitě chráněn a do budoucna se tato ochrana ještě zvýší.

Můžeme také konstatovat, že velké množství elektronických dat spravovaných státem je občanovi často i zdarma dostupných, jedná se především o různé registry, jako je katastr nemovitostí nebo obchodní rejstřík. Další registry jsou dostupné příslušným úředníkům (např. karta řidiče). S postupným zaváděním e-governmentu a jistým propojováním těchto registrů by mělo být prvořadým zájmem efektivní fungování státní správy. Nyní je alespoň k dispozici jednotná www stránka s odkazy na jednotlivé elektronické registry a elektronické služby státu: **http://www.202020.cz/**

Po útocích na WTC v New Yorku v roce 2001 vzrost ze strany států požadavek na mnohem větší rozšíření kamerových systémů, sledovacích zařízení, odposlechů, skenerů a dalšího shromažďování dat z důvodu zajištění kolektivní bezpečnosti. V této souvislosti můžeme hovořit přímo o invazi do soukromí jednotlivců, je otázka, zda již není zdravá míra tohoto sledování státem překročena.

# Nebezpečí zneužití dat v digitálním světě

*Digitální svět zjednodušuje přenos informací v masivním objemu, k jeho přenosu se zpravidla využívají veřejné přenosové trasy, je možné využít velkokapacitní přenosná média. Tyto technologie pak zjednodušují přenos dat, jejich možné zneužití jak zpracovateli, tak třetími osobami.*

Prudký rozvoj informačních technologií způsobil, že vlastnictví výkonného počítačového vybavení a rychlé připojení k síti internet je dnes naprosto běžnou záležitostí nejen v nejvyspělejších ekonomikách světa, ve středně rozvinutých státech, ale stává se zcela běžnou věcí prakticky po celém světě. Internet využíváme prakticky denně, prohlížíme zpravodajství, hledáme informace, vzděláváme se, komunikujeme s ostatními lidmi a firmami, nakupujeme on-line v eshopech, obchodujeme s jinými firmami, sledujeme multimediální obsah nebo spravujeme své bankovní účty a spoustu dalších činností. Využití je obrovské. V rámci své práce v kyberprostoru vkládáme obchodní, finanční a technické údaje, údaje osobní povahy. Zpravidla nás vůbec nezajímají technické aspekty fungování internetu, je pro nás důležité, že se informace z místa A dostane do místa B. Málokdo se zajímá o to, kudy informace proudí, zda jsou údaje určitým způsobem zašifrovány, jestli někdo naši komunikaci neodposlouchává nebo zda rovnou naše informace dobrovolně neposkytujeme někomu, kdo by s nimi neměl pracovat (opět odkážeme na kauzu Snowden). V rámci kyberprostoru je určité množství hrozeb, o kterých by měl být každý uživatel alespoň v základní míře informován.

Je dobré vědět, že z technického hlediska může být veškerá komunikace na internetu s vynaložením určitého úsilí odposlouchávána. To je důvod, proč by veškeré informace, které nemají zcela veřejnou povahu, měly být přenášeny a uloženy zabezpečeně, tedy šifrovaným přenosovým kanálem. To sice vlastnímu odposlechu nezabrání, ale útočník získá nečitelná data. Všimněte si, že například běžné zpravodajské weby využívají při komunikaci s internetovým prohlížečem nešifrovaný protokol http://, zatímco například on-line platba kartou bude zcela jistě probíhat přes šifrovaný protokol https://. Zadávat na web číslo platební karty prostřednictvím nešifrovaného protokolu http: by tak bylo holým šílenstvím.

Možnosti zneužívání dat na internetu, krádeže identity, čísel platebních karet, to vše samozřejmě neuniklo pozornosti kriminálních živlů, vydělila se samostatná skupina kyber-zločinců, kteří páchají novodobou trestnou činnost z pohodlí a bezpečí svých domovů, o některých z nich můžeme hovořit jako o elitě počítačové kriminality. Zapomeňme na filmy a na studentské koleje plné kostnatých nemytých hackerů, podle analýz FBI to dnes jsou velmi dobře organizované skupiny vysoce vzdělaných profesionálů a o to těžší je boj s nimi. Přitom pomíjíme tajné služby.

Nejlepší obranou je být dobře informován, představme si tedy několik základních termínů a technik útoků:

* Phishing – je jedním z prvních úspěšných útoků, který si pohrává se sociálním inženýrstvím. Základem jsou rozeslané e-maily, které se vhodně voleným textem snaží přesvědčit příjemce o potřebě aktivní komunikace s nějakou institucí, zpravidla bankou a podsouvá odkaz na kliknutí, který na tyto stránky vede. Odkaz je falešný, odkazuje na podvržené stránky, které graficky vypadají shodně jako originální a snaží se formou určitých formulářů vylákat z návštěvníka nějaké privátní informace, například číslo platební karty, platnost a CVC kód. Zpočátku byl phishing v Čechách snadno odhalitelný, jelikož byl psán anglicky nebo velmi špatně přeložen. Nyní jsou již phishingové e-maily a stránky psány naprosto bezchybnou češtinou. Musíme být obezřetní a nejlépe nevyužívat podsunuté odkazy v e-mailech.
* Vishing – forma phishingu využívající sofistikovanější automatizované telefonní služby, princip je podobný jako u phishingu, ale požaduje zavolat na určitou telefonní linku, kde se opět automat snaží vylákat mnohé osobní údaje. Variantou je výzva k volání na čísla s vysokým tarifem. Rada zní – na takové výzvy nereagovat.
* Pharming – je velmi nebezpečná forma phishingu s podsunutými falešnými stránkami například bankovních ústavů. Nebezpečnost spočívá v tom, že je zpravidla kompromitován DNS server, který se stará o překlady internetových adres nebo síťový router, přes který jsme připojeni, což způsobí směrování na podvodné stránky, i když otevřeme čistý prohlížeč a ručně vložíme www adresu například banky. V tomto případě má postižený uživatel pramalé šance podvod odhalit. Vodítkem může být nestandardní přihlašovaní nebo potvrzovací SMS zpráva došlá z jiného než obvyklého čísla. Toto je velmi riziková forma napadení, naštěstí velmi složitá na provedení.
* Carding – jsou zjednodušeně řečeno krádeže údajů o platebních kartách a to jak ze serverů obchodníků nebo vydavatelů karet, tak přímo od jejich majitelů. Majitelé platebních karet musí být při jejich používání velmi obezřetní, neponechávat karty bez dozoru, nenechat je zkopírovat. V době bezkontaktních karet je rovněž velmi nebezpečné položit takovou kartu na stůl podvodného obchodníka. Stůl může mít zespodu namontován platební terminál a částka do 500 Kč nemusí být potvrzena PIN.
* Sniffing – je způsob odposlechu internetové komunikace, může být instalován jako program nebo jako jednoúčelová krabička na kabelu nebo být nainstalován na komunikačním uzlu. Veškerá komunikace proudící přes tuto krabičku je pak zachycena a může být analyzována. Využívá se především k odchycení přihlašovacích jmen a hesel. Pokud však komunikujeme prostřednictvím šifrovaného spojení, je tato metoda neúčinná.
* WebBug – je svým způsobem drobná štěnice. Samo o sobě se přímo nejedná o nebezpečný útok. Jde spíše o sběr dat. Technicky se například do e-mailu vloží miniaturní odkazující obrázek, bílá tečka. Jakmile e-mail někomu přepošleme a adresát jej otevře, útočník získává síťové informace, kam původní e-mail všude doputoval.
* Cookies – jsou malé síťové identifikátory používané na www stránkách. Využívají se zcela legálně a neškodně například při pohybu na stránkách, kde musíme být přihlášeni jménem a heslem. Mezi jednotlivými stránkami webu přenášejí stavovou informaci, že jsme to právě my. Existují také tzv. sledovací cookies, které mají dlouhou platnost a které mohou být čteny různými weby. Majitel webů (nebo spolupracující organizace) pak snadno zjistí, na kterých všech webech jsme se pohybovali při prohlížení internetu.

Při užití informačních a komunikačních technologií, internetu, sociálních sítí nebo třeba elektronického bankovnictví je třeba být neustále ve střehu a mít povědomí o možných útocích. Jen tak je možné je včas rozpoznat a účinně se bránit. Na internetu platí, že určitý zdravý stupeň paranoie je potřeba.

# Nutnost ochrany osobních údajů

*Občan je z pohledu komerčních subjektů a státu znevýhodněn, leckdy jsou údaje o něm zpracovávány bez jeho vědomí nebo s jeho vynuceným nebo nevynuceným souhlasem. Všechna tato data musí být chráněna, neboť se mohou stát nástrojem pro poškození osoby, které se týkají.*

V době elektronických komunikací a rychlého zpracování obrovských objemů dat s poměrně malými náklady je jejich shromažďování, třídění a zpracovávání činností mnoha státních institucí, úřadů, ale i soukromých organizací. Některá zpracovávaná data mají charakter osobních údajů, některá jiná data jsou anonymizována nebo charakter osobních dat nemají. Zpravidla jsme my všichni velmi často jejich tvůrci či zdrojem.

Anonymní nebo anonymizovaná data nejsou pro naši osobní bezpečnost nikterak závadná, zpravidla se používají jako podklad ke zpracování statistických informací pro rozhodování jejich vlastníků o různých nastaveních a činnostech. Takovým podkladem mohou být například počty lidí cestující hromadnou dopravou pro rozhodování o tom, jaké linky posílit nebo jaké vystačí s vozy o menší kapacitě nebo delším intervalem přepravy. Pokud jsme zdrojem takové jedné elementární informace z celku, tato informace pro nás nemá žádný význam, pro organizátora dopravy však význam má – nikoliv ovšem elementární, ale v celém souhrnném množství.

Správci údajů pracují také s informacemi, jejichž zdrojem jsme my sami a tyto informace mohou mít povahu osobních údajů. Pak už se jedná o informace, které se nás osobně dotýkají, o zpracování osobních dat musíme být spraveni a když už je správce údajů zpracovává, musí být zajištěna jejich ochrana.

Praxe bohužel ukazuje, že ke krádežím osobních údajů dochází a pokud se jedná o velké objemy a „zajímavá“ osobní data, vždy se najde kupec. To bohužel následně láká další potenciální kyber-zločince. Z poslední doby je známý případ krádeže osobních dat ze společnosti T-Mobile, nyní již bývalým zaměstnancem IT oddělení, který zcizil databázi zákazníků i s mnoha dalšími citlivými údaji, což může být pro mnoho zákazníků velmi citlivé (kromě jména a příjmení to byly adresní informace, informace o útratách a používaných mobilních telefonech – tedy informace, z nich je možné docela dobře profilovat bonitu osoby). Podobným případem byla krádež osobních údajů přibližně 10 miliónů klientů společnosti Visa a MasterCard před zhruba 5 lety, kde byla data ukradena přes zprostředkovatelskou firmu, která pro karetní společnosti data zpracovávala.

Dalším typem možným způsobem získání osobních údajů mohou být hackerské útoky na informační systémy správců a zpracovatelů, například na eshopy, a získání dat průnikem do uložených počítačových databází a jejich přenosem prostřednictvím internetu.

Je tedy zřejmé, že osobní údaje jsou velmi cennou a žádanou komoditou a je o ně velký zájem. Z toho důvodu je důležité, aby správci osobních údajů měli své systémy maximálně zabezpečené, aby data byla šifrována a v hojné míře se využívala pseudonymizace, tedy fyzické oddělení částí osobních dat od sebe tak, aby každá jednotlivá část sama o sobě osobním údajem nebyla. Toto je například jedena z novinek v Nařízení Evropského parlamentu a Rady (EU) 2016/679, které musí být do národních právních systémů členských států EU zakomponováno do května 2018. V případě, že při takovémto správném užití pseudonymizace přesto dojde k případnému zcizení dat, budou tyto údaje pro útočníka bezcenné.

# Znevýhodněné skupiny osob

*Především mladistvé osoby, osoby, jež nejsou zběhlé v užívání digitálních prostředků, osoby nemocné, invalidní, pracovně znevýhodněné nebo osoby v těžkých životních situacích si zaslouží speciální ochranu.*

Digitální věk je typický především neskutečně rychlým vývojem technologií. Málokdo si uměl v roce 1980 představit, že v dnešní době budou nejen téměř všichni dospělí, ale i děti chodit s mobilními telefony, které jsou výkonnými počítači s mnoha funkcemi, kde vlastní možnost „telefonovat“ je jen jednou z mnoha dalších funkcí.

Pro mnoho skupin spoluobčanů je však vývoj technologií tak rychlý, že s ním nestačí držet krok a svou technickou i informační nedostatečností se dostávají skoro až na okraj hlavního proudu společnosti a mohou se tak stát obětí drzých výmluvných obchodníků a podvodníků, leckdy na hranici té nejhrubší kriminality, a svým jednáním se téměř dobrovolně a nevědomky poškodit. Známé jsou případy obchodníků se zázračně levným plynem a elektřinou, s pojištěním všeho možného i nemožného, lichváři s půjčkami s nehorázným úrokem, oddlužovací agentury, po jejichž „záchraně“ byl dlužník ještě větším dlužníkem.

Většinou jde o celkem podobný scénář – z různých legálně i podvodně získaných registrů osob se vytipuje někdo snadno zneužitelný, většinou se jedná o starší o samotě žijící osobu, sociálně slabšího spoluobčana, mladistvého, ale i člověka v produktivním věku. Ideálně ale takového, kdo není zběhlý v užívání informačních technologií, kdo si nemůže nebo neumí v rozumně krátkém čase zjistit více relevantních informací pro své následné rozhodnutí. Pak už jen následuje vysvětlení výhod od člověka „tak slušného“, tak „pěkně oblečeného“ nebo s tak „milým hlasem v telefonu“, podpis smlouvy, a pokud postižený nevyužije možnosti ve 14-denní lhůtě od smlouvy odstoupit (§1829 nového občanského zákoníku), stává se smlouva platnou a vyvázání se z ní je většinou drahá záležitost.

Budeme-li si chránit své osobní údaje, svoji osobní identitu, minimálně tím podvodníkům ztížíme přístup k údajům o své osobě, nebo se pro ně staneme doslova neviditelnými. Technicky zdatnější by měli v přiměřené a vhodné míře informovat své blízké, především děti a starší osoby, že informační technologie dávají podvodníkům do rukou silný nástroj pro práci se zpravidla ukradenými daty a že je nebezpečné komukoliv předávat jakékoliv osobní údaje a podepisovat dokumenty, smlouvy nebo je stvrzovat souhlasem na dálku.

# Nutná osvěta osob od školního věku do stáří

*Nutnost alespoň základní osvěty od dětského věku po stáří, ochrana vlastního soukromí, ostražitost v internetovém prostředí, přístup k sociálním sítím.*

Prostředí internetu a informačních technologií je velmi zajímavý obor, který díky interakci láká děti od útlého věku, přes období zrání, dospělosti a tento zájem nás neopouští ani ve zralém věku nebo ve stáří.

Je především na rodičích, aby v době, kdy děti objevují taje informační společnosti, jim formou výchovy předali správné návyky, které je ochrání před možnými nebezpečími, naučili je základním prvkům počítačové bezpečnosti, ochrany osobnosti a v neposlední řadě i ochraně vlastních osobních údajů. Tato investice se do budoucna jistě vyplatí.

Dítě prochází několika vývojovými stádii a podle toho by je rodiče měly vhodnou formou na vstup do digitálního světa připravit:

* batolecí věk, od narození do 3 let – základní vývojové stádium, kdy rozhodně není třeba dítě seznamovat s informačními technologiemi. Rozvíjí se motorika, vyvíjí se osobnost a je rozhodně lepší, aby si dítko hrálo se svými rodiči a s kostičkami nežli s tabletem
* předškolní věk, 3 - 6 let – v této době je již možné s dítětem u počítače pracovat, doporučuje se však pouze ve spolupráci s rodiči, kteří připravují a filtrují vhodný obsah, dítě není vhodné nechávat u počítače bez dozoru. Vzhledem k dostatečné abstraktní vnímavosti je to doba, kdy je vhodné upozorňovat přiměřenou formou na možná nebezpečí číhající na internetu. Rovněž se doporučuje vymyslet dítěti vhodnou přezdívku a připravit jej tak na možné vytvoření jeho alternativní internetové identity. V případě, že je dítěti umožněno využívat počítač bez přímého dohledu, doporučuje se použít software rodičovské ochrany s nastaveným omezeným přístupem
* školní věk, 7 – 11 let – Mnoho dětí v tomto věku s počítačem a internetem běžně pracuje. Mnoho dětí s počítačem raději pracuje samo (myslí si, že již vše umí), logicky uvažuje, ale je pro něj těžké rozeznat skrytá internetová nebezpečí, v této době mají příliš pozitivní pohled na svět. Je vhodné, aby dítě používalo pouze „schválený“ okruh webových stránek, které rodič vyhodnotí jako bezpečné prostředí. S dítětem by měl mít rodič navázán vztah důvěry a děti by měly být poučeny o všech možných hrozbách internetu a v případě jejich rozpoznání by o tom měly svého rodiče informovat. Pro dítě by se mělo stát samozřejmostí informovat rodiče, jakmile bude na internet vkládat svoji identitu. Nedoporučuje se v této době dětem zakládat e-mail a profily na komunikačních nebo sociálních sítích
* období puberty a dospívání, 11 let a více – s pubertou přichází mnohé hormonální a psychické změny, což se projevuje i při práci s počítačem a internetem. Mládež touží po komunikaci se svými vrstevníky, navazují se první vztahy. Na jednu stranu mladiství touží po soukromí před svými rodiči, na druhou stranu jsou ochotni zveřejňovat nejrůznější informace osobní povahy bez ohledu na skrytá nebezpečí. Důrazně varujte dospívající před zveřejňováním osobních fotografií, zveřejňováním své pravé identity neznámé protistraně, varujte je před schůzkami s cizími lidmi, je vhodné poučit je o výhodách anonymity na internetu, o používání alternativní internetové identity, poučte dospívající o etickém chování, o základech práva a o povinnostech, o ochraně osobních údajů. Jasně vysvětlete pojem ochrana osobnosti, věnujte pozornost tomu, že není možné libovolně zveřejňovat informace o ostatních, natáčet videa a vkládat je např. na YouTube. Naučte dospívajícího člověka vnímat rozdíly mezi počítačovou hrou, realitou na internetu a reálným životem.

Děti a mladiství mají na rozdíl od dospělých snahu co nejvíce s okolním světem komunikovat. Tato jejich otevřenost byla v době bez informačních technologií omezena ve své podstatě na „dvorek“, kam si chodili hrát, nevhodné informace, pomluvy, hašteření mezi jedinci je pak časem běžným a přirozeným způsobem zapomenuto. Jinak je tomu v kyberprostoru, informační technologie vložené informace zaznamenají a velmi často se tato sdělení, ať již se jedná o názor, fotografii nebo video, jen těžko z internetu odstraní, v době sociálních sítí a různých sdílení příspěvků o to hůře.

Na internetu tak číhá mnoho nebezpečí, která nejsou pro děti a mladistvé na první pohled patrná, tyto hrozby jim musí vhodnou formou interpretovat rodič nebo škola a upozornit na možná úskalí zveřejňování informací:

|  |  |
| --- | --- |
| **Nevhodná sdělení** | **Příklady možných ohrožení** |
| Zveřejnění skutečné identity (jméno, příjmení, adresa) | Nezvané návštěvy, stalking, vydírání, nátlak, vyhrožování, poškozování domu, přepadení, únos |
| Zveřejnění e-mailu, telefonního čísla | Obtěžující telefonáty, „prozvánění“, obtěžující SMS nebo MMS, spam, obtěžující e-maily, lákání k šikaně, kyberšikana |
| Zveřejnění údajů o preferencích zboží, osobních údajů | Profilování, cílená reklama, spam |
| Sdělování informací o vlastní osobě, pocity, školní výsledky | Posměšné komentáře, urážky, kyberšikana |
| Zveřejnění fotografie | Urážlivé a posměšné komentáře, kyberšikana |
| Zveřejnění intimní fotografie | Urážlivé a posměšné komentáře, kyberšikana, vydírání, sexuální nabídky, nekontrolované šíření |
| Zveřejnění informací o bytovém vybavení | Pozvánka pro zloděje |
| Zveřejňování mnoha různých informací (i na různých místech) | Vyprofilování, krádež a zneužití identity |

S povděkem musíme konstatovat, že informovanost dětí, mládeže a dospívajících je z hlediska ochrany osobních údajů každým rokem na lepší úrovni. Nejenom že jsou více a lépe informováni jak od rodičů, tak i ve školách. Především ÚOOÚ je v tomto směru aktivním propagátorem bezpečí, který spolupracuje s Ministerstvem školství a tělovýchovy na vzdělávání pedagogických pracovníků, kteří jsou pak schopni relevantní informace předávat svým žákům v rámci výuky informačních technologií, Národní centrum bezpečnějšího internetu připravilo semináře a metodické materiály pro pedagogické pracovníky pro výuku od prvního stupně základní školy až po střední školství.

Zároveň od roku 2007 vyhlašuje Úřad pro ochranu osobních údajů soutěž „Moje soukromí. Nedívat se, nešťourat“ s tématikou ochrany osobních údajů. V loňském roce 2016 proběhl již 10. ročník soutěže rozdělený do kategorií 7-13 let a 14-18 let, vyhlášení výsledků proběhlo za účasti České televize a informace byla odvysílána na ČT :D. Za zmínku stojí, že program spolupráce Úřadu pro ochranu osobních údajů s MŠMT byl v roce 2007 na celoevropské úrovni v Madridu Agenturou pro ochranu údajů oceněn cenou za nejlepší službu veřejnosti v oblasti ochrany osobních údajů.

Naše děti s internetem vyrůstají, je všude kolem nás. Rozhodně nechceme nabádat k příliš silnému ochranářskému přístupu dětí a mladistvých k informačním technologiím, je naprosto jisté, že by si k nim stejně našli jinou cestu. Internet obsahuje mnoho velmi užitečných informací, jejich získávání a práce s nimi i přes jisté riziko jistě bude spíše bonusem pro vývoj, budoucí vzdělávání a další profesní rozvoj. Důležité tak je především seznámení s možnými riziky a naučení mladého člověka používat internetové prostředí bezpečně a odpovědně.

# Ochrana osobních údajů v EU a ve světě

*Regulace a ochrana osobních údajů v ČR, ve státech Evropské unie a ve světě, možnost přes-hraničního zpracování dat, především globálními firmami.*

Zatímco ochrana osobních údajů je v evropských státech velmi podobná a velmi propracovaná, především z důvodu členství v Radě Evropy a v Evropské Unii, která této oblasti legislativy přikládá velmi vysokou důležitost a jednotlivé státy jsou povinny nařízení Směrnic Evropského parlamentu a Rady implementovat do svých právních řádů (o EU se již déle jak 40 let hovoří jako o laboratoři na ochranu osobních údajů), ve světě je situace velmi rozdílná a právní postavení subjektu údajů (fyzických osob) není na tak vysoké úrovni jako v EU.

Z pohledu informačních technologií jsou patrně nejdůležitějším příjemcem dat soukromé i státní organizace usazené v USA – naprostá většina globálně působících firem, jako je např. Facebook, Google nebo Microsoft, je usazena právě tam. Na rozdíl od EU jsou vláda, parlament a úřady USA přesvědčeny, že přílišná centrální regulace a zákonné restrikce spíše škodí, nežli pomáhají, a tak i oblast ochrany osobních údajů ponechávají spíše na samoregulaci rozvinutého a ustáleného konkurenčního trhu, není zde tedy žádný ucelený právní systém na federální úrovni, který by oblast ochrany osobních údajů jako celek, ošetřoval. V tomto kontextu raději ponechme stranou znepokojivé informace o sledování získané v kauze Snowden.

Především z důvodu čím dál více populárních nákupů prostřednictvím internetových tržišť jako je například Aliexpress, Banggood, DX a dalších, je třeba se věnovat i ochraně osobních údajů u těchto firem usazených v Čínské lidové republice. Čína nemá, podobně jako USA, žádné ucelené zákony upravující oblast ochrany osobních údajů, práv na informace, práv k přístupu k nim, na jejich opravu nebo vymazání tak, jako je tomu v evropském právu. Nicméně Čína má několik relevantních sektorových zákonů, které v rámci základního, obchodního, občanského a trestního práva ve svém souhrnu určitý stupeň ochrany osobních dat „spotřebitelům“ zaručují. Stejně jako v ostatních státech se stupeň ochrany určitým způsobem upravuje a zvyšuje.

Z výše uvedených skutečností pak vyvstává otázka, zda je vůbec bezpečné se v celosvětovém internetovém prostředí připojovat na různé služby, např. e-shopy, cloudy, sociální sítě, a další? Doporučujeme věnovat pozornost provozním podmínkám a referencím při ukládání osobních dat do informačních systémů, a to především u těch provozovatelů, kteří jsou usazeni mimo EU. Vzhledem k velkému konkurenčnímu boji na celosvětovém internetovém trhu se dá do jisté míry spoléhat na samoregulaci velkých a globálních provozovatelů, na přizpůsobování těch menších a na pozitivní vývoj v legislativní oblasti v ostatních státech, které se zpravidla předpisy EU inspirují a určitá pravidla postupně zavádějí. Právní vymahatelnost v případě sporů o ochranu osobních údajů je však mimo EU diskutabilní.

# Nové nařízení Komise EU v ochraně osobních údajů

*Nové nařízení Komise EU, integrace nového nařízení do legislativy ČR, co nového přinese a jak se ochrana osob z pohledu ochrany osobních údajů může zlepšit.*

Informační technologie, mobilní komunikace, internet věcí, megabity za vteřinu, terabajty dat, interaktivní televize, sociální sítě, společnost 4.0 – to všechno jsou oblasti a termíny, o kterých nebylo před několika roky ani možné uvažovat. Nyní jsou to běžné slovní obraty a právní prostředí na překotný vývoj musí náležitým způsobem reagovat.

Ochrana osobních údajů v jednotlivých evropských zemích vychází především ze Směrnice Evropského parlamentu a rady č. 95/46/EC o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volném pohybu těchto údajů. Přestože je směrnice vypracována s ohledem na možný budoucí rozvoj technologií, vznikly oblasti, které se nedaly předpokládat. Z této směrnice koncepčně vychází nové Obecné nařízení, jeho základní struktura a klíčové instituty budou většinou stejné. Po stanovení působnosti a definicích jsou pojednány principy nebo zásady ochrany dat, pak práva subjektu údajů, povinnosti správců a zpracovatelů, mezinárodní přenosy dat, dozorové úřady a jejich spolupráce, soudní a správní ochrana, odpovědnosti a sankce, a další ustanovení. Nové nařízení na půdě Evropské unie připravila Komisařka Viviane Redingová.

V květnu 2016 bylo Evropským parlamentem přijato Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. 4. 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

Vzhledem k tomu, že jde o nařízení, které platí přímo a má bezprostřední účinek, jsou všechny členské státy právem EU velmi omezeny v možnostech přijímání rozdílné legislativy. Přesto tu jsou některé legislativní možnosti změny či povinnosti, které mohou jednotlivé státy aplikovat odlišně. Účinnost nařízení vstoupí v platnost v květnu 2018, do té doby jej musí všechny členské státy EU aplikovat do svých právních systémů.

Toto nové Obecné nařízení zasáhne většinu oblastí fungování státu včetně soukromého sektoru, jedinou výjimkou je prakticky jen policejní práce v terénu, postihy trestné činnosti a činnosti zpravodajských a jiných služeb.

Nové nařízení je oproti původní směrnici rozšířené, místo původních 34 článků je 91 článků, místo 25 stran textu je stran 100. Některé povinnosti správců a zpracovatelů se zjednodušují, některé činnosti jsou zcela nové, navíc se kromě principů a základních práv na evropské úrovni sjednocují i některé dříve neuvedené detaily.

Text Nařízení je možné stáhnout ve formátu PDF z oficiálního umístění zde:

**http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32016R0679&from=CS**

Nové Obecné nařízení je rozděleno do několika částí:

* účel a působnost, definice pojmů (články 1 – 4)
* zásady zpracování osobních údajů (články 5 – 11)
* práva subjektu údajů (články 12 – 23)
* povinnosti správce a zpracovatele (články 24 – 43)
* zásady přeshraničních předávání dat (články 44 – 50)
* nezávislé dozorové úřady (články 51 – 54)
* spolupráce a jednotnost (články 60 – 76)
* právní ochrana, odpovědnost a sankce (články 77 – 84)
* zvláštní situace (články 85 – 91)
* přenesené pravomoci (články 92 – 93)
* závěrečná ustanovení (články 94 – 99)

Komisařka Reding s týmem tvůrců je přesvědčena, že nové Obecné nařízení přinese ročně až 2,3 miliardy Euro do evropské ekonomiky z důvodu sjednocení předpisů v členských státech a z důvodu přínosu více jistot zákazníkům a výrazně větší objem on-line nákupů. Nabízí se otázka, zda je metodika odhadu správná, jelikož Komise považuje za administrativní a finanční zátěž jen předpis, podle kterého musí podnikatel ohlašovat určité skutečnosti na úřad (dáno stávající úpravou). Ohlašovací povinnost se správcům do jisté míry skutečně omezuje. Zatímco nyní musí správce údajů hlásit na ÚOOÚ (a na obdobné úřady v ostatních zemích EU) většinu nových zpracovávání osobních údajů (podle § 16 zákona 101/2000 Sb.), nařízení tuto povinnost ponechává jen v malém množství výjimek (článek 34). Každopádně pozice subjektů údajů se posiluje.

Na druhou stranu se nově zavádí řada nových povinností, například hlásit technické narušení ochrany údajů (článek 31) nebo zavedení zmocněnce pro ochranu osobních údajů, které správcům a zpracovatelům odčerpají nemalé finanční částky. Většinu nových činností sice nemusí správce nebo zpracovatel na Úřad hlásit, musí je však provést. Mezi takové tíživé povinnosti náleží povinnost provádět hodnocení dopadu na soukromí (DPIA, článek 35) a povinnost zaměstnávat nebo mít smluvně zajištěného pověřence ochrany údajů (DPO, článek 37). Podle řady zástupců států tak ve skutečnosti přinese nařízení pro soukromé subjekty i pro veřejné orgány více nákladů než úspor, protože ne všichni působí ve více zemích, ale přesto budou muset plnit nové povinnosti, jako by tak činili.

Členské státy EU podaly řadou protinávrhů, nejzajímavějšími byly zejména:

* přístup založený na riziku (Risk-Based Approach), který různé povinnosti správců a zpracovatelů podmiňuje tím, že hrozí nějaké významné riziko. „Risk-based approach“ se výrazně projevuje například v článcích o záměrné ochraně údajů (čl. 25), o povinnosti dokumentace zpracování (čl. 30), o zabezpečení zpracování (čl. 32) nebo o povinnosti zpracovávat hodnocení dopadů na ochranu údajů (čl. 35).
* návrhy na „navrácení“ povinností na úroveň podle směrnice 95/46/EC nebo jejich další balancování. Některé povinnosti (např. vyvěsit politiky zpracování údajů nebo konzultovat veřejnost při přípravě hodnocení dopadů podle čl. 35 odst. 9) byly zrušeny bez náhrady nebo významně oslabeny.
* větší samoregulace soukromého sektoru formou tzv. „pseudonymizace“, kodexů chování (čl. 40) a osvědčení (čl. 42), které by měly usnadnit plnění jiných povinností správce.

Komise navrhla celkem 26 aktů ve své svěřené pravomoci a dále celkem 23 prováděcích aktů. Toto bylo považováno za příliš silné rozšíření pravomocí Komise, neboť šlo zejména o:

* snížení právní jistoty povinných subjektů
* o pravomoc měnit základní prvky nařízení, což je v rozporu se Smlouvami
* nevhodné řešení příslušné otázky
* nevhodnou formu řešení (ve srovnání s vnitrostátními předpisy, kodexy chování, rozhodování dozorových orgánů nebo jejich Sboru).

Schválený text Obecného nařízení tak zahrnuje pouze několik delegovaných a prováděcích aktů, přičemž za nejdůležitější lze označit přijímání rozhodnutí o odpovídající ochraně ve třetí zemi podle článku 45. Role Komise tak byla oslabena zejména ve prospěch nového Evropského sboru pro ochranu osobních údajů, který bude sdružovat dozorové orgány, bude moci rozhodovat spory mezi nimi a vydávat sjednocující stanoviska v řadě oblastí praktické aplikace Obecného nařízení.

Hlavní rozdíly nového Obecného nařízení a původní Směrnice č. 95/46/EC jsou hlavně v těchto oblastech:

* posílení působnosti (více oblastí unijního práva, silnější působnost extrateritoriální)
* posílení ochrany dětí (podmínky souhlasu se zpracováním, podmínky výmazu dat)
* posílení informačních povinností správců (bezplatnost, lhůty)
* posílení některých práv subjektů údajů (bezplatnost, lhůty, rozsah)

Důležitá jsou nová či výslovně upravená práva subjektu údajů:

* explicitně určené právo „být zapomenut“ (čl. 17)
* právo na přenositelnost osobních údajů (čl. 18)
* podrobná úprava vztahu správce a zpracovatele
* posílení kontroly nad správci mimo území EU
* posílení řady požadavků na správce a zpracovatele
* posílení pravidel o bezpečnosti dat (zejména technické) a hlášení narušení bezpečnosti osobních dat
* částečně povinný silný pověřenec ochrany dat pro veřejnou správu, v určitých případech i pro soukromé subjekty
* podrobná úprava instrumentů měkkého práva (kodexy chování, certifikace)
* zásadní sjednocení pravomocí dozorových úřadů pro ochranu dat
* nový článek omezující přenosy údajů do třetích zemí na základě činnosti orgánů veřejné moci těchto zemí, včetně soudů
* podrobná úprava spolupráce dozorových úřadů
* principiálně zcela nová úprava společného rozhodování dozorových úřadů v různých typech přeshraničních případů
* zavedení rozhodovací pravomoci pro kolegium dozorových úřadů v konkrétních věcech
* sjednocení prostředků pro soudní ochranu před rozhodnutím či nečinností dozorového úřadu a pro soudní ochranu před nezákonným zpracováním, včetně náhrady škody
* **sjednocení a zásadní zvýšení sankcí formou 2 % nebo dokonce 4 % podílu z ročního globálního obratu podnikatele nebo absolutní částkou 20 mil. nebo 40 mil. Euro pro všechny ostatní subjekty (použije se vyšší částka)**
* sektorové úpravy pro smíření práva na ochranu údajů se svobodou projevu, s přístupem k úředním dokumentům, pro národní identifikační čísla (RČ apod.), pro zaměstnanecké vztahy atd.

Nové Obecné nařízení o ochraně osobních dat od platné směrnice přebírá v téměř nezměněné formě následující oblasti a definice:

* ponechává většinu hlavních definic (osobní údaj, citlivé údaje, správce, koncept souhlasu atd.)
* ponechává většinu zásad ochrany dat (principy a zákonnost zpracování)
* ponechává většinu práv subjektů údajů a základní povinnosti správců
* ponechává systém opt-out z přímého marketingu
* ponechává koncept bariéry u přenosů do třetích zemí s důkladnými restrikcemi a požadavky na ochranu osobních údajů
* ponechává zásadní prvky postavení nezávislých dozorových úřadů (u nás ÚOOÚ)
* ponechává koncept výjimek pro privilegovaná zpracování (archivní, statistická, vědecká, historická)
* ponechává koncept výjimek pro ochranu veřejných zájmů (bezpečnost, ekonomika, ochrana práv jiných atd.)

Velkou většinu pravidel Obecného nařízení nemůže členský stát příliš legislativně ovlivnit, musí je ve své podstatě přijmout téměř beze změny, je tu ovšem systémová mezera v oblasti vyvážení ochrany údajů a svobody slova a je tu možnost zákonem stanovit řadu výjimek z práv subjektů údajů. Celkem existuje mezi 99 články Nařízení asi 30 míst, které po členských státech vyžadují nebo jim umožňují nějakou volbu nebo výjimku, nebo i vlastní úpravu.

Legislativní povinnosti dané novým Obecným nařízením musí členské státy EU aplikovat do května 2018 a upravit tyto oblasti:

* postavení akreditačních těles (které ověřují plnění pravidel pro nově zavedené „pečetě soukromí“ apod.)
* postavení dozorového orgánu, jeho nezávislost, jmenování předsedy apod.
* úprava dalších sankcí (včetně trestních)
* úprava svobody projevu ve vztahu k ochraně osobních údajů

V rámci implementace do národního práva umožňuje nové Obecné nařízení o ochraně osobních údajů upravit například následující legislativní oblasti nové úpravy:

* mírně specifikovat: zpracování některých citlivých údajů, rodné číslo, zaměstnanecké vztahy, pravomoci ÚOOÚ ve vztahu k mlčenlivosti (profesní, bankovní atd.)
* zvolit určitou variantu: věk dítěte pro on-line souhlas určit mezi 13-16 lety, rozšířit povinné pověřence ochrany dat i na další oblasti, omezení přenosů určitých dat do třetích zemí, pokuty pro veřejné instituce za porušení ochrany údajů
* stanovit výjimky z práv subjektu údajů v konkrétní oblasti (např. kvůli výběru daní, kvůli ochraně dalších osob, nebo kvůli právní jistotě – veřejné rejstříky apod.), nebo v oblasti archivů, vědeckého a historického zkoumání a statistik
* dále rozšiřovat nebo zpřísňovat úpravu: rozšíření povinnosti provádět konzultace s dozorovým orgánem, rozšířit povinné pověřence pro ochranu údajů, úplně zakázat přenosy dat do určitých zemí, rozšířit práva aktivistických organizací před soudem o žaloby na náhradu škody a o hromadné žaloby bez pověření zastupováním.

Implementace nového Obecného nařízení spadá do působnosti Ministerstva vnitra, pro jeho přípravu je při Úřadu vlády ČR vytvořena pracovní skupina sestávající ze zástupců Úřadu na ochranu osobních údajů, zástupců státní správy (ministerstva, úřady), profesních a zájmových organizací a soukromých subjektů.

Vzhledem k tomu, jak vysoký stupeň důležitosti dává EU ochraně osobních údajů, je nanejvýš vhodné se s novou právní úpravou seznámit a v případě, že organizace (správce, zpracovatel) je tímto novým nařízením dotčen, měl by se již nyní v dostatečném předstihu na změnu připravit. Je nutné upozornit na zvláště vysoké sankce v případě porušení pravidel správci a zpracovateli osobních údajů. Subjektům údajů, tedy fyzickým osobám, nové nařízení přinese silnější právní postavení a jistoty.

# Výhled do budoucna

*Co můžeme očekávat do budoucna, co mohou přinést nové technologie, zbavíme se dobrovolně svého soukromí?*

Je nesporné, že rozvoj informačních technologií, relativně levná výroba elektroniky, dostupnost datových služeb téměř kdekoliv ať již prostřednictvím kabelových sítí, sítí mobilních operátorů nebo jiných technologií, poskytovaných mnoha různými subjekty za relativně nízké poplatky nám dává téměř neuvěřitelné možnosti. Vyvíjí se nová miniaturní zařízení, vznikají nové služby. Zapnutí topení na dálku v domě prostřednictvím SMS a mobilního telefonu již považujeme téměř za zastaralou technologii.

Novým fenoménem se stal tzv. internet věcí, souhrn miniaturních, či větších, často jednoúčelových ale i složitých zařízení, například teploměrů, vypínačů osvětlení, automatických startérů, otvíračů dveří, různých ovladačů téměř čehokoliv, jednoúčelová „objednací“ tlačítka, inteligentních lednic, lokalizačních zařízení nebo třeba fitness náramků či osobní váhy, které jsou zpravidla bezdrátově (nebo i kabelem) připojena na internet a mohou tak být vzdáleně ovládána nebo odesílat nasbírané informace. Technologie nabírá neskutečnou rychlostí na obrátkách.

Téměř každý z nás nyní již používá bezdrátové platební karty využívající NFC komunikační čip pro zabezpečenou rádiovou komunikaci na krátkou vzdálenost. Částky do 500 Kč zaplatíte dotykem karty k platebnímu terminálu tak říkajíc mrknutím oka, vyšší částky „zdrží“ zadáním PIN. Do okamžiku, než takovou platební kartu ztratíte, je to velmi příjemný a rychlý platební nástroj.

Digitální domácnost je zde. Za necelých 20 USD si můžete zakoupit opravdu úhledný miniaturní prsten s vestavěnou bezdrátovou technologií NFC, která pro svou činnost nepotřebuje baterie. Budoucnost? Ne. Dotykem ruky se odemkne byt, zapne se televize, roztáhnou žaluzie. Stejně tak si můžete odemknout některé modely aut, motor se nastartuje, když do rukou uchopíte volant a ještě se přenastaví opěrka podle vašich preferencí. Pouhým uchopením se odemkne mobilní telefon, tablet nebo PC, dotykem se otevře turniket do zabezpečené oblasti v zaměstnání, některé typy umí fungovat jako platební karta. Použití nových technologií nám může výrazně zpříjemnit život.

V některých obchodech může mobilní telefon sloužit jako průvodce, detekuje pomocí rádiových signálů s malým dosahem, například pomocí technologie Bluetooth nebo NFC vaši přesnou polohu u konkrétního regálu a může nabízet konkrétní informace nebo cenové akce o produktech, které se nacházejí ve vaší blízkosti. Potřebujete znát parametry nové televize? Nabízí prodejce speciální cenu? Stačí se projít v blízkosti konkrétního produktu a informaci dostanete přímo na displej svého telefonu. A obchodník patrně informaci, že se o daný produkt zajímáte.

Od roku 2013 se v Česku testuje systém eCall, jehož primárním úkolem je automatizovaně asistovat při nehodě, v nouzi zavolat asistenci nebo záchranáře. Jedná se o doplněk vozu, soustavu počítače, telemetrického modulu, lokalizačního GPS modulu a modulu pro mobilní komunikaci doplněné reproduktorem a mikrofonem. Systém by se měl aktivovat až při nehodě v okamžiku nárazu, případně prostřednictvím tísňového tlačítka a spojit se tak s dispečinkem integrovaného záchranného systému, zaslat GPS souřadnice a předat informace o incidentu (síla nárazu, počet cestujících osob apod.). Jedná se o jakousi černou skříňku do auta. Pokud by systém měl fungovat tak, jak je nám předkládáno, jistě se jedná o chvályhodné řešení, které může pomoci v nouzi. Jsou zde ale také pochybnosti. Systém by měl být povinně montován do všech vozů vyrobených od roku 2017, termín se však již několikrát odsouval. Opravdu chceme mít povinně potenciálně sledovací zařízení ve svém voze? Nehrozí zneužití pro účely sledování a odposlechu v případě „potřeby“ od státních orgánů? Nehrozí zneužití a obdobné sledování a odposlechy od kriminálních živlů? Již nyní je známo několik případů sledování a odposlechů vozidel z USA pomocí bezpečnostních systémů „Connect Vehicle“ od Toyoty, nebo pomocí systému „OnStar“, který je montován do určitých typů vozů General Motors.

Dnes se téměř všichni pohybujeme po městě se zapnutými mobilními telefony, máme aktivovanou funkci pro zjišťování polohy podle satelitů GPS, Glonas nebo nového evropského systému Galileo, většinou nevypínáme komunikační prostředky WiFi, Bluetooth nebo NFC, vybíráme peníze elektronickými platebními kartami, platíme s nimi v navštívených obchodech, nakupujeme on-line v e-shopech nebo prostřednictvím SMS jízdenky na hromadnou dopravu. Při našem pohybu zanecháváme ve světě dostatečně silnou elektronickou stopu. Je možné nás, konkrétního jednotlivce lokalizovat, zjistit naše návyky? Upřímně si musíme odpovědět, že ano. Poskytujeme k tomu dobrovolně součinnost, využíváme zdarma mnoho těchto technologií, které nám dávají určitou přidanou hodnotu, zpříjemňují nám život. V naprosté většině případů se hromadně získaná data používají anonymně a sledují se podle ní trendy větších skupin lidí, nežli jednotlivců. Pokud by však někdo disponoval dostatečnými prostředky, nečiní problém sledovat a analyzovat chování jednotlivce (vzpomeňme profilování v případě nabízených reklam na internetu). Naši stopu můžeme velmi výrazně omezit vypínáním mobilů, placením hotovými penězi, využíváním alternativních identit. Chceme se sami dobrovolně v dnešním technologiemi protkaném světě omezovat? Svět kolem nás není sci-fi, je to realita, mnoho dříve nedostupných technických prostředků je dnes dostupných běžným uživatelům.

Není tedy lepší odpojit se od internetu, moderních komunikačních prostředků a pro jistotu vypnout elektřinu? To jistě ne. Ale musíme si položit otázku, zda nás nové moderní technologie našeho soukromí nezbavují? A nevzdáváme se svého vlastního soukromí dobrovolně? Na tuto otázku odpovídat nebudeme, ponecháme ji k zamyšlení každému jednotlivci. Buďme k našim informacím, k osobním údajům obezřetní, je to náš osobní majetek.

*Bible, Zjevení Janovo – 13. Kapitola, verše 16-18:
(16) A působí, aby všem, malým i velkým, bohatým i chudým,
 svobodným i otrokům, byl dán cejch na pravou ruku nebo na čelo
(17) a aby nikdo nemohl kupovat ani prodávat, leda ten,
 kdo má cejch: jméno šelmy nebo číslo jejího jména.
(18) Zde je moudrost. Kdo má rozum, ať spočte číslo té šelmy.
 Je to číslo člověka, a jeho číslo je šest set šedesát šest.*