**Bezpečnost jedince v digitální společnosti  
(praktický návod, jak si zachovat aspoň trochu soukromí)**

**Expertní skupina pro rozvoj systému iPodpora**

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

# Obsah

[Obsah 2](#_Toc512244733)

[1 Velký bratr včera a dnes 3](#_Toc512244734)

[2 Digitální stopa a metadata 3](#_Toc512244735)

[3 Nedáváme světu zbytečně mnoho dat sami? 3](#_Toc512244736)

[*4* Fenomén Facebook, Google+, Instagram a další 3](#_Toc512244737)

[5 Potenciální nebezpečí zneužití dat v digitálním světě 3](#_Toc512244738)

[*6* Ohrožená skupina – děti, mladiství, dospělí i senioři 3](#_Toc512244739)

[*7* Přineslo GDPR změnu ve sběru dat? 3](#_Toc512244740)

[8 Praktické kroky ke snížení digitální stopy 4](#_Toc512244741)

[9 Mysleme na budoucnost 4](#_Toc512244742)

# Velký bratr včera a dnes

*Firmy i instituce vždy měly větší či menší zájem vlastnit informace o zákaznících, partnerech, konkurenci nebo obecně o lidech.*

Sběr informací byl v dávné době, ale i dnes větším či menším zájmem každého jednotlivce, každé ekonomické skupiny, každého společenského nebo státního útvaru. V dřívějších dobách, kdy ještě nebyla k dispozici výkonná výpočetní technika a levné obrovské úložné kapacity, byl sběr těchto dat poměrně náročným úkolem, přičemž rozsah získávaných dat nebyl tak rozsáhlý jako dnes. Jednak nebyly k dispozici technické prostředky pro jejich získávání, ale hlavně nebylo technicky možné větší objemy získaných dat zpracovávat.

Dnes je situace oproti minulé době zcela jiná. Za zlomek dřívější ceny máme k dispozici výpočetní techniku obrovských výkonů, cena jednotky uložených dat se za posledních 20 let snížila 100 000 krát

**Cena 1 MB diskové kapacity v 1998: asi 60,00 Kč  
Cena 1 MB diskové kapacity v 2018: asi 0,0007 Kč**

Není pak výjimkou, že technologické firmy nabízejí na internetu zdarma 5 nebo 15 GB dat v cloudových řešeních (Google disk, Microsoft OneDrive, …). Pak začínáme chápat, proč nám technologické firmy nabízejí služby a prostor zdarma – analýza námi uložených dat přináší vyšší zisk, než je cena prostoru a přidružených služeb.



# Digitální stopa a metadata

*Téměř každý dnes používá od rána do večera digitální techniku, počítače, tablety, mobily ale i jiná zařízení, skoro vše komunikuje prostřednictvím internetu a vytváří tak určitá využitelná servisní data.*

Přemýšleli jste někdy nad tím, jakou jste zanechali ve světě digitální stopu na internetu? Schválně, zadejte do nějakého velkého vyhledávače celé své jméno (pro větší přesnost jej zadejte do uvozovek). Kolik odkazů bylo nalezeno a kolik se jich váže přímo k vaší osobě? Pokud denně užíváte internet, nakupujete v e-shopech nebo občas něco přidáte na Facebook, jistě odkazů nebude málo.

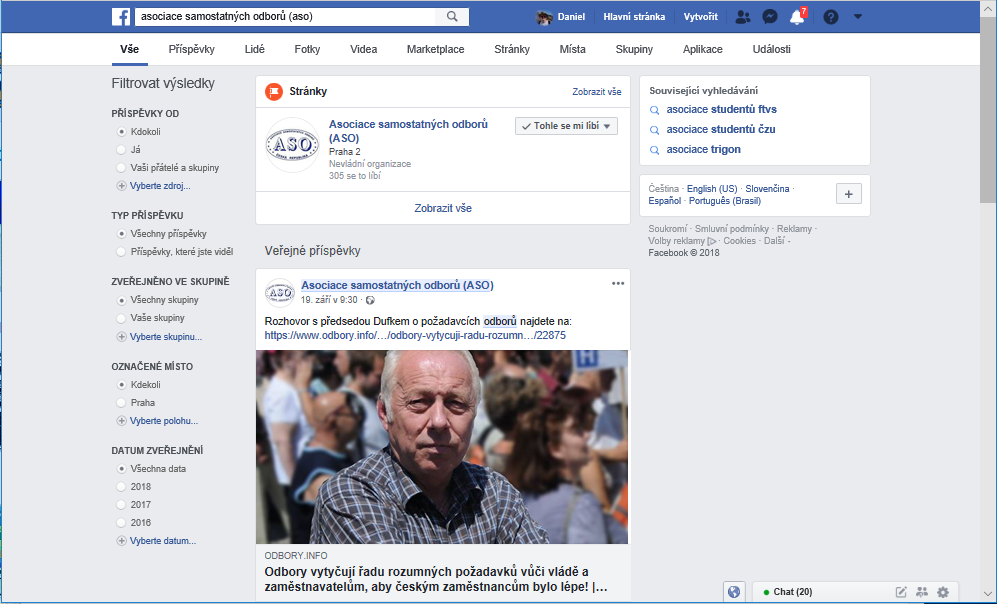
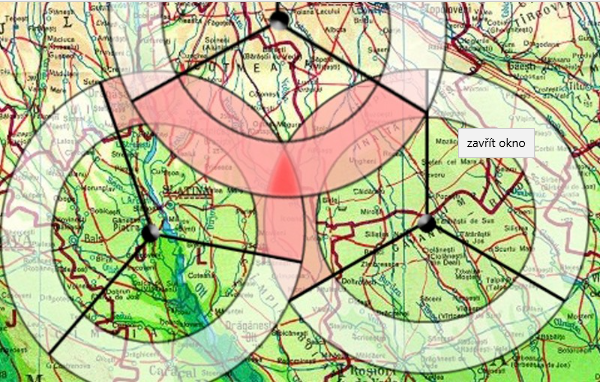
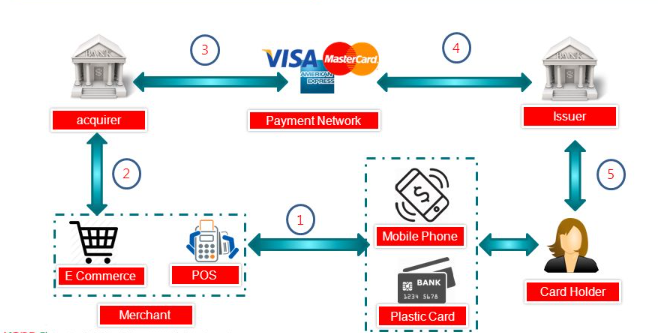
Co to však digitální stopa je? Ve své podstatě se jedná o jakoukoliv digitální informaci o naší činnosti, o našem každodenním životě. A zde je potřeba se zamyslet, jaké informace (v digitální formě) vlastně při běžné denní činnosti produkujeme.

Jedním typem informací jsou vlastní vložené nebo napsané texty, tabulky, čísla, fotografie, videa a další typy člověku běžně čitelných informací a pak zde máme mnoho dat popisných, které netvoří přímo vlastní obsah, ale jedná se o data spíše popisná, která určitým způsobem vlastní užitečná data popisují. Těmto popisným informacím říkáme metadata a jedním z historických příkladů může být katalogizační lístek v knihovně, který obsahoval údaje o konkrétní knize jako je například název, jméno autora, rok vydání, počet stran, umístění v knihovně. Informace mohou být opravdu rozličné.

Dnešní moderní digitální doba však užití metadat značně rozšířila a v počítačové oblasti se s nimi pracuje velmi široce. Metada vytváří náš digitální fotoaparát ke každému snímku a ukládá je skrytě uvnitř JPG nebo RAW souboru (většinou se využívá tzv. exif záznam obsahující např. název, datum a čas, typ fotoaparátu, nastavení času a clony, GPS souřadnice a mnoho dalších parametrů). Dalším příkladem mohou být metadata suborového systému na disku našeho počítače, který kromě vlastních „užitečných“ dat obsahuje další potřebné informace jako umístění souborů v sektorech disku, přístupová práva atd. Uživatelé hudby v MP3 formátu znají metadata popisující skladbu, její název, autora, vydavatele…

Obecně lze říci, že metadata popisují vlastní data nebo objekty. Těmi daty nejsou jen www stránky, obrázky nebo muzika. „Datovým“ objektem může být také naše platební karta, elektronická jízdenka, mobilní telefon, tablet, počítač nebo třeba i člověk. I člověk může být svým způsobem datový objekt, který je možné metadaty popsat.

Z našeho pohledu je důležité vědět, jak data a metadata vznikají:

1. **Aktivně vytvořené digitální informace** – ve své podstatě se jedná o vše, co aktivně sami vytvoříme, co sami napíšeme, vyfotografujeme a někam na internet vložíme. Jsou to informace, které zasíláme e-mailem (náš e-mail může skončit kdekoliv, to ovlivní jen příjemce, ne my), informace, které vkládáme na Facebook nebo do jiných sociálních sítí, ale třeba také poznámky vložené do chatů nebo texty zapsané do komentářů pod článkem na zpravodajském webu. Rovněž to mohou být různé registrace do e-shopů nebo zájmových webů. Fotografie umístěné na Instagram nebo do jiné fotogalerie. Zpráva pro nadřízeného nebo příkazy a informace podřízeným, které dnes častěji posíláme prostřednictvím počítače. Informace, které píše autor tohoto textu a který pak bude zveřejněn na internetu. Okruh informací, které sami vytváříme je obrovský a každý by našel další a další oblasti. Toto jsou informace, které jistým způsobem můžeme ovlivnit. Tvorbu těchto informací máme pod kontrolou. Zda máme kontrolu nad jejich dalším digitálním životem – o tom lze leckdy pochybovat.  
     
     
     
   *Sociální sítě jsou dnes patrně největším shromaždištěm a generátorem digitálních informací, které uživatelé na internet dobrovolně sami vkládají. Facebook obhospodařuje přes 2 miliardy uživatelů, WhatsApp užívá přes 1.3 miliardy uživatelů, Instagram má přes 700 milónů uživatelů. Toto obrovské množství lidí produkuje neskutečné množství dat, která se ve výpočetních centrech analyzují, hledají se trendy, zvyklosti, prodává se cílená reklama. Zatím hovoříme spíše o trendech než o jednotlivcích, ale výpočetní výkon roste…*
2. **Informace vytvářené pasivně bez našeho vědomí** – zde již vstupujeme na tenký led, jelikož není vždy zcela jasné, zda se tyto informace vytváří, či nikoliv. Žijeme v digitální době a zcela omezit užívání elektronických zařízení jako jsou počítače, mobilní telefony a podobně úplně nejde. Užití všech těchto zařízení způsobuje „někde na pozadí“ vytváření informací o jejich použití (a o nás). Náš počítač máme nejspíš připojený k internetu, takže o „něm“ jistě někdo ví, patrně poskytovatel internetu, nejspíš také tvůrce operačního systému, možná další softwareové firmy, jejichž programy používáme. Náš operátor mobilního telefonu ví, že jsme připojeni k jeho síti, že máme aktivní mobilní data, ví kde se nalézáme a to ani nemusíme telefonovat, stačí, když telefon máme v kapse. Všechny tyto informace vznikají technicky na pozadí v počítačových systémech, které vše kontrolují a řídí. Tuto digitální stopu vytváříme, aniž bychom se o to sami aktivně přičinili.  
     
     
     
   *Každý mobilní telefon je při svém provozu zaregistrován minimálně na jedné vysílací základnové stanici (tzv. BTS). Principiálně na základě zpoždění signálu je mobilní telefon zařazen do příslušného time-slotu, přičemž průsečíkem time-slotů můžeme relativně přesně určit polohu mobilního telefonu i s vypnutou GPS a mobilními daty. Přesnost se dle hustoty a počtu dostupných vysílačů a rozdělení signálu do sektorů pohybuje v řádu desítek až stovek metrů. Tyto lokalizační informace tvoří jednu skupinu metadat při používání mobilního telefonu.*
3. **Polo-aktivně vytvořené** – toto by mohla být patrně kombinace obojího výše uvedeného, tedy informace které sami vytváříme svojí aktivitou (kde nějakou datovou stopu předpokládáme), ale nejsme zcela přesvědčeni o tom, co tuto datovou stopu bude tvořit – typicky by mohlo jít o různé registrace pomocí počítače, přístupy k volným wifi sítím vyžadujícím vložení e-mailu, objednávky v e-shopech, „anonymní“ prohlížení webu, využití aktivní (on-line) navigace v autě, použití platebních karet, elektronických jízdenek, přístupových karet a mnoho dalších denně prováděných činností. Při použití platební karty, digitální jízdenky nebo přístupové karty nelze předpokládat, že by nějaké další informace nevznikaly. Taktéž náš bankovní dům, kromě toho, že ví kolik máme peněz, ví od koho přišla výplata, ví že svojí platební kartou zaplatíte za potraviny zpravidla ve stejném obchodě, ví že na oběd chodíte do restaurace na růžku, kde obvykle platíte kartou, ale také o vás ví, že jste jeli na dovolenou k moři a zaplatili zmrzlinu, protože prostě platit kartou je pohodlnější a bezpečnější než v kapse nosit hotovost. Dozajista České dráhy vědí, že autor tohoto textu jezdí do práce vlakem z místa A do místa B, protože se pravidelně prokazuje elektronickou kartou, kterou si průvodčí „odpípne“ na svém přenosném terminálu. Svojí činností určitou digitální stopu vytváříme, předpokládáme ji, ale nevíme, co ještě dalšího se „někde“ ukládá. Tuto oblast máme pod kontrolou jen částečně.  
     
     
     
   *Během platby kartou na platebním terminálu probíhá na pozadí čilá komunikace mezi několika subjekty (prodejce, zpracovatelská finanční instituce, vydavatel karty, banka zákazníka, kontrolní instituce atd.). Komunikace je šifrovaná, nicméně mimo vlastní platby se ukládá spousta pomocných informací.*

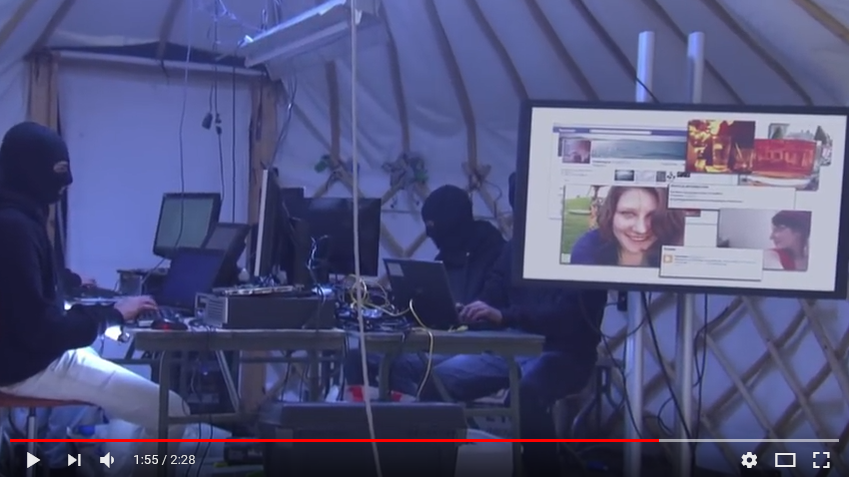
# Nedáváme světu zbytečně mnoho dat sami?

*V každodenním životě produkujeme, aniž bychom chtěli, mnoho využitelných dat. Obrovské množství konkrétních dat však sami světu poskytneme zcela vědomě. Je to správné?*

Hezký experiment nebo ukázku digitálních stop a možností jejich využití provedl v Bruselu Duval Guillaume, který se krom jiného zabývá právě digitální bezpečností – pozval pár náhodných lidí, kterým předváděl „věštění“ – překvapení dotčených osob o dovednostech věštce bylo značné, ale o to větší, když jim odhalil pravý zdroj informací, který mu do sluchátka předával tým pracovníků od počítačů, kteří v reálném čase spoustu informací zjistili z internetu z volně dostupných zdrojů:

  
*Náhodným osobám sděluje „věštec“ soukromé informace*

 *Po sdělení několika privátních, osobních informací je osobám odhalen způsob získání těchto údajů*

 *Tým počítačových odborníků během rozhovoru „věštce“ s vyhlédnutou náhodnou osobou vyhledává dostupné informace na internetu a předává je věštci do sluchátka. Všechny „věštěné“ skutečnosti pocházely z veřejných zdrojů, jak je o sobě sami jednotlivci na internetu uvedli.*

Celé video si můžete pustit na internetu z následující adresy:

[**https://youtu.be/F7pYHN9iC9I**](https://youtu.be/F7pYHN9iC9I)

Co na tomto experimentu bylo nejzajímavější? Všechna data byla získaná během chvilky prostřednictvím internetu z veřejných zdrojů, především ze sociálních médií nebo z veřejných inzertních serverů. Většinou si při psaní příspěvků na internet neuvědomujeme, jaký dosah může námi vložená informace mít. Tento experiment byl jen zábavnou hříčkou, zkuste se ale zamyslet nad tím, jaký dosah by mohlo mít zpracování uložených informací „nepřátelským“ subjektem, který by mohl disponovat přístupem k mnohem širšímu spektru dat, mohl by strojově porovnávat závislosti a propojení. Takový subjekt by nám minimálně mohl znepříjemnit život.

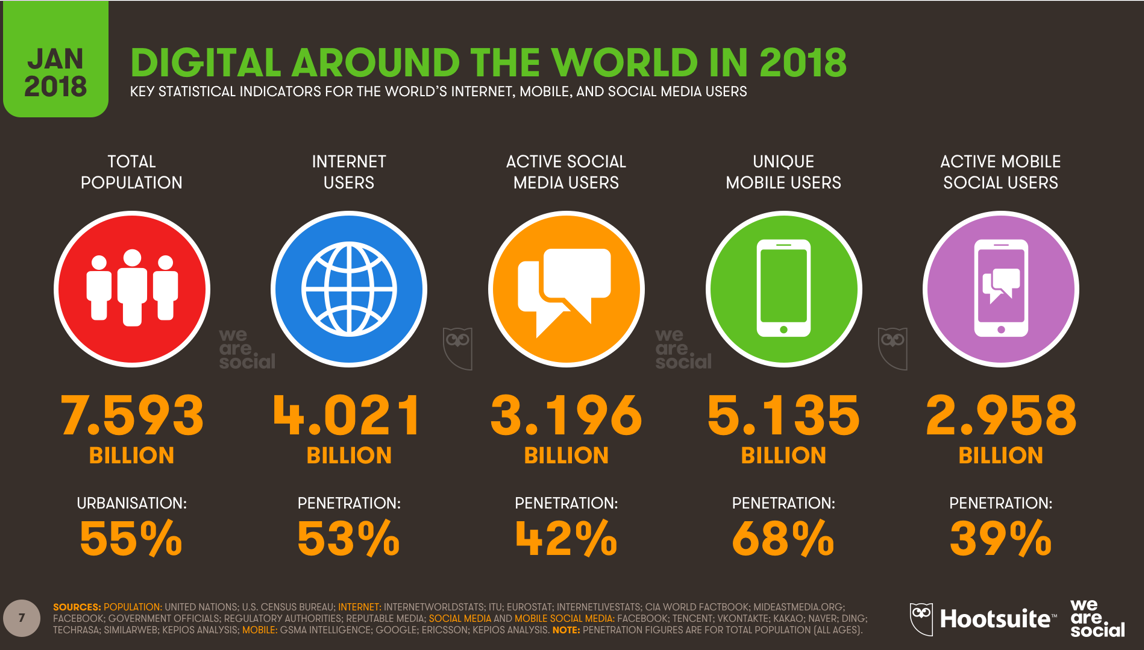
**Nezapomínejte – hlavním zdrojem informací, které na internetu o nás jsou k dispozici, jsme my sami a naši blízcí!**

# Fenomén Facebook a další sociální média

*Sociální sítě jsou velmi mocným nástrojem k získávání dat. Obrovské množství lidí jejich prostřednictvím sdílí skoro celý svůj soukromý život.*

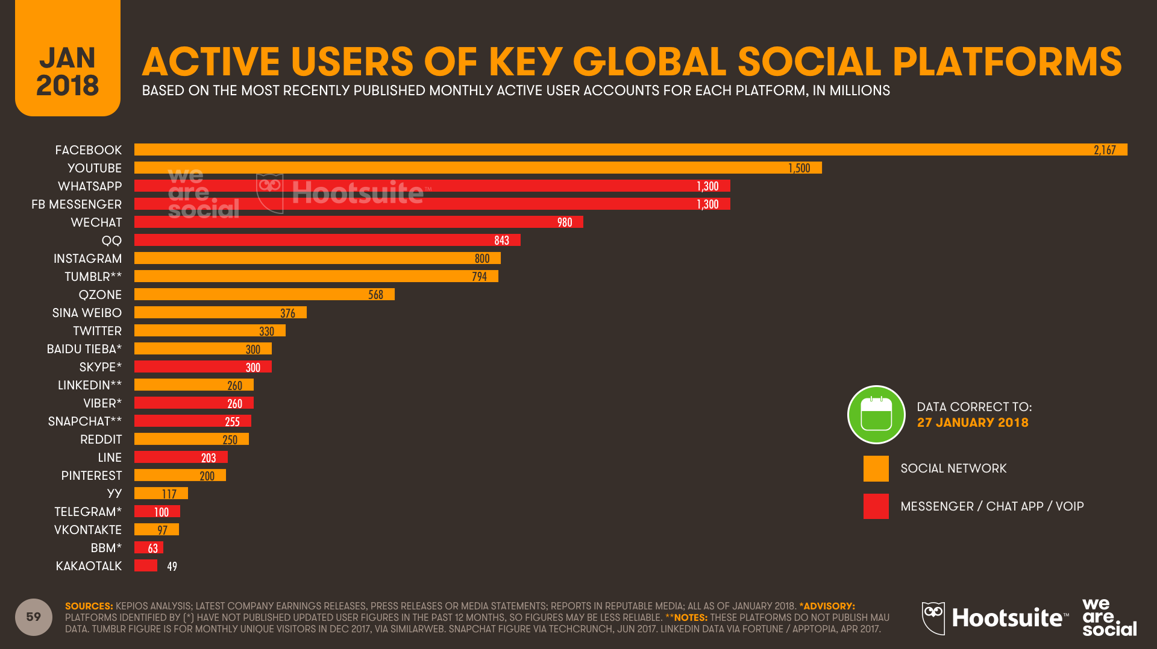
Na začátku roku 2018 bylo na Zemi více jak 7,5 miliardy lidí, přičemž více jak polovina světové populace používá ve svém životě internet. Sociální sítě využívá více jak 3 miliardy lidí, naprostá většina z nich pak k sociálním sítím přistupuje prostřednictvím mobilních telefonů. To je ohromné číslo, ohromný počet lidí.

Je zcela zjevné, že sociální sítě hýbou světem a internet již není pouze pro uživatele rozvinutých ekonomik. Internet je dnes široce dostupný téměř po celém světě a možnost připojení se neustále rozšiřuje především z důvodu nižší ceny za přenos a dále výrazným snížením ceny mobilních zařízení, které přinášejí internet do kapsy opravdu širokému spektru lidí. Výjimkami jsou dnes prakticky jen některé oblasti řízené autoritářskými režimy, ale i zde začíná být internet či obdoba místních sociálních sítí (i když silně cenzurovaná) k dispozici.

Trendem posledních let je pak čím dál tím větší příklon ve využívání sociálních sítí z mobilních zařízení, což bylo důsledkem především snižování ceny za GB mobilních dat, zvýšením užitných vlastností mobilních telefonů (zvětšení plochy displeje, navýšení výkonu, navýšení objemu úložné kapacity, zlepšení kvality fotoaparátů, dostupnost kvalitních aplikací pro přímou komunikaci s danou sociální platformou). V neposlední řadě tento rozmach způsobilo zavedení a rozšíření vysokorychlostního mobilního internetu, tedy rozvoj sítí 3 (3G) a 4 generace (LTE). Bez vysokorychlostního připojení by byl takový rozvoj nemyslitelný.   
  
  
*Z 3,2 miliardy aktivních uživatelů sociálních médií využívá ke komunikaci s těmi platformami mobilní zařízení téměř 3 miliardy uživatelů.*

Fenménem několika posledních let jsou především sociální sítě Facebook, platformy pro sdílení vidí YouTube, komunikační platformy WhatsApp, FB Messenger, WeChat nebo QQ, platformy pro sdílení fotografií Instagram, Thumblr a spousta dalších všeobecnýc, regionálních nebo specializovaných sociálních médií.

Téměř 30% světové populace, zahrnující nemluvňata, děti i osoby v pokročilém věku, používá Facebook. Mnoho z těchto uživatelů na Facebook (případně prostřednictvím dalších služeb) vkládá svoje příspěvky, nahrává svoje fotografie či videa.

  
*Počty aktivních uživatelů sociálních médií (žlutě sociální sítě, červeně komunikační platformy) - v miliónech*

Trocha statistických dat ohledně Facebooku pomůže chápat globální rozsah této sociální platformy:

* Ve 2Q 2018 má Facebook 2.23 miliardy aktivních uživatelů
* Ve 4Q 2016 měl Facebook 1.74 miliardy mobilních uživatelů
* Ve 4Q 2016 měl Facebook denně 1.15 miliardy aktivních mobilních uživatelů (*předchozí dva údaje jsou poslední oficiální data z 01/2017, novější jinde uváděné údaje jsou odhadovány*)
* 29,7% uživatelů tvoří lidé ve věkovém rozpětí 25 až 34 let
* Facebook užívá 76% žen a 66% mužů (*ze 100% žen a 100% mužů – agregované údaje z* [*https://www.brandwatch.com/2015/01/men-vs-women-active-social-media/*](https://www.brandwatch.com/2015/01/men-vs-women-active-social-media/))
* 50% 18-24 letých uživatelů po probuzení kontroluje Facebook
* Na Facebooku stráví každý uživatel v průměru 20 minut denně
* Odhaduje se, že na Facebooku je 83 miliónů falešných profilů
* Každou minutu je na Facebook vloženo 510 000 komentářů, 293 000 příspěvků a 136 000 fotografií

# Potenciální nebezpečí zneužití dat v digitálním světě

*Digitální svět zrychluje a zjednodušuje přenos informací, přenosové sítě jsou rychlé, datová úložiště obrovská, výpočetní výkon nadmíru dostatečný. Technologie zjednodušují možné využití či zneužití dat.*

Online vydírání se neliší od toho v reálném světě. Taktéž někdo někoho nutí, aby něco konal nebo trpěl – jen se liší v tom, že útočník neužije násilí, pohrůžku násilí nebo pohrůžku jiné těžké újmy, ale zejména pohrůžku zveřejnění citlivého materiálu.

Rizikovou skupinu v online vydírání nelze jasně definovat, neboť jeho obětí se může stát kdokoliv. V případě, že se obětí stane dítě, nebezpečí spočívá zejména v tom, že si často samo nedokáže poradit a ze studu či jiných důvodů pomoc u dospělého nehledá. Takový případ může skončit tragicky.

V případě, že se stane obětí dospělý člověk, rovněž často nehledá pomoc, neboť je povětšinou obětí tzv. sextortionu (vydírání využívající sexuálně explicitní materiály) a oznámení na Policii ČR jako druh pomoci vyloučí ze studu – před policistou, před partnerem apod.

Online vydírání lze teoreticky předcházet velice snadno – postačí nevkládat na internet žádné osobní údaje nebo osobní citlivé materiály v podobě fotografií nebo audiovizuálních nahrávek. Rovněž je třeba se vyvarovat sdělování osobních a intimních záležitostí – o to víc, pakliže komunikuji s osobou, kterou neznám osobně.

V praktickém pojetí se online vydíráni předchází hůře. Spousta uživatelů internetu plní své profily sociálních sítí materiálem osobního charakteru bez domyšlení, kdo všechno se k takto zveřejněnému materiálu může dostat. Navíc tyto profily často chrání velice slabými hesly a kybernetický predátor nemá složitou práci v tom, jak tyto citlivé materiály získat a užít ku svému účelu.

Několik základních pravidel, která bychom měli mít vždy na paměti:

* Dostatečně si chránit svoje profily  
   *- chránit přístupová jména a hesla k na sociální sítě, k emailové schránce apod.*
* Dodržovat základní pravidla bezpečného používání sociálních sítí

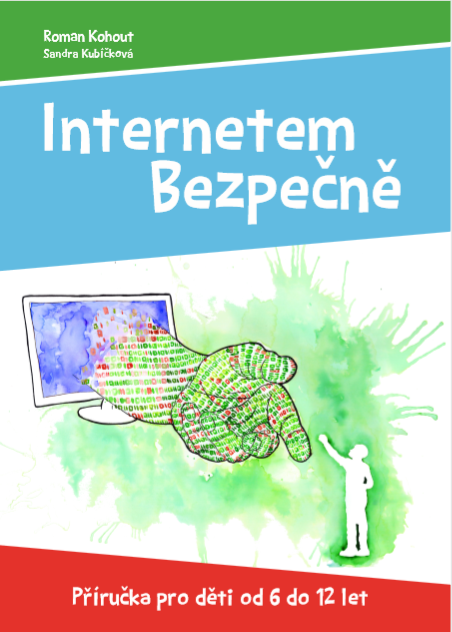
*- dvakrát se zamyslete nad informací, kterou na internet vkládáte*

* Být obezřetný při kontaktu s osobou, kterou neznáme v reálném životě  
  *- nezapomínejte, že za elektronickou identitou se může skrývat kdokoli i s nekalými úmysly. Rovněž nezapomínejte na to, že elektronická identita může být ukradená.*

# Ohrožená skupina – děti, mladiství, dospělí i senioři

*Digitální data dnes ve velkém neprodukují snad jen nemluvňata. Je na každém konkrétním jednotlivci, aby k informacím o sobě přistupoval zodpovědně.*

Žijeme v době, kdy je užívání internetu dětmi prakticky nevyhnutelné a znalosti dětí v oblasti informačních a komunikačních technologií často převyšují znalosti jejich rodičů. Mnozí rodiče vzhledem k této skutečnosti na ochranu svých dětí v online prostředí prakticky rezignují. Nechají své děti v online prostředí bez dozoru.

Naivita, důvěřivost, nekritické přejímání informací a nedostatek životních zkušeností však může být důvodem, že se dítě stane obětí virtuálních predátorů.

Ochraně těch nejzranitelnějších je však třeba věnovat mnohem více prostoru, než tomu bylo doposud. Je běžné slyšet rodiče, jak svému dítěti vštěpují do paměti, že staršího je třeba pozdravit, nebo že před přechodem pro chodce je nutné se rozhlédnout. Avšak není zcela běžné, že rodič obdobným způsobem vede dítě k bezpečnému chování v online prostředí.

Pro uživatele, kteří se chtějí blíže seznámit s pravidly bezpečného používání internetu a především sociálních sítí, jako je Facebook a další sociální média, doporučujeme navštívit web Internetem bezpečně na adrese:

[**https://www.internetembezpecne.cz/**](https://www.internetembezpecne.cz/)

Partnery tohoto chvályhodného projektu jsou Karlovarský kraj, velké komerční subjekty, ale také například Policie ČR nebo linka bezpečí. Ke stažení jsou na tomto místě i příručky jak pro dospělé, tak pro mladé uživatele internetu.

# Přinese GDPR změnu ve sběru dat?

*Nové nařízení Komise EU v oblasti ochrany osobních údajů zpřísňuje práci s osobními daty. Změní se ale ve skutečnosti něco?*

GDPR, General Data Protection Regulation nebo česky zkráceně Obecné nařízení o ochraně osobních údajů bylo hojně probíráno především v první polovině roku 2018, když se blížil termín jeho zavedení v platnost (25.5.2018). Hodně zjednodušeně jde o soubor definic, pravidel a nařízení pro nakládání s osobními daty jednotlivců, který měl, především v IT oblasti, značný dopad. A přesto, že se jedná o nařízení platné v rámci EU, museli se mu přizpůsobit i firmy z okolního světa, pokud na území EU chtěly poskytovat své služby.

Pravidla proto upravily i takové celosvětové gigantické firmy jako jsou společnosti Google, Facebook, Microsoft a další. Můžeme tedy předpokládat, že tyto společnosti opravdu ctí zásady ochrany osobních údajů a že se přímo nemusíme obávat jejich zneužití nebo k určitým typům zpracování musíme dát jednoznačný souhlas.

Nicméně je zde obrovské množství informací, kterými tyto velké korporace vládnou a je jen nezodpovězenou otázkou, jaké všechny operace jsou nad námi vloženými, případně naší činností vygenerovanými daty prováděny.

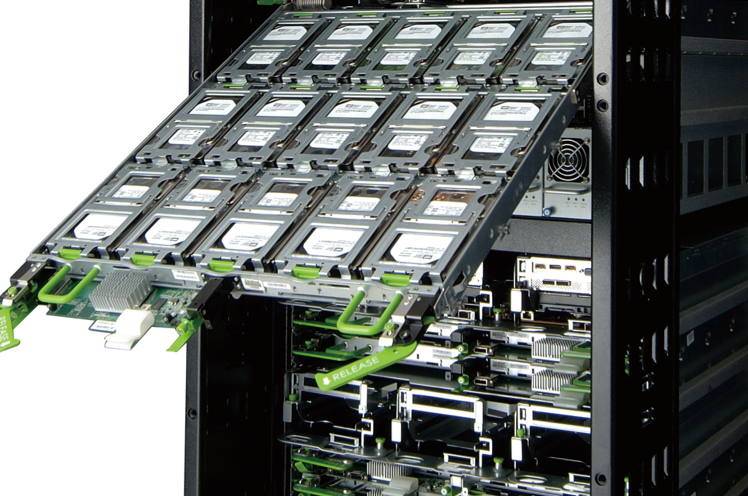
Vzhledem k tomu, že se zpravidla jedná o zpracování anonymizovaných dat, není toto zpracování jakýmkoliv způsobem regulováno. Kdo však vládne globálními informacemi, může ovládat globální obchod, může určitým způsobem ovládat globální myšlení. A stále nesmíme zapomínat na to, že žádná z globálních technologických firem není usazená v EU.

**15 EB (exa byte)**

Je odhadovaná kapacita redundantního úložného prostoru firmy Google – tedy asi 15 miliónů Gigabyte, použijeme-li poněkud představitelné jednotky. To vše ovládá asi 1.8-2.4 miliónu serverů

**Google jen jedním z mnoha…**

Odhadovaná globální nainstalovaná úložná kapacita v jednotlivých data-centrech po světě je v roce 2018 asi 750 EB, výhled do roku 2020 uvádí instalovanou globální kapacitu asi 2500 EB…



# Praktické kroky ke snížení digitální stopy

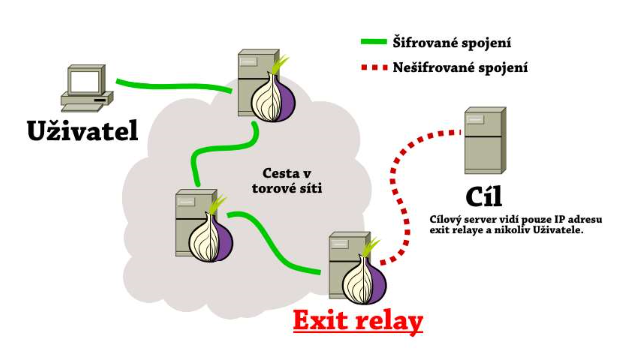
*Firmy i instituce se snaží sbírat digitální data o jednotlivcích, jak jen to jde, a jak je jim umožněno. Zabraňme jim v tom. Můžeme změnit své chování, můžeme používat speciální nástroje. Braňme si svoji svobodu. Aspoň trochu!*

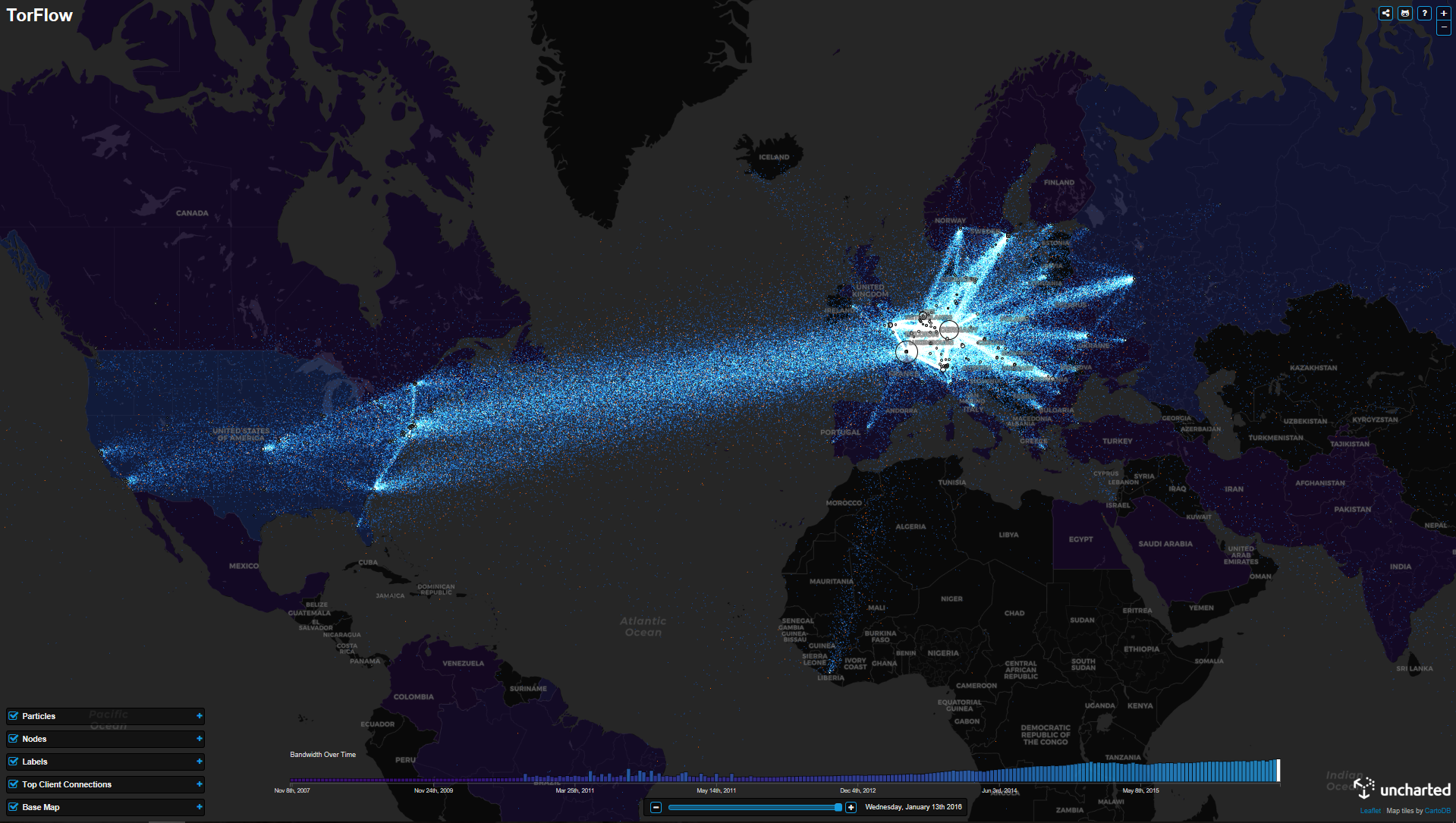
**Síť Freenet**

**Síť I2P**

**Síť TOR**

Síť TOR byla vytvořena jako neziskový projekt se záměrem umožnit jeho uživatelům pohybovat se po internetu anonymně, tedy bez toho, aby druhá strana (nebo kdokoliv na cestě dat) zjistil, kdo je konkrétním uživatelem. Pro skrytí identity, tedy technicky skrytí vaší IP adresy, se používá technika šifrovaného přenosu dat prostřednictvím vstupních bodů, přenosových uzlů a výstupních bodů. Koncový prvek (například www server) tedy ví že komunikuje s tzv. výstupním bodem, ale již je pro něj nezjistitelné, že původním žadatelem informace je váš PC.



  
Datový provoz na anonymní síti TOR

**Je síť TOR opravdu bezpečná?**

Částečně. Prvkem, který ohrožuje anonymitu internetového provozu na síti TOR jsou především výstupní uzly, v podstatě se mohou stát trojským koněm celého systému – výstupním bodem (tzv. „exit relay“) může jím být vlastně kdokoliv, kdo si spustí výstupní TOR server (který je k dispozici zdarma), tedy nejen bohulibý nadšenec snažící se zajistit skutečně bezpečnou a anonymní komunikaci, ale i hacker odposlouchávající vše co si s protistranou vyměňujete, včetně uživatelských jmen a hesel, případně přímo injektující do vaší komunikace škodlivý kód, který se může nainstalovat na PC. Úplně stejně takový výstupní TOR uzel může provozovat třeba i „tajná“ vládní agentura činící totéž výše uvedené. Vaše identita tedy může být odhalena skrze výstupní bod.

Dalším problémem je možnost odhalení komunikace a identity klientů a serverů v anonymizační síti TOR (míníme tím koncová zařízení, tedy například PC uživatele a nějaký koncový server poskytující data) prostřednictvím speciálních technik a zařízení na odposlech komunikace – pomocí tzv. snifferů – tzv. „confirmation attack“ nebo TC-attack. V tomto případě se naprosto jednoznačně jedná o státní instituce a tajné služby, protože je potřebná součinnost ISP (poskytovatelů internetu) z různých koutů světa a jen mocné státní, či spíše nadnárodní instituce mají moc si toto vynutit. Takto byly v minulosti odhaleny identity anonymních uživatelů sítě TOR prostřednictvím spolupráce FBI, Europolu a Eurojustice. Princip spočívá v porovnání datového paketu vstupujícího do sítě TOR (tedy u klienta, například v ČR) s paketem vystupujícím ze sítě TOR (tedy např. v USA u www serveru) – je tedy patrná nutná potřebná spolupráce a technologická komunikace napříč všemi možnými státy, což bylo v době návrhu a vzniku sítě TOR téměř nesmyslné sci-fi. V dnešním globálním světě s globálními operátory těžko některý z nich půjde přímo proti nařízení FBI či Eurojustice a odmítne instalaci takového zařízení.

**Existuje nějaké řešení?**

Jistou možnost dává zřetězení jednotlivých zabezpečovacích praktik. Nikdy se však nejedná o zcela bezpečné a zaručeně anonymní spojení. Podmínkou je, aby VPN bylo bezpečné, neukládalo záznamy o provozu (nelogovalo). Jenomže provozovatel VPN bude vždy také jen konkrétní člověk a když bude „vyzván“ ke spolupráci, jistě institucím jako je FBI, Europol nebo BIS příliš vzdorovat nebude. Nicméně celý řetězec komunikace je již velmi složité vysledovat a zatím tento způsob skrytí identity odolává. Naše doporučení, chcete-li na internetu skrýt svoji identit a „být v relativním bezpečí“ je tedy toto:

1. Na internet přistupujte přes veřejné WiFi přístupové body
2. Následně se do internetu připojte prostřednictvím „bezpečného“ šifrovaného VPN spojení
3. Poté, až přes VPN, se připojit do sítě TOR
4. Komunikujte pouze se zdroji využívající šifrovanou komunikaci (tedy šifrovaná SSL komunikace s weby https://, stejně tak šifrovaně pošta přes SSL/TLS atd.)

A ještě poznámka k „bezpečnému“ přístupovému VPN bodu – ten nejbezpečnější bude patrně ten váš vlastní a navíc takový, který bude těžko možné spárovat s vaší osobou. Tedy někde anonymně objednaný a anonymně placený…

**Fakta a informace (z druhé ruky):**

* Tor je bezpečná síť, ALE… za splnění určitých podmínek lze komunikaci de-anonymizovat
* Mnoho Tor výstupních bodů provozuje samotná NSA (USA) či GCHQ (UK)
* V roce 2014 FBI ve spolupráci s Europolem (za přispění NSA) vyřadila z provozu a zatkla více jak 400 provozovatelů serverů na „darknetu“ využitím techniky man-in-middle a TC-attack.
* Většina ISP sleduje provoz svých zákazníků

# Mysleme na budoucnost

*S každým klepnutím do klávesnice počítače, tabletu nebo mobilu si každý vytváří svoji jedinečnou digitální stopu. Ta může být prospěšná, ale zároveň může uškodit. Mějme to na paměti.*

Naším záměrem rozhodně není nabízet techniky a návody k napomáhání nebo přímo k páchání trestné činnosti. Myslíme si ale, že každý jednotlivý člověk má mít právo na svobodné informace, má mít právo na svobodnou a nemonitorovanou komunikaci, má mít právo vystupovat anonymně.

Dříve samozřejmě bylo také možné ze strany státních institucí (nebo i soukromých subjektů) určitým způsobem monitorovat vybrané jednotlivce, dnes je však díky rozvoji výkonné techniky a rychlého propojení celého světa internetem možné sledovat obrovské počty lidí naráz, a to bez zjevného zájmu veřejnosti, data o nás jsou sbírána i jen pro vytváření zisku ze zpracování těchto dat, a to bez našeho souhlasu (leckdy bez našeho vědomí). Naše komunikace, ať již e-mailová, přes www stránky nebo prostřednictvím sociálních sítí je velmi často analyzována buď z důvodu profilace (za účelem prodeje dat z marketingových důvodů, cílení reklamy apod.) nebo jen za účelem „prevence“ kriminality ze strany státních orgánů.

Je toto správná cesta? Nemyslíme si to. Chraňme si svoji soukromou komunikaci, svoji identitu, svoji anonymitu.

# Slovníček a zdroje

Darknet - speciální „neveřejný“ web skrytý pomocí technik jako je Freenet, I2P, Tor a dalších, obsahující jak informační weby, tak i eshopy s ilegálním zbožím

FBI - Federal Bureau of Investigation – Federální vyšetřovací úřad Ministerstva spravedlnosti USA

Freenet - Softwareový systém pro zajištění anonymizace uživatele na internetu

I2P - Softwareový systém pro zajištění anonymizace uživatele na internetu

ISP - internet service provider – poskytovatel internetových služeb

Node - „uzel“ – zpravidla označuje zařízení (PC), přes které prochází komunikace, na okrajích se využívají „entry“ (vstupní) a „exit“ (výstupní) uzly

NSA - National Security Agency – Národní bezpečnostní agentura USA

TOR - Softwareový systém pro zajištění anonymizace uživatele na internetu

We are social - <https://wearesocial.com/>