VELKÝ BRATR
tě hlídá

Naše data jsou cennou surovinou – bohužel ale také otevřenou knihou pro zpravodajské agentury a softwarové giganty, jako například Google.

CLAUDIO MÜLLER

FOTO: NIKOLAUS SCHÄFFLER

KDO MÁ VAŠE DATA?

Téměř každý shromažďuje neosobní metadata. Ta ale mohou být použita k vytvoření konkrétního osobního profilu.

	Stát (úřady, zpravodajské služby)	Poskytovatelé (internet, mobilní telefon)	Webové služby (Google, Facebook)	Webové stránky (např. zprav. servery)	Datové trackery (reklama)	Softwarové firmy
OSOBNÍ ÚDAJE						
Jméno	●	●	●			●
Datum narození	●	●				
Adresa	●	●				
Účet/číslo kreditní karty	●	●	●			●
E-Mail	●	●	●			●
Telefonní číslo	●	●	●			●
Připojení k internetu		●				
Národnost	●					
Platební neschopnost	●					
Policejní záznam	●					
Přestupky	●					
Stěhování	●					
METADATA						
IP Adresa	●	●	●	●	●	
Autorizační údaje (tel. číslo, e-mail)	●	●				
Informace o surfování (www stránky)			●	●	●	
Verze softwaru (browser, OS, doplňky)			●	●	●	
Diagnostická data z programů						●
Údaje o poloze	●		●		●	●
Identifikační číslo zařízení	●	●				●
Systémový jazyk, časové pásmo, fonty			●	●	●	
Rozlišení obrazovky, barevná hloubka			●	●	●	
Velikost okna prohlížeče			●	●	●	
Nainstalované doplňky			●	●	●	
OBSAH DAT						
Vyhledávání			●	●		
Obsah e-mailů/chatu/SMS	●	●	●			
Záznamy hovorů	●		●			●
Kontakty	●		●			●
Fotografie, videa	●		●			●
Přátelé, rodina	●		●			●
Zájmy			●	●	●	
Navštívené weby	●	●	●		●	●
Pracovní záznamy	●		●			
Webové účty			●			
Oblíbení záložky			●			
Kalendář akcí			●			
Nainstalované aplikace			●			

Volný přístup k informacím, čtyřiadvacetihodinové nakupování, nové formy komunikace a zábavy – výhody internetu jsou tak rozmanité, že si je nelze nechat ujít, zčásti i proto, že jsou prakticky zadarmo. Internetové společnosti, jako je například Google, přesto vydělávají miliardy. Jak to dělají? Snadno, pomocí informací – informací o nás. Také zpravodajské služby (klíčové slovo je zde Prism) pilně sbírají digitální stopy, které po sobě denně zanecháváme.

Přehled v levé části stránky ukazuje, kdo všechno může o nás získávat data a o jaké typy dat se jedná. Co se týče sběru dat, nejjednodušší to mají provozovatelé webových stránek, kteří snadno zachytí každé kliknutí a každé vložení textu. Na základě údajů, které lze získat pomocí záznamu navštívených webů a zadaných údajů, pak někteří velcí poskytovatelé obsahu (například Google, Amazon nebo Facebook) dokážou odhalit i poměrně citlivé osobní informace, týkající se soukromých zálib nebo osobních vztahů. Reklamní služby, které jsou aktivní na mnoha internetových stránkách, mohou navíc pomocí metadat vytvořit rozsáhlé profily (viz článek V síti datových dealerů v Chipu 4/2013). Situaci také zhoršují klasičtí dealeři dat, kteří sbírají off-line data, jako jsou jména a adresy, a tyto údaje posléze prodávají k reklamním účelům. Není asi žádným překvapením, že naprostá většina lidí má alespoň jednu věrnostní kartičku obchodu či obchodního řetězce a při jejím získání dobrovolně firmě poskytla své údaje pro předání subjektům třetí strany pro marketingové účely.

Z hlediska podílu informací, které se mohou týkat věcí, jako je naše využití času, nebo dokonce i dat o naší poloze, si na své přijde i klasický software a poskytovatelé aplikací.

Pro spotřebitele je ale obvykle velmi obtížné zjistit, kdo data sbírá, jaká data se o něm shromažďují a k čemu se používají. IT giganty samy sebe rády líčí jako přátele uživatelů, ale jakmile jsme začali klást otázky týkající se využití dat, jejich zástupci nás prostě jen odkázali na jejich právní předpisy ohledně ochrany dat. Některé části těchto předpisů však nemůže nikdo, kdo není advokát, pochopit, a jakmile dojde na důležité otázky, předpisy jsou často velmi vágní. Klasickou odpovědí například bylo: „Osobní data jsou k dispozici našim pobočkám a dalším důvěryhodným firmám či osobám, které zpracovávají údaje naším jménem […].“

To je skvělé, ale kdo přesně jsou tyto společnosti a osoby? Tento konkrétní příklad slovního vyjádření je součástí prohlášení o ochraně soukromí dat Googlu (Google's data privacy statement), mnoho jiných společností ho ale používá také.

Pokud však chcete zjistit, jak konkrétně se data zpracovávají, nedělejte si iluzi o tom, že by vám někdo něco prozradil. Některé státy (jako například Německo) sice mají zákony, které nutí firmy tyto informace poskytnout (Spolkový zákon o ochraně dat – BDSG), to se ale týká pouze německých firem. U zahraničních firem neexistuje žádná záruka, že budete mít možnost získat informace, které požadujete. Zde se totiž objevuje zásadní problém spojený s oblastí ochrany údajů. Jak by vnitrostátní právní předpisy měly regulovat přenos dat do zahraničí?

Většina laiků netuší, že v tomto případě platí právní předpisy svázané se zemí, ve které sídlí firma poskytující danou službu. A asi nikoho nepřekvapí, že si firmy s obchodem založeným na získávání informací vybírají za sídla země, ve kterých jsou zákony na ochranu osobních informací korektně řečeno poněkud volnější. To je důvod, proč má například Facebook sídlo v Irsku. Důležité je také zmínit, že tyto informace obvykle člověk může zjistit (ve více či méně skryté formě) při vytváření účtu u služby a čtení licenčních podmínek. Naprostá většina lidí však tento dialog jen odklikne nebo přidá zatržítko u položky „Souhlasím“. Ještě komplikovanější právní situace je kolem získávání a shromažďování dat vládními agenturami. Teoreticky pro ně také platí zákony, obvykle jsou ale zároveň předmětem zvláštních právních předpisů.

Nejdřív sbírejte, pak se teprve ptejte

Tyto zákony nicméně nedokážou zabrzdit globální tok informací. V optických vláknech v silných kabelech denně protékají miliony gigabajtů dat, která se shromažďují v obrovských datových centrech.

Aby firmy a organizace dokázaly porozumět tomu, co toto obrovské množství dat může odhalit, musí data nejprve analyzovat. V tom vynikají již několik let především velké internetové společnosti. Například Google analyzuje požadavky na vyhledávání a používá Google Instant pro dokončení vyhledávacích dotazů, nabízející nejpravděpodobnější možné výrazy pro vyhledávání. Poté zobrazí výsledky hledání odpovídající požadavkům uživatele, s přihlédnutím k jeho profilu a například i poloze – přičemž vše se děje v reálném čase.

Amazon již roky analyzuje naše nákupní chování a přichází se stále přesnějšími doporučeními, co byste si ještě rádi koupili.

Policie využívá informace o trestné činnosti, která již byla spáchána, aby byla schopna předpovědět, kde a kdy se s největší pravděpodobností stane další zločin. Tato technika se již nějakou dobu používá v amerických městech, jako je Los Angeles a Seattle. Zpravodajské služby a protiteroristické jednotky vkládají svou víru do analýzy velkého množství dat, aby mohly co nejdříve identifikovat potenciální teroristy.

Jakmile ale dojde na předpovědi, samostatné údaje samy o sobě bohužel nestačí. Ty je nutné kombinovat s profily uživatelů. A aby bylo možné rozpoznat uživatele, tj. aby se data mohla určitou dobu shromažďovat tak, aby vytvořila profil, je nutné získat o uživateli co nejvíce údajů – například z cookies, které webové stránky ukládají do počítače uživatele. I pokud se snažíte cookies navštívených stránek mazat, lze o vás získat velké množství informací – například pomocí všudypřítomných reklamních bannerů a využití cookies nové generace (tzv. flash cookies). Tato data pak v kombinaci s dalšími údaji (například doplňky prohlížeče, nastavením systému...) vytváří jedinečný otisk prstu, který dokáže uživatele identifikovat. O tom se můžete přesvědčit například na webu **panopticlick.eff.org**, kde lze získat i základní informace o tom, z jakých informací lze váš webový „otisk prstu“ vytvořit.

Metody používané v off-line světě mohou být méně technologicky pokročilé, přesto to ale neznamená, že jsou méně účinné. Pomocí kombinací veřejně dostupných informací a dat zakoupených od různých reklamních firem lze získat poměrně přesný profil uživatele, obsahující kromě adresy, e-mailu a telefonu také věk a pohlaví, případně nákupní preference. Tyto balíky dat označované jako „leads“ lze pak snadno pomocí zadaných kritérií filtrovat a výsledná data prodávat zájemcům – například pojišťovacím firmám nebo mobilním operátorům.

V některých zemích je ale z důvodu volnějších zákonů situace ještě horší – typickým příkladem jsou USA, kde se kvůli relativně slabým zákonům o ochraně soukromých dat s těmito citlivými informacemi čile obchoduje. Například americká společnost LeadsPlease prodává seznamy e-mailových adres za neuvěřitelnou cenu: 1 000 adres stojí jen 85 dolarů. A co víc, subjekt, který si objedná 50 000 adres, získá slevu ve výši více než 40 procent. Kromě jmen a adres tyto datové soubory/sady obsahují více než dvě desítky dalších informací, například kvalifikovaný odhad týkající se ročních příjmů osoby či údaje o tom, zda dotyčná osoba je či není milovníkem zvířat. A to jde pouze o oficiální a legálně získané informace. Dokážete si představit, jak důkladné profily mohou mít zpravodajské organizace, pokud tato data propojí s těmi získanými pololegální cestou?

Digitální a analogové informace

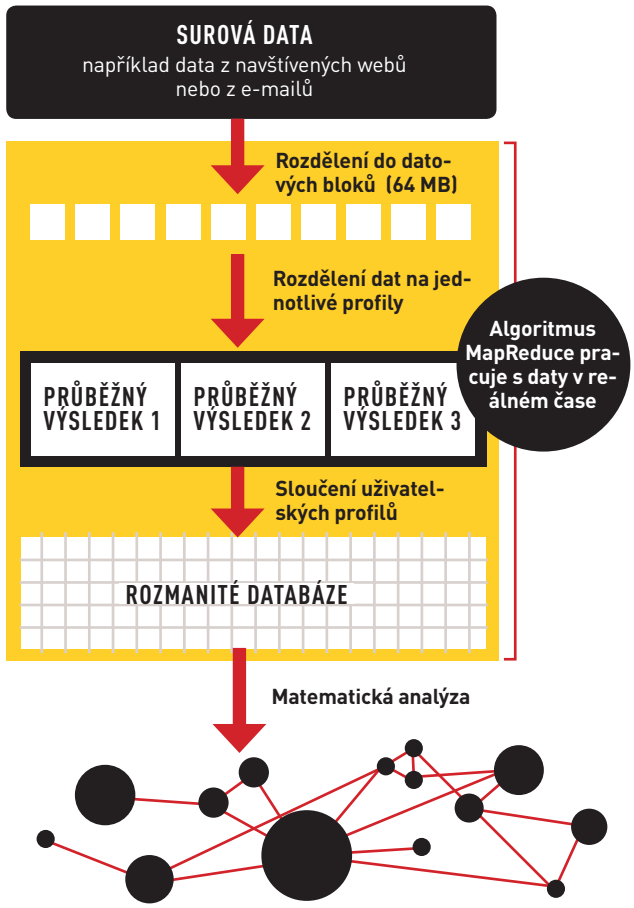
Co je z hlediska uživatele nepříjemné (ale pro firmy z hlediska analýzy velmi zajímavé), to je propojení on-line i off-line dat. Jedním z průkopníků této činnosti je americká společnost Acxiom, působící také například v sousedním Německu. Podle vlastních prohlášení má Acxiom k dispozici až 1 500 údajů o více než 500 milionech spotřebitelích po celém světě.

Tento balík dat je obrovský i proto, že společnost kombinuje (i desítky let staré) off-line databáze s údaji, které jsou shromažďovány z více než 75 000 internetových stránek. Off-line data obvykle pochází od reklamních společností, medicínských firem nebo vydavatelů. Za zmínku rozhodně stojí, že historie této firmy v Evropě sahá až do roku 1962, kdy firma vytvořila první fond ad-

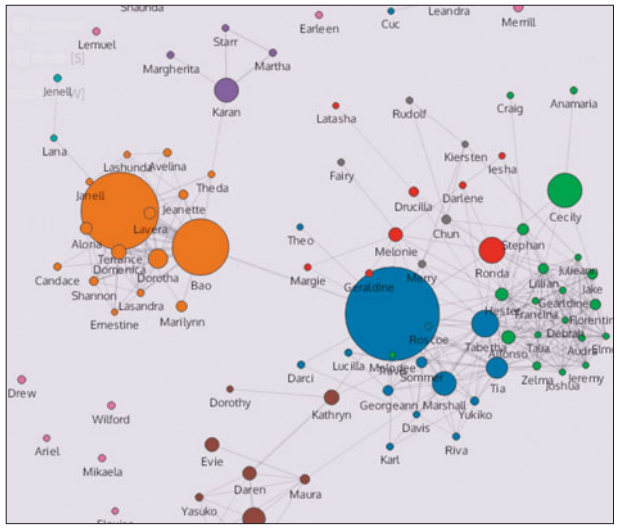
ANALÝZA VELKÝCH DATOVÝCH OBJEMŮ

V REÁLNÉM ČASE – NĚKOLIK PETABAJTŮ

On-line firmy a zpravodajské služby mají stejný problém: Při používání informací ze svých datacenter musí zpracovat obrovské množství dat v reálném čase. To lze ale provést pomocí sofistikovaných algoritmů, jako je například MapReduce, který byl vyvinut společností Google.



Příklad: shluková analýza
Vizualizace sociálních vztahů



VÝSLEDEK ANALÝZY DAT

Analýzou dat z e-mailu lze vypočítat pomocí klastrové metody počet sociálních kontaktů uživatele

res využívaných k obchodním účelům. V roce 1982 přibyl k aktivitám firmy i telefonní marketing a v roce 2005 se objevily její první e-mailové zpravodaje (tedy to, co většina uživatelů označuje za spam). Vzhledem k tomu, že zákony některých evropských zemí propojení on-line a off-line dat nedovolují, oficiálně k ničemu takovému nedochází. Acxiom se ale například chlubí tím, má více než 40 milionů sad osobních údajů, které se skládají ze jmen a poštovních adres.

Otázkou zůstává, kolik dat tvoří konkrétní údaje o uživatelích a kolik údaje určené pouhým odhadem odvozeným od informací ze statistických úřadů (např. údaje o příjmu nebo používání médií). Podle Carstena Diepenbrocka, ředitele německé pobočky firmy Acxiom, se ale data obecně nevztahují k jednotlivci. „Jsou agregována geograficky a zahrnují kteroukoliv pátou až tisící domácnost. To znamená, že Acxiom svým klientům poskytuje statistické pravděpodobnosti, jež jim sdělují, kde by bylo možné prodat které produkty."

Všeználci: Zpravodajské služby

NSA a další zpravodajské služby se také pokouší sloučit data shromážděná v režimu off-line s údaji shromážděnými on-line a jejich dalším cílem je korelace dat s konkrétními osobami. Bývalý analytik NSA Edward Snowden na začátku června odhalil obrovský rozsah operací týkajících se sběru údajů, které byly prováděny pod záminkou války proti teroru. Jedním ze zdrojů zde byli například i poskytovatelé telefonních a internetových služeb.

Oficiálně platí, že tito poskytovatelé musí uvolnit relevantní data a umožnit vyšetřovatelům sledovat konkrétní komunikaci v případě, že jde o (příslušnými orgány posvěcené) trestní stíhání. Podle informací získaných od Snowdena jsou ale v praxi získávány informace o všech lidech, tedy nejen informace týkající se podezřelých osob v probíhajícím vyšetřování.

Pro analýzu datového toku navíc zpravodajské služby využívají různé další technologie – například metodu hloubkové inspekce paketů (DPI). Použití této metody je téměř nutností, protože internetem proudí obrovské množství dat (streamování hudby či videa, P2P). To je možné pomocí DPI ignorovat a zkoumat pouze ta data, která tajné služby zajímají – například e-maily a zprávy z instant messengerů. Obvykle jsou v komunikaci vyhledávána klíčová slova související s terorismem či dodávkami zbraní, případně terminologie vztahující se na materiály, které se používají k výrobě bomb. Konkrétní údaje o tom, jaké množství dat a informací bylo kontrolováno u nás, zveřejněno nebylo, obrázek si ale můžete udělat i z oficiální informace ze sousedního Německa, kde byly v roce 2011 analyzovány asi tři miliony e-mailů a telefonních hovorů.

Nicméně poskytovatelé nejsou jediným výhradním zdrojem dat. Zpravodajské služby také shromažďují data v uzlech sítě a připojných bodech podvodních kabelů. Provozovatelé největšího světového uzlu DE-CIX ve Frankfurtu nad Mohanem sice tvrdí, že k jejich zařízení externí subjekty nemají přístup. Nikdo ale neví, zda totéž platí i v případě dalších asi 340 uzlů, které existují ve zbytku světa, z nichž osmdesát se nachází v Severní Americe.

Podle deníku Guardian má britský monitorovací program s názvem „Tempera" schopnost přímého přístupu k datům z transatlantických kabelů s optickými vlákny, které jsou hlavními tepnami internetových dat, jež cestují mezi USA a Evropou. Podle tohoto deníku může Tempora monitorovat více než 200 optických vláken a ukládat data po dobu až 30 dnů.

Data jsou přístupná na transfer pointech mezi poskytovateli a podmořskými kabely. Tato operace se rovněž dotýká českých

OBCHOD S INFORMACEMI

JAK CENNÁ JSOU VAŠE DATA

Informace o nemoci je z hlediska reklamního průmyslu nejcennějším druhem informací, protože pomáhá průmyslu inzerovat cíleně léky.

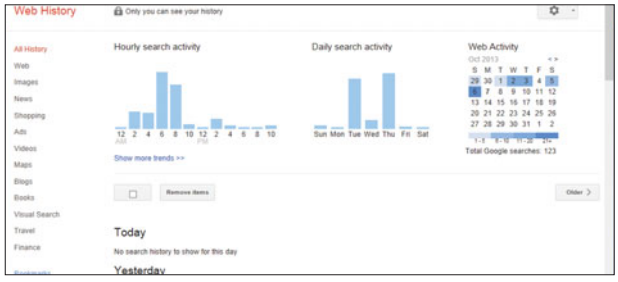
INFORMACE	CENA (ZA 100 UŽIV.)
ONEMOCNĚNÍ (NAPŘ. BOLESTI ZAD, ALERGIE)	26 $
ZASNOUBENÍ (MÉNĚ NEŽ TŘI MĚSÍCE)	12 $
KRÁTCE PŘED PORODEM	11,50 $
MAJITEL NEMOVITOSTI	10,50 $
SNAŽÍM SE ZHUBNOUT	10,50 $
PRÁCE (PODNIKATEL)	10 $
ZASNOUBENÍ (VÍCE NEŽ TŘI MĚSÍCE)	10 $
TĚHOTENSTVÍ (PRVNÍ DÍTĚ)	9,50 $
PLÁNOVANÉ STĚHOVÁNÍ	8,50 $
TĚHOTENSTVÍ (DALŠÍ DÍTĚ)	8 $
MAJITEL LODI	7,60 $
PRÁCE (ZAMĚSTNANEC)	7,20 $
DÍTĚ (VĚK, POHLAVÍ NEZNÁMÉ)	3,50 $
KONÍČKY (CESTOVÁNÍ, FITNES)	3 $
DÍTĚ (ŽÁDNÉ DALŠÍ ÚDAJE)	1,50 $
PLÁNOVANÁ KOUPĚ (MOBIL)	1,25 $
NEDÁVNO ŽENATÝ/ROZVEDENÝ	1 $
ETNICKÝ PŮVOD	0,50 $
STARŠÍ DĚTI	0,50 $
NEDÁVNO NAVŠTÍVIL FILMOVÝ WEB	0,30 $
ČÍSLO DEBETNÍ KARTY	0,10 $
NEDÁVNO NAVŠTÍVENÉ WEBOVÉ STRÁNKY	0,08 $
PLÁNOVANÝ NÁKUP (OBLEČENÍ)	0,08 $
VĚK	0,05 $
RODINA	0,05 $
PSČ	0,05 $
ÚROVEŇ VZDĚLÁNÍ	0,05 $

CELKOVÁ HODNOTA 1 UŽIVATELE (MAXIMUM INFORMACÍ): CCA 1,65 $

ZDROJ: FINANCIAL TIMES

ZLATÝ DŮL GOOGLU: VYHLEDÁVÁNÍ

Vyhledávání dokáže odhalit mnoho zájmů uživatele a pro celou řadu firem je to proto cenný zdroj informací.



SLEDOVÁNÍ UŽIVATELE NA WEBU

Základem pro získávání dat jsou sledovací soubory cookies na webových stránkách.

uživatelů, neboť jeden z kabelů (označovaný jako TAT-14) je prý sledován britskou zpravodajskou agenturou GCHQ. Tento kabel přenáší nezanedbatelný podíl on-line komunikace mezi Českou republikou a USA. Podle dostupných informací zaregistrovala v roce 2011 GCHQ téměř 39 miliard událostí, což je dokonce vyšší počet než součet jednotlivých akcí v rámci programu NSA.

Třetí zdroj informací a dat pro tajné služby představují samotní poskytovatelé služeb. Podle Edwarda Snowdena má program Prism možnost přímého přístupu na servery provozované společnostmi Google, Facebook, Microsoft, Apple, Yahoo, AOL, Dropbox a Paltalk.

Další zajímavá informace od Snowdena se vztahovala k událostem v polovině července. Podle něj dal Microsoft NSA přímý přístup ke komunikačním údajům, navzdory předchozímu firemnímu tvrzení o opaku. V případě Outlook.com má NSA údajně schopnost získat data ještě předtím, než jsou zašifrována. NSA prý také dokáže nahrávat audio- a videorozhovory provozované službou VoIP Skype (která patří společnosti Microsoft). NSA má dokonce i rozhraní spojené s on-line úložištěm služby SkyDrive, které také může využít k získání dat. Microsoft a NSA ale prohlašují, že údaje jsou poskytnuty až poté, co soud takové operace schválí.

Pokud jde o samotná data, zpravodajské služby čelí stejnému problému jako Google a spol.: Jak může být tak obrovská hromada nestrukturovaných dat, která obsahuje obrovské množství informací v mnoha různých formátech, zpracovávána? Stejně jako proces rafinace ropy je i tento proces, při kterém se z dat stávají použitelné informace, poměrně komplikovaný. Ještě před několika lety trvalo provedení podobných analýz i několik týdnů. Dnes se ale vše děje v reálném čase. Pro provozování tzv. velkých dat už totiž existuje celé průmyslové odvětví, které poskytuje analytické nástroje potřebné k procesu jejich třídění.

Data filtrují vysoce výkonné algoritmy

Analýza začíná procesem destilace dat. Nestrukturované hlasové vstupy, data o připojení, texty a jiné kousky informací jsou zpracovány tak, aby vytvářely strukturované databáze, které mohou být prohledávány pomocí jednoduchých dotazů: Kdo mluví s kým? O čem spolu hovoří? Jakou mají náladu?

Na podobném principu funguje též Graph Search, což je nový vyhledávací nástroj Facebooku. U něj stačí například jen zadat „přátelé v Brně, kteří se narodili v červnu“, a o zbytek se postará vyhledávací algoritmus.

Jedním z nejpoužívanějších velkých datových nástrojů je Hadoop, který používá také Facebook. Tento nástroj umožňuje analyzovat data, která existují v distribuovaných výpočetních sítích v petabajtovém rozsahu. Nástroj využívá algoritmus MapReduce, který byl vyvinut firmou Google (na obrázku → **str. 34**). Hadoop rozděluje data do bloků, z nichž každý obsahuje asi 64 MB dat, a samotné bloky jsou pak tříděny jednotlivě. Pro ilustraci: Konvenční databázové aplikace jsou obvykle schopné zpracovávat datové bloky obsahující jen 32 kilobajtů dat. Navíc v případě Hadoopu trvá proces analýzy bloku jen několik zlomků sekundy. Druhý krok procesu analýzy spočívá ve vytvoření prognostických modelů. To, v závislosti na cíli a záměru, představuje použití různých matematických postupů. Tyto procesy zahrnují procesy spojené s detekcí anomálií, dále ty, které souvisejí s detekcí zvláštních rysů datových toků, a ty, které souvisejí s metodou shlukové analýzy. Jejich cílem je rozdělit objekty do skupin (klastrů), které vyplynou v důsledku přítomnosti specifických rysů či podobností. Sociální grafy a propojení mezi jednotlivými uživateli tak mohou být vytvořeny například na základě telefonních připojení. Zpravodajské služby používají tuto metodu k identifikaci vztahů, které existují mezi různými lidmi.

Rozsah jejich přístupu pochopitelně překračuje i národní hranice a z hlediska časového horizontu jde i několik let nazpět. Podle Johna Inglise, zástupce ředitele NSA, jsou sledovány a monitorovány dvě až tři kontaktní úrovně osoby. To znamená, že pokud každý člověk zná sto lidí, pak úroveň třetího kontaktu této osoby obsahuje až milion lidí (100 × 100 × 100), kteří jsou sledováni na základě jediného podezřelého. K těmto souhrnným údajům pak využijí přístup analytici zpravodajských služeb s cílem nalézt a prošetřit určitou osobu.

Kdo tajně vydělává peníze na surfařích?

Klíčová otázka z pohledu datového analytika je následující: Co dokážu ze získaného údaje vyvodit? Aplikací, které daná data umí nejen třídit, ale také z nich vyvozovat určité závěry, je už celá řada. Například společnosti vydávající kreditní karty používají programy pro analýzu vzorů chování uživatele, aby zjistily, zda karta nebyla odcizena. Google například používá vyhledávací dotazy, aby mohl předvídat epidemie chřipky. A výzkumníci analyzují lidský genom, který je jedním z nejkomplexnějších zdrojů dat naší existence, s cílem dosáhnout pokroku v oblasti medicíny.

Důležité ale je si uvědomit, jak mohou být chyby při analýze a vyhodnocování dat důležité: zdaleka nejde jen to, že vám Amazon začne doporučovat produkty, o které nemáte vůbec žádný zájem, nebo že Google začne zobrazovat špatné výsledky vyhledávání. V praxi totiž může dojít k tomu, že zpravodajská agentura podezřívá nevinného člověka ze zločinu jen na základě analýzy. A to je nepřijatelné nejen ze sociálního hlediska, ale také proto, že pro danou osobu to může mít katastrofální následky. Příkladem takovéto nezvládnuté „prevence kriminality“ je například Murat Kurnaz, který byl označen jako podezřelý z účasti na terorismu a souvisejících činností a neprávem uvězněn v zařízení Guantanamo Bay.

Mezi těmito dvěma extrémy práce s daty se nachází široká šedá zóna, o které uživatelé nevědí zhola nic. Tedy o tom, co se s našimi daty děje, kromě faktu, že je jiní používají k tomu, aby vydělali peníze. A firmám se opravdu může hodit téměř cokoliv, záleží jen na oblasti jejich podnikání. Například z pohledu reklamního průmyslu jsou informace týkající se zdravotní historie, rodinného stavu a nadcházející výstavbě nového domova cennější než osobní údaje týkající se věku a bydliště (viz tabulka → **str. 35**).

Existuje ale jedna skupina lidí, kteří využijí a zpeněží jakékoliv soukromé informace – kybernetičtí zločinci. Ti si dokonce vytváří rozsáhlé datové sady odpovídající určitému jednotlivci, známé též jako „fullz“. Tyto balíky informací obvykle obsahují jména, detaily bankovních a kreditních karet a části osobních informací, například telefonní čísla a e-mailové adresy. Při použití v kombinaci s padělanými kreditními kartami nebo řidičskými průkazy mohou tyto údaje představovat slušnou finanční odměnu. Podle Dell SecureWorks mají hodnotu až 1 000 eur na osobu. Fullz lze získat asi za 400 eur, v závislosti na jeho obsahu. Jednotlivé údaje jsou levnější: přístupové údaje k PayPal účtu znázorňující stav účtu stojí 15 až 150 eur, zatímco soubor údajů o kreditní kartě, včetně bezpečnostního čísla, lze získat za méně než jedno euro za kartu.

Všechna tato data – a to je dobrá zpráva – lze ovlivňovat pomocí rozhodování, kam a na co klikáme. To znamená, že každý uživatel může učinit vědomé rozhodnutí, kolik za sebou zanechá datových stop.

AUTOR@CHIP.CZ