Úvod

Předkládaný kurz přispěje k vaší digitální zdatnosti v oblasti ochrany dat.

Témata kurzu:

- Co jsou to data
- Proč chránit svoje osobní údaje
- Obecné nařízení o ochraně osobních údajů (General Data Protection Regulatiom (GDPR)
- Hjak chránit své osobní údaje
- Big data
- Big data – jejich zneužívání
- Ochrana dat v podnikání

- Klíčová slova:

Data, osobní údaje, typy dat, soukromí, svoboda, ochrana dat, Obecné nařízení o ochraně osobních údajů, General Data Protection Regulation (GDPR), subjekt údajů, rodičovský souhlas, big data, marketing, internet věcí (Internet of Things /IoT), umělá inteligence (Artificial Intelligence/AI), zneužívání, špehování (surveillance), analýza chování (behavioral analytics), filtová bublina (filter bubble), dozvuková komora (echo chambre), manipulace, kmenovitost (tribalism), spirála ticha (spiral of silence), obchodní data, záloha (backup), ztráta dat, lidská chyba.

Data

Data je výraz pro údaje používané pro popis nějakého jevu nebo vlastnosti pozorovaného objektu. Data se získávají zápisem, měřením nebo pozorováním, vyjadřují skutečnost formálním způsobem tak, aby je bylo možno přenášet nebo zpracovat (např. počítačem). Z dat se vytvářejí informace a znalosti.

Data se shromažďují a analyzují s cílem vytvářet **informace** vhodné pro rozhodování, zatímco **znalosti** jsou odvozeny z rozsáhlého množství zkušeností, které se zabývají informacemi o předmětu. Například výška a poloha Mount Everestu jsou obecně známá data. Tato data mohou být obsažena v knize o Mount Everestu spolu s dalšími informacemi, na základě kterých lze rozhodnout, jak nejlépe na horu vylézt. Společně s využitím zkušeností o tom, jak se leze po horách, vzniká návod jak dosáhnout vrcholu Mount Everestu – to chápeme jako „znalost“.

Digitální data jsou souborem podvojných (binárních) hodnot jedniček (1) a nul (0) odlišných od analogových dat. V moderních počítačových systémech (po roce 1960) jsou veškerá data digitální.

Zdroj: Wikipedia

„Před tím, než napíšu své jméno na tabuli, potřebuji vědět, jak hodláte tyto údaje použít.“

Co jsou to osobní údaje?

Osobní data jsou veškeré informace o žijící osobě. **Osobní údaje** (anglicky Personal Data, Sensitive Personal Information) jsou takové informace, na základě kterých lze konkrétního žijícího člověka jednoznačně identifikovat.

Obvykle se za osobní údaje považují:

- jméno a příjmení
- státem vydané identifikační údaje (např. rodné číslo, číslo OP, číslo pasu, číslo řidičského průkazu atd.)
- pohlaví
- datum narození a věk
- osobní, rodinný stav
- telefonní číslo
- adresa bydliště
- e-mailová adresa
- IP adresa počítače (MAC adresa zařízení)
- základní biometrické údaje - otisk prstu, sítnice

Zvláštní skupinou jsou pak takzvané **citlivé osobní údaje**, které vypovídají o zdravotním stavu, genetických údajích, výši platu nebo například o politických názorech osoby. Mezi citlivé osobní údaje patří zejména :

- hesla, PIN, PUK
- zdravotní stav, sexuální orientace, národnost
- unikátní biologické rysy (otisk prstu, obraz sítnice, genetická charakteristika)
- výše příjmu, výše jmění
- bankovní údaje, údaje o pojištění

Zdroj: Managementmania.cz

Typy dat

Pozor!
Osobní údaje, které sice byly zbaveny informací umožňujících identifikaci, zašifrovány nebo pseudonymizovány, ale lze je použít ke zpětné identifikaci žijící osoby, zůstávají osobními údaji.

Naproti tomu osobní údaje, které byly anonymizovány takovým způsobem, že příslušná osoba již není identifikovatelná, již nejsou považovány za osobní údaje. Údaje se pokládají za skutečně anonymizované, pokud je anonymizace nezvratná.

Příklady údajů, které nejsou pokládány za osobní:

- registrační číslo společnosti,
- e-mailová adresa, jako je například info@firma.com,
- anonymizované údaje.

Zdroj: Evropská komise

Obecné nařízení na ochranu osobních údajů (GDPR)

Státy Evropské unie musí aktualizovat své zákony na ochranu osobních údajů v souladu s Obecným nařízením na ochranu osobních údajů (General Data Protection Regulation/GDPR), které je účinné od 25. května 2018. GDPR usiluje o vyšší transparentnost ochrany dat a rozšiřuje práva na ochranu soukromí s ohledem na osobní údaje.

Požadavky GDPR:

- Omezuje ukládání a využívání osobních údajů podnikatelskými subjekty bez výslovného souhlasu dotčených osob.
- Vyžaduje od společností, aby do 72 hodin upozornily všechny dotčené osoby a dohlížející orgány na únik osobních údajů.
- Firmy, které zpracovávají nebo monitorují data ve velkém, musí určit pracovníka odpovědného za dohled nad údaji a zajistit, aby společnost odpovídala předpisům GDPR.

Pokuty za porušení požadavků mohou dosáhnout výše 20 milionů Eur nebo 4 % celosvětového obratu firmy v minulém finančním období – v závislosti, co je vyšší.

Zdroj: Techtarget (anglicky)

Definice

Pro účely Obecného nařízení (GDPR) se rozumí:

1) "**osobními údaji**" veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen "**subjekt údajů**"); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby;

2) "**zpracováním**" jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení;

Zdroj: PRIVAZYplan

Obecné nařízení na ochranu osobních údajů (GDPR)

Zákonnost zpracování - čl.6 Obecného nařízení

Zpracování je zákonné, pouze pokud je splněna nejméně jedna z těchto podmínek a pouze v odpovídajícím rozsahu:

a) subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů;
b) zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů;
c) zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje;
d) zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby; …

Podmínky použitelné na souhlas dítěte v souvislosti se službami informační společnosti - čl.8 Obecného nařízení

Zpracování osobních údajů dítěte je zákonné, je-li dítě ve věku nejméně 16 let. Je-li dítě mladší 16 let, je takové zpracování zákonné pouze tehdy a do té míry, pokud byl tento souhlas vyjádřen nebo schválen osobou, která vykonává rodičovskou zodpovědnost k dítěti. Členské státy mohou pro uvedené účely právním předpisem stanovit nižší věk, ne však nižší než 13 let.

- *Pozn.: V České republice je v návrhu zákona stanovena věková hranice dítěte na 15 let*

Právo na výmaz ("právo být zapomenut") – čl. 17 Obecného nařízení

Subjekt údajů má právo na to, aby správce bez zbytečného odkladu vymazal osobní údaje, které se daného subjektu údajů týkají, a správce má povinnost osobní údaje bez zbytečného odkladu vymazat, pokud je dán jeden z těchto důvodů:

a) osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány;
b) subjekt údajů odvolá souhlas, na jehož základě byly údaje podle čl. 6 odst. 1 písm. a) nebo čl. 9 odst. 2 písm. a) zpracovány, a neexistuje žádný další právní důvod pro zpracování; ,
c) subjekt údajů vznese námitky proti zpracování podle čl. 21 odst. 1 a neexistují žádné převažující oprávněné důvody pro zpracování nebo subjekt údajů vznese námitky proti zpracování podle čl. 21 odst. 2;
d) osobní údaje byly zpracovány protiprávně; ..

Zdroj: PRIVAZYplan

Obecné nařízení na ochranu osobních údajů (GDPR)

GDPR zpřísňuje ochranu dětí!

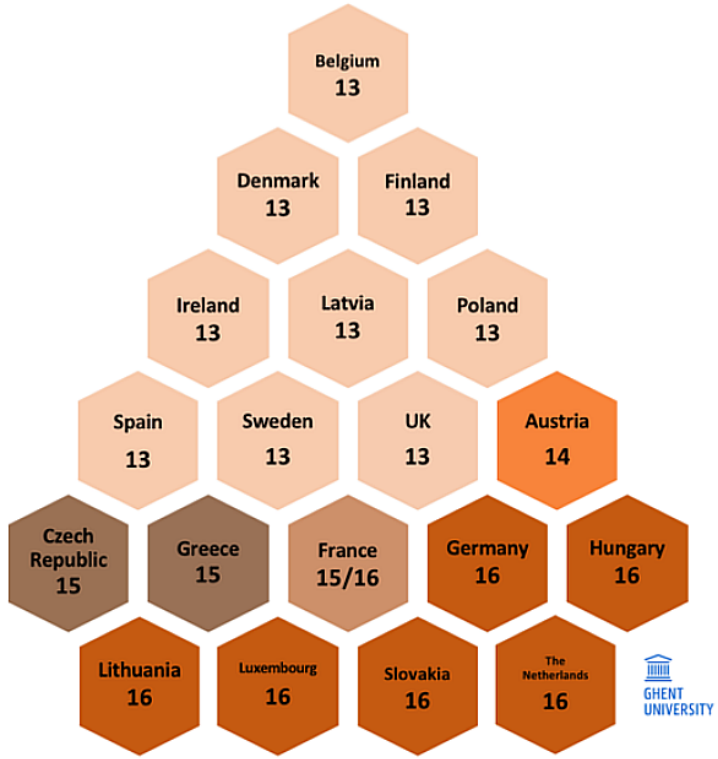
Podmínky použitelné na souhlas dítěte v souvislosti se službami informační společnosti - čl.8 Obecného nařízení

Zpracování osobních údajů dítěte je zákonné, je-li dítě ve věku nejméně 16 let. Je-li dítě mladší 16 let, je takové zpracování zákonné pouze tehdy a do té míry, pokud byl tento souhlas vyjádřen nebo schválen osobou, která vykonává rodičovskou zodpovědnost k dítěti. Členské státy mohou pro uvedené účely právním předpisem stanovit nižší věk, ne však nižší než 13 let.

Podmínky vyjádření souhlasu - čl.7 Obecného nařízení
Pokud je zpracování založeno na souhlasu, musí být správce schopen doložit, že subjekt údajů udělil souhlas se zpracováním svých osobních údajů.

Zdroj: PRIVAZYplan

V České republice je v návrhu zákona stanovena věková hranice dítěte na 15 let, věkové hranice v ostatních státech EU ukazuje obrázek:



Current provisional indications of age of consent across the EU

Zdroj: Betterinternetforkids.eu

Proč chránit své osobní údaje?

"Svoboda znamená právo na soukromí a jednání podle svého, dokud nepoškozujeme práva a soukromí ostatních"

Více: Orlando Patterson, NY Times

Jaká jsou vaše práva?

Pokaždé, když se připojujete k internetu sdílíte o sobě informace. Čím častěji na internet chodíte, tím důležitější je, abyste byli vy a vaše osobní údaje chráněny.

Máte právo:

- na **informace** o tom, jak jsou zpracovávány vaše osobní údaje,
- **získat přístup** k vašim osobním údajům, které má někdo v držení,
- požádat o **opravu** nesprávných, nepřesných nebo neúplných osobních údajů,
- požádat o **vymazání osobních údajů**, pokud již nejsou nutné nebo pokud je jejich zpracovávání nezákonné, …

Více se dozvíte na: EU Justice and Costumers

Pomněte:
*Když chráníte své osobní údaje, chráníte tím **své soukromí, svoji volnost a svobodu!***
Vaše osobní údaje jsou často prodávány, například když vytváříte svůj osobní účet na sociální síti, dáváte svůj souhlas poskytovateli služeb využít vaše osobní údaje pro marketingové účely.

Jak obchodníci na netu vědí, o co mám zájem? Video názorně ukazuje, odkud berou informace. Shlédněte na: YouTube (anglicky)

Jak chránit své osobní údaje?

Základní pravidla pro práci s osobními údaji

- Přemýšlejte a prověřujte, komu dáváte své údaje k dispozici.
- Zadávejte jen nutné minimum údajů.
- Pravidelně mažte cookies a historii vyhledávání ve svém internetovém prohlížeči
- Vytvořte si samostatnou e-mailovou adresu pro registrace do internetových služeb. Vyhnete se tak záplavě reklamních nabídek v e-mailu, který používáte pro běžnou komunikaci.
- Zvažte, zda opravdu chcete dostávat od každého e-shopu jeho reklamní nabídky. Ačkoliv se máte rozhodovat sami, obchodníci vám často tuto volbu „usnadní“ a souhlas zaškrtnou za vás. Nebojte se zaškrtnutí odstranit, pokud informační zprávy dostávat nechcete. Poměrně často totiž zároveň s tímto souhlasem poskytujete obchodníkovi svolení k předání vaší e-mailové adresy dalším osobám.
- Nepoužívejte slabá nebo lehce odhadnutelná hesla. Silné heslo nemusí být nutně složité k zapamatování – například heslo ArelYnekAcha, které vzniklo ze jména Karel Hynek Mácha vynecháním prvních písmen a mezer. Nepoužívejte ani stejné heslo pro všechny služby. Důležité služby jako internetové bankovnictví by měly mít složitostí odpovídající heslo!

Zdroj: Jak na internet

Ochrana osobních údajů
Zdroj: Jak na internet

Velká data (big data)

Velká data (anglicky Big data, česky někdy veledata) jsou podle jedné z možných definic soubory dat, jejichž velikost je mimo schopnosti zachycovat, spravovat a zpracovávat data běžně používanými softwarovými prostředky v rozumném čase.
Často bývá v textech na dané téma používáno i v češtině přímo big data jako pojem označující technickou kategorii, tedy bez překladu.

Zdroj: Wikipedie

V poslední době je termín "big data" spojován s využitím **prediktivní analýzy**, analýzy chování uživatelů (**behavior analytics**) a dalších pokročilých analytických metod, které extrahují hodnoty z dat nebo datových souborů s vymezeným obsahem. Zdroj: Wikipedia

Zdroj: Webopedia

Velká data a osobní údaje

Osobní údaje jsou údaje, které se týkají identifikovatelného žijícího jednotlivce. Mnoho příkladů analýzy velkých dat vůbec nezahrnuje osobní údaje. Používání údajů o klimatu a počasí by například mohlo umožnit nové objevy a vylepšené služby bez použití osobních údajů.
Existuje však mnoho příkladů analýzy velkých dat, které zahrnují zpracování osobních údajů ze zdrojů jako jsou sociální média, věrnostní karty a senzory v klinických studiích. Pokud se používají osobní údaje, musí organizace zajistit, aby dodržovaly své povinnosti vyplývající z platných právních předpisů o ochraně údajů.

Zdroj: Rada Evropy (anglicky)

Big data a marketing

Big data (velká data) jsou přesně tím, jak to zní: obrovské objemy údajů.

Zatímco velká data mohou mít různé typy zdrojů, odhaduje se, že většina z nich pochází z nestrukturovaných zdrojů. Jak je možné si představit, sociální média jsou možná největším zdrojem nestrukturovaných zdrojů pro velká data.

Lajky, tweety, názory, komentáře, oblíbené položky a vše ostatní, co mohou uživatelé dělat a komunikovat v jakékoliv platformě sociálních médií, mohou zainteresované strany shromažďovat a analyzovat.

Zdroj: TheNextWeb (anglicky)

Velká data jsou hnacím motorem každého marketingového rozhodnutí

Stejně jako každý jiný průmysl, společnosti sociálních médií považují velká data za užitečná pro analýzu trhů a předpovídání chování spotřebitelů. V roce 2012 Jay Parikh, viceprezident pro inženýrství na Facebooku, zjistil, že Facebook zpracovává **každý den** více než 500 terabajtů dat, 300 milionů fotografií denně, 2,6 miliardy "lajků" a 2,5 miliardy nahrávek obsahu. Všechna tato data jsou zpracovávána v pouhých minutách, které dávají Facebooku vhled na reakce uživatelů a schopnost rozvinout nebo upravit nabídku.

Zdroj: DataFloq (anglicky)

Big data – zneužívání

Internet věcí (Internet of Things/ IoT)

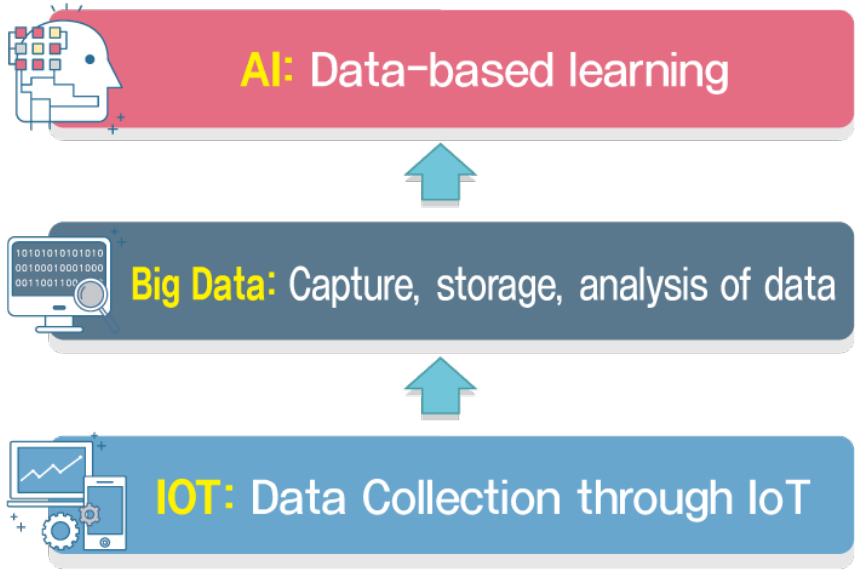
Forbes popisuje Internet věcí (IoT) jako koncept připojování veškerých přístrojů s vypínačem k **internetu** (a/nebo navzájem mezi sebou). Pokud má přístroj vypínač, může být pravděpodobně nastaven jako součást IoT.
Za přístroje chytré domácnosti (“smart home”) lze považovat zámek, který se odemyká, když detekuje přiblížení vašeho telefonu nebo třeba světla, která se rozsvítí, když detekují pohyb.
Prostřednictvím těchto chytrých („smart“) přístrojů lze sbírat data.

Velká data (Big Data) – velké soubory dat ze sociálních sítí, internetu věcí (IoT), apod.
Pojem velká data zahrnuje získávání, uchovávání a analýzu dat.

Umělá inteligence (Artificial intelligence/AI)

Podle slovníkové definice je umělá inteligence schopnost strojů napodobovat inteligentní chování lidí.
Například aplikace Alexa společnosti Amazon je příkladem umělé inteligence, která je schopná inteligentně odpovídat a mluvit lidským hlasem. Alexa je nyní přítomná ve více než 5 milionech domácností. Můžete se Alexy zeptat na počasí nebo ji požádat o objednání taxi, ona to zařídí. Znamená to, že umělá inteligence už dosáhla hromadného nasazení.

Zdroj: FPT Tech Insight



Source: FPT Tech Insight

V čem je problém?

Umělá inteligence spolu s IoT a využitím velkých dat umožňuje shromažďovat a vyhodnocovat údaje o chování každého člověka na zemi. Data mohou být a jsou často zneužívána bez vědomí lidí – jak uvádíme v následujícím slajdu :

Špehování – Analýza chování - Manipulace

Big data a špehování

Hromadný dohled (Mass surveillance)

Hromadný dohled je spletitý dohled nad celou nebo podstatnou částí populace za účelem sledování této skupiny občanů. Dohled často provádějí místní a federální vlády nebo vládní organizace, například organizace jako NSA a FBI, ale mohou být prováděny i korporacemi (jménem vlád nebo z vlastní iniciativy). V závislosti na právních předpisech a soudních systémech jednotlivých států se zákonnost a povolení vyžadované k provádění hromadného dozoru liší. Často se odlišuje od cíleného sledování.

Zdroj: Wikipedia (anglicky)

Dohledový kapitalismus (Surveillance capitalism)

Dohledový kapitalismu je nový druh kapitalismu, který zpeněžuje data získaná prostřednictvím sledování (slídění/šmírování). Podle akademičky Shoshany Zuboffové byl nejprve rozpoznán a konsolidován společností Google, která se pro dohledový kapitalismus stala tím, co před sto lety znamenal Ford a General Motors pro masovou výrobu a manažerský kapitalismus. Později byl převzat Facebookem a dalšími, kteří používají nečitelné mechanismy extrakce, modifikace a kontroly chování pro vytváření nových trhů založených na predikci a úprav chování.
Kapitalismus se tak soustředil na rozšíření podílu společenského života, který je otevřen sběru a zpracování dat. Může to mít významné důsledky pro zranitelnost a kontrolu společnosti, stejně jako pro soukromí. Zvýšený sběr dat však může mít pro jednotlivce i společnost různé výhody, jako je samooptimalizace (Quantified Self), společenská optimalizace (například inteligentní města) a nové nebo optimalizované služby (například různé aplikace Google). Přesto shromažďování a zpracování dat v kontextu vytváření zisku jako hlavního motivu kapitalismu může představovat neodmyslitelné nebezpečí.

Zdroj: Wikipedia (anglicky)

Pokud TY můžeš přečíst tento nápis, MY tě můžeme vidět

Big data – behaviorální analýza

Behaviorální analýza

Behaviorální analýza využívá obrovské objemy dat surových událostí uživatelů zaznamenaných během relací, kdy spotřebitelé používají aplikaci, hru nebo webové stránky. To vše včetně dopravních dat, jako je navigace, kliknutí, interakce na sociálních médiích, rozhodnutí o nákupu a reakce na marketing. Analýza chování **umožňuje prognózu budoucích akcí a trendů** na základě shromažďování těchto údajů. Zdoj: Wikipedia (anglicky)

Behaviorální analýza umožňuje personalizovat vyhledávání na webu.

Filtrační bublina

Filtrační bublina je stav intelektuální izolace, který může vyplývat z personalizovaných vyhledávání, když algoritmus webových stránek selektivně odhadne, jaké informace by uživatel chtěl vidět na základě informací o uživateli, jako je jeho umístění, minulé chování a historie vyhledávání. V důsledku toho jsou uživatelé oddělováni od informací, které nesouhlasí s jejich názory, a účinně je izolují do svých kulturních nebo ideologických bublin. Například výsledky amerických prezidentských voleb v roce 2016 byly spojeny s vlivem sociálních mediálních platforem, jako jsou Twitter a Facebook, a v důsledku toho vyvolaly otázky ohledně účinků fenoménu "filtrační bubliny" na podléhání uživatelů falešným zprávám a echo komorám.

Zdroj: Wikipedia (anglicky)

"Psychografická analýza" společnosti Cambridge analytica je ukázkou toho, jak mohou být lidé manipulováni na základě analýzy jejich dat.

Zdroj: Motherboard (angl.)

„Sociální média, která se snaží potěšit své uživatele, mohou uživatelům přisouvat informace, o kterých se domnívají, že je budou rádi slyšet, ale neúmyslně tak separují to co vědí do jejich vlastních filtračních bublin." *Eli Pariser, **TED 2011** (anglicky)*

Big data – manipulace

Ozvěnová komora (Echo chambre)
Vaše osobní údaje jsou shromažďovány, analyzovány a filtrovány / zneužity, aby se vytvořila sociální/filtrovací bublina. Echo komora přichází, aby ovládala vaší mysl:

Termín echo komora je metaforickým popisem situace, ve které je víra lidí posilována nebo násobena komunikací a opakováním uvnitř uzavřeného systému, v němž lidé mají potřebu hledat informace, které upevňují jejich stávající názory. To může zvýšit politickou a sociální polarizaci a extremismus. V extrémní "ozvěnové komoře" (echo chamber) si jeden poskytovatel informací vytvoří tvrzení, které pak mnozí podobně smýšlející lidé opakují, poslouchají a znovu opakují (často v přehnané nebo jinak zkreslené podobě), dokud většina lidí nepředpokládá, že poněkud extrémní varianta příběhu je pravdivá. Další nově vznikajícím pojmem pro tento **efekt opakování a homogenizace** na internetu v rámci společenských komunit je **kulturní tribalismus**.

Zdroj: Wikipedia

"Thanks. Great political discussion."

Ozvěna.
„Díky. Skvělá politická diskuze.“

Tribalismus
Tribalismus je stav, kdy se člověk cítí být příslušníkem nebo přívržencem kmene (kmen anglicky: „tribe“). Tribalismus označuje způsob myšlení nebo chování, ve kterém jsou lidé věrní své společenské skupině.
Lidé jsou sociální zvířata špatně vybavená, aby mohla žít osamoceně. Tribalismus a společenská vazba pomáhají udržovat jednotlivce ve skupině, i za cenu rozvrácení osobních vztahů. To znemožňuje jednotlivcům odejít, nebo připojit se k jiným skupinám. To také vede k šikanování, když člen kmene není ochotný přizpůsobit se zájmům kolektivu.

Zdroj: Wikipedia

Spirála ticha
Teorie masové komunikace, která stanoví, že jednotlivci mají strach z izolace, což vyplývá z myšlenky, že sociální skupina nebo společnost obecně by mohla izolovat, zanedbávat nebo vyloučit členy kvůli jejich názorům. Tento strach z izolace vede následně k tomu, že lidé mlčí, místo aby své názory vyslovili. Média jsou důležitým faktorem, který se vztahuje jak na dominantní myšlenku, tak na její vnímání lidmi.

Zdroj: Wikipedia

Ochrana dat v byznysu

Lidská chyba hraje významnou roli při ztrátě dat, podle nedávného výzkumu ji zaviní ve 32% případů. Co zbývajících 68 procent?
Mezi nejčastější příčiny patří porucha hardwaru, poškození softwaru, škodlivý software a úskoky matky přírody (přírodní katastrofy, požáry).

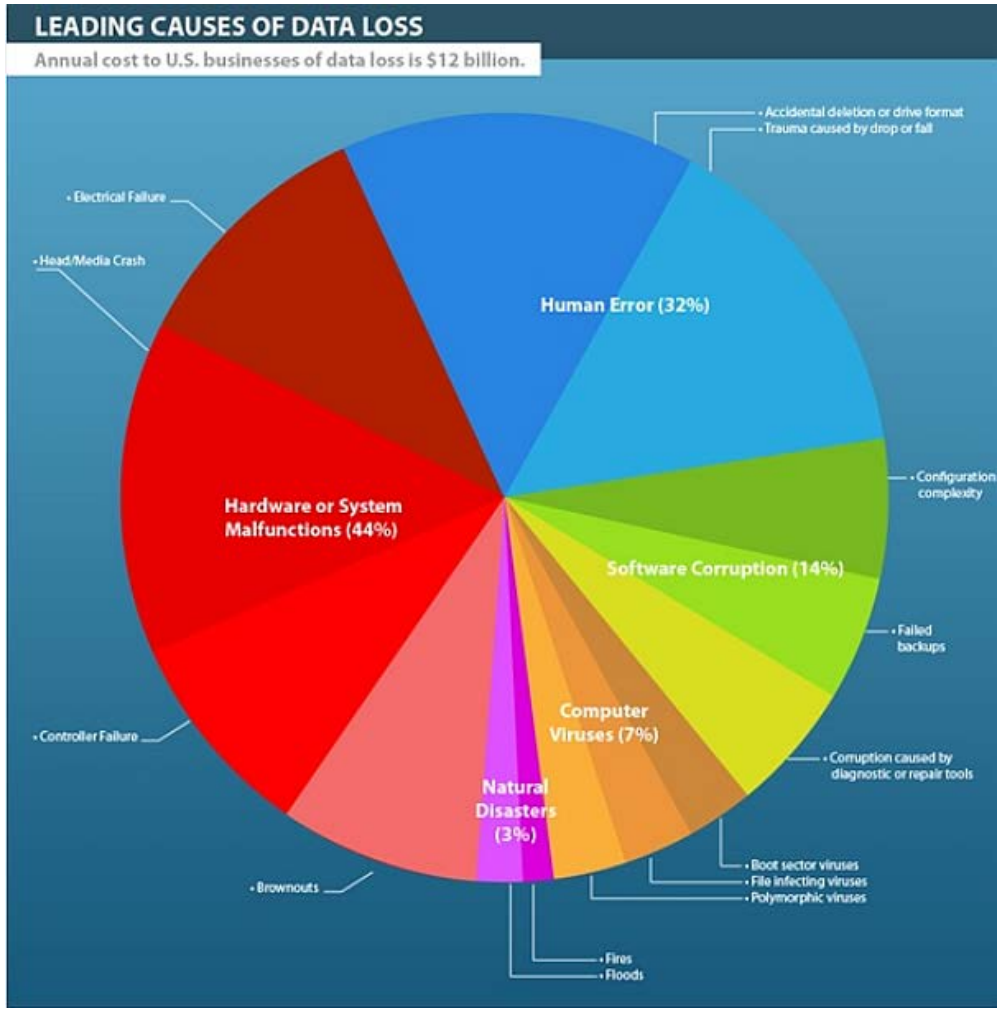
Hlavní příčiny ztráty dat uvedené v grafu:

1. *Výpadek hardware nebo systému (44 % případů)*
2. *Lidská chyba (32 %)*
3. *Poškozený software (14 %)*
4. *Počítačový virus (7 %)*
5. *Přírodní katastrofy (3 %)*

Odhad ročních ztrát firem v USA zaviněné ztrátou dat: 12 miliard USD

- *Firmy, které utrpí výpadek počítače na déle jak 10 dní nikdy plně neobnoví svoji finanční kapacitu,*
- *Ze 350 podniků, které působily ve Světovém obchodním centru před bombovým útokem v roce 1993, bylo o rok později 150 podniků mimo byznys.*

Zdroj: Dell



Praktické úlohy

Nechte se překvapit!

Chcete se dozvědět jaké OSOBNÍ ÚDAJE o vás sbírají sociální sítě?

- Zeptejte se Facebooku ZDE:

Přístup a stahování vašich informací na Facebooku
https://www.facebook.com/help/contact/166828260073047

- Googlu se můžete zeptat ZDE:

Export kopie dat: google.com/takeout

Chcete vědět více?
Něco o DataSelfie?
Mrkněte se na Tyinternety.cz !

(https://tyinternety.cz/digital/data-selfie-zjistete-zaklad-toho-co-o-vas-vi-facebook/)