4

Záplava dat

Kdysi dávno jsme o datech mluvili jazykem knihovníků. Údaje se kolacionovaly a pečlivě katalogizovaly, aby byly připravené k nahlédnutí a připomínkám. Exploze online sledování, levných senzorů a výkonného počítačového zpracování se však stala předzvěstí nové éry – éry velkých dat – a způsobila metaforický posun.[68] Dnes se data obrazně valí kolem nás jako voda. Tvoří řeku, příval. Data jsou nová ropa: jsou úžasná, nekontrolovatelná a mají ošklivý zvyk unikat.

Metafora ropy je také vykresluje jako vzácné palivo pro digitální průmysl. To evokuje rychlé sondování, dychtivou těžbu a občas nebezpečné vykořisťování. V šesté kapitole uvidíme, jak datovou revoluci využívají orgány, například vlády, policejní sbory a armády, nejprve však prozkoumejme nové způsoby jejich komerčního využití.

Tím nejočividnějším je reklama. Nehmotnost digitálních technologií umožňuje oslovit ohromné množství uživatelů po celém světě; máte-li o nich více informací, můžete na ně lépe cílit a z reklamy získat vyšší výnos. Proto je v zájmu platforem financovaných reklamami shromažďovat

68 Cornelius Puschmann a Jean Burgess, „Metaphors of Big Data", *International Journal of Communication*, 8, 20 (2014).

co nejvíce informací o co největším počtu uživatelů. Harvardská vědkyně Shoshana Zuboffová tento vzkvétající obchod popisuje jako *kapitalismus sledování*, a dává mu tedy nálepku, jež přilákala aktivisty i datové disidenty, k nimž patří odborník na zabezpečení Bruce Schneier: „Za půl století se budou lidé na dnešní postupy zpracovávání dat dívat stejně, jako se dnes my díváme na prastaré obchodní praktiky, například pachtýřství, dětskou práci a firemní prodejny. Budou jim připadat nemorální."[69]

Každý systém, který pohlcuje množství údajů o našem životě, má etické důsledky, hyperbola s kapitalismem sledování však diskusi zamlžila. Označíme-li všechny weby a sociální sítě financované reklamou za formy sledování, dopustíme se zkreslení, jež naznačuje, že uživatelé nemohou s poskytováním svých údajů souhlasit ani profitovat z výsledné technologie. Tropus technologických platforem, které shromažďují spousty údajů, aby je mohly prodat inzerentům, je ekonomicky negramotný. Například pro Google a Facebook by prodej uživatelských údajů znamenal obchodní sebevraždu. Ano, tyto společnosti mají motivaci informace shromažďovat, jenže to dělají proto, aby inzerentům prodávaly *přístup k uživatelům*, nikoli samotné údaje. To je významný rozdíl. Obchodní modely společností Facebook a Google vyžadují fanatickou ochranu informací o uživatelích; zřeknout se údajů by znamenalo vzdát se konkurenční výhody. Nálepku sledování si mnohem více zaslouží datové zprostředkovatelské firmy jako Acxiom a Datalogix, jež shromažďují informace z veřejných záznamů, kupují historii, záruky a sebe navzájem a to všechno pak skutečně přeprodávají. Datové zprostředkovatelské firmy existují několik desetiletí, lze tedy stěží tvrdit, že jde o nový fenomén.

Data za reklamou

Data však chce nejen reklamní průmysl. Data živí také analytiku, díky níž mohou firmy porozumět svým trhům a měřit zlepšení produktů a spotřebitelé sledovat svá těla a životy. Rostoucí význam dat však především souvisí s umělou inteligencí (AI).

69 Bruce Schneier, „We Give Up Our Data Too Cheaply", *VICE Motherboard*, 2. března 2015, vice.com.

Bez dat žádná umělá inteligence neexistuje. Moderní systémy hlubokého učení (deep learning) studují rozsáhlé soubory tréninkových dat a s výslednými modely pak srovnávají nová data v rámci takzvané *inference*. Tyto systémy již ukazují vzrušující potenciál přiřazování schémat. V kontrolovaných podmínkách dokáže umělá inteligence odhalit zápal plic lépe než radiolog,[70] smlouvy o důvěrnosti (NDA) vyhodnotit rychleji než právníci[71] a na znalostní otázky odpovědět lépe než člověk.[72] Data vytrénují umělou inteligenci, jež bude kontrolovat domácnost, řídit motorová vozidla a ovládat zabezpečovací systémy. Již dnes můžeme odemykat zařízení a nakupovat pomocí údajů o našem obličeji; banky používají k omezení podvodů hlasovou identifikaci. Jedno parkoviště v Pekingu dokonce rozpoznání obličeje používá k přidělování toaletního papíru a návštěvníci dostávají nejvýše šedesát centimetrů každých devět minut.

Pro funkčnost a uživatelské zkušenosti s těmito technologiemi jsou nejdůležitější data. Neposkytnete-li osobní údaje hlasovému asistentovi, při jeho používání se budete trápit, protože hlasový asistent se nezlepší tím, že vás lépe pozná. Na bota s celkovou amnézií začne rychle padat prach. Jestliže se odhlásíte z nových bezpečnostních technologií své banky, ocitnete se znovu ve starém světě nepraktických hesel a generátorů kódů.

Všechna tato různorodá použití s sebou nesou určité etické riziko. Proto je závažnou chybou soustředit se při diskusi o datové etice pouze na reklamu. Ti, kteří tvrdí, že zneužívání přirozeně vyplývá z reklamních modelů, přehlížejí, že ze shromažďování většího množství údajů má prospěch *každá* firma. Sotva záleží na tom, kdo to zaplatí.

70 Dave Gershgorn, „Stanford trained AI to diagnose pneumonia better than a radiologist in just two months", *Quartz*, 16. listopadu 2017, qz.com.

71 „AI vs. Lawyers", lawgeex.com.

72 Allison Linn, „Microsoft creates AI that can read a document and answer questions about it as well as a person", microsoft.com, 15. ledna 2018.

Nezpracované údaje jsou oxymóron

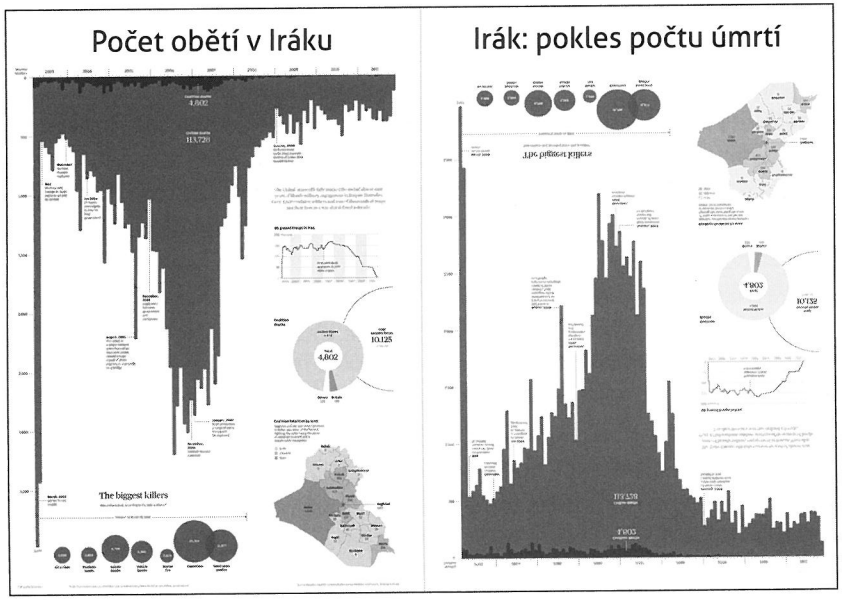
Přestože datový stín vrhá prakticky všechno, co děláme, musíme mít na paměti, že stíny jsou vždy jen obrysy. Data se běžně interpolují, zaokrouhlují, zkracují nebo jsou prostě špatná. Anesteziolog Dr. Julian Goldman zkoumal hodiny v 1300 lékařských zařízeních a zjistil, že téměř 20 % se jich opožďovalo o více než 15 minut, a časové údaje klíčové pro dávkování léků tak ztrácely na platnosti.[73] Budete-li si procházet jakoukoli americkou marketingovou databázi, objevíte překvapivý počet zákazníků z obce Schenectady ve státě New York, což se zdá bizarní, dokud si nevšimnete PSČ: 12345.

Metafora dat jako ropy má jeden významný nedostatek: popisujeme-li data jako zboží, ignorujeme jejich původ. Zatímco ze stávajících (třebaže tenčících se) ložisek ropy stačí jenom čerpat, získávání dat není pasivním krokem. Výběr dat, která budeme shromažďovat a která vynecháme, technologie, které k jejich shromažďování a zpracovávání použijeme, i techniky k jejich analýze jsou samy o sobě zatížené skrytými předpoklady a předsudky. Například vypátrat amerického vlastníka zbraně je záměrně obtížné a potřebujete k tomu stopu vedoucí od místních prodejců zbraní po přepravní kontejnery Úřadu pro alkohol, tabák, zbraně a výbušniny (ATF) plné mikrofilmů. Počítačové vyhledávání je díky úsilí Národní střelecké asociace (NRA) zakázáno proto, aby se tento proces co nejvíce ztížil. Nemožnost oddělit data od kontextu jejich získávání a zpracování vedl Geoffreyho Bowkera k vyslovení památné věty: „Nezpracované údaje jsou oxymóron a špatný nápad; data se naopak musí pečlivě připravovat."[74]

Reprezentace dat s sebou také přináší konotace a podjatost. Designéři dobře vědí, jak přesvědčivé asociace může vyvolávat rozvržení, písmo a barva. Andy Cotgreave například na následující ilustraci převrací význam poselství pozoruhodné grafiky Simona Scarra o válce v Iráku pomocí jiného titulku a otočení grafu vzhůru nohama.

73 Julian M. Goldman, MD, „Medical Device Interoperability Ecosystem Updates: Device Clock Time, Value Proposition, and the FDA Regulatory Pathway", NSF CPS Large Site Visit, 31. ledna 2012.

74 Geoffrey C Bowker, *Memory Practices in the Sciences* (MIT Press, 2006).



Publikováno v *South China Morning Post*;
pro obr. vpravo poskytl souhlas Andy Cotgreave.

Musíme si tedy dát pozor na schopnost údajů uvádět nás v omyl. To je v rozporu s převládající ideologií, která data doprovází a která paradoxně tvrdí, že data žádnou ideologii nemají. Mnoho technologů přesvědčených o tom, že data jsou podstatou veškerého poznání, je brání jako objektivní a přesný odraz světa kolem nás; z tohoto pohledu pak větší počet informací znamená větší moc a data jsou ta *správná* data.[75] Argument zní, že pokud jim není co vytknout, nelze nic vytknout ani rozhodnutím, která se o ně opírají.

75 Viz Adam Greenfield, *Radical Technologies* (Verso 2017).

Smíření s nejistotou

Ve špatných rukou jsou však i přesné údaje škodlivé. Zatím největší katastrofou bylo porušení soukromí agenturou Equifax, která v roce 2017 vydala jména, čísla sociálního pojištění, data narození a adresy 145 milionů Američanů. Ukradeno bylo dalších 209 000 čísel kreditních karet. V době, kdy píšu tento text, tedy poté, co několik řídících pracovníků agentury muselo odejít a vedení postiženým občanům nabídlo monitorování bonity, má společnost Equifax, jejíž hodnota dosahuje 16 miliard dolarů, jen o 4 % horší hodnocení než před únikem dat. Důsledky krádeže identity tak dopadají více na spotřebitele než na odpovědné společnosti.

Bohaté zásoby dat a špatné zabezpečení také lákají k vydírání. Útoky na webové pornostránky Adult FriendFinder a Ashley Madison, vyvolané údajně morálním odporem, vedly k vydírání uživatelů, kteří platili za mlčení, nebo k tomu, že je hackeři podvodně přiměli k instalaci malwaru umožňujícího další vysávání dat.

Ostudně málo zabezpečená jsou připojená domácí zařízení, jejichž výrobci si konkurují výhradně cenou, což má za následek donebevolající zranitelnost. Vědci se nabourali do teleskopického vibrátoru s endoskopem Svakom Siime Eye, který umožňuje sledování streamovaného videa kdekoli v dosahu Wi-Fi; botnet Mirai, dnes připisovaný třem studentům, kteří se snažili narušit činnost rivalských serverů hry Minecraft, zneužil nezabezpečená hesla správců, a 600 000 zařízení se tak stalo nepoužitelných. Jak poznamenal jeden anonymní šprýmař: „Písmeno Z ve zkratce IoT (internet věcí) znamená zabezpečení."

Veřejnost ochromená nekonečnými úniky dat, nečitelnými zásadami ochrany osobních údajů a protivnými formuláři pro udělení souhlasu se smířila s nejistotou: do dalšího porušení ochrany údajů. Je těžké jí to dávat za vinu. I uživatelská řešení navrhovaná technologickým odvětvím – správci hesel, dvoufaktorové ověřování, střídání hesel – netechnické uživatele neúměrně zatěžují a problém nespravedlivě individualizují.

Řada potíží souvisejících s datovou etikou se točí kolem soukromí. Ochrana osobních údajů představuje složité téma, které lidé obecně chápou, ale špatně definují. Dalece přesahuje prosté zabezpečení a dotýká se důležitých hodnot, například důstojnosti a důvěry. Zaměstnanec firmy, který si prohlíží citlivé údaje bez řádného důvodu, soukromí lidí porušuje,

a to i v případě, že se tyto údaje ukládají bezpečně a se souhlasem uživatelů.

Někteří teoretici popisují ochranu soukromí jako právo zvolit si ústraní, odmítnout roli ve veřejné sféře. Jiní ji definují jako důvěrnost, včetně odborníka na právo Richarda Posnera, který říká, že lidé si pod pojmem soukromí představují „utajování informací o své osobě, jež by jiní mohli využít k tomu, aby je poškodili".[76] Tyto formy ochrany soukromí již nemusí být udržitelné. Člověk, který chce zcela utajit své osobní údaje, se musí z moderní společnosti stáhnout: kreditní karty, mobilní telefony a e-mail osobní údaje odhalují a umožňují jejich sledování. Naprostá informační izolace je bez vystoupení ze systému nemožná.

Moderní ochranu soukromí snad lépe pochopíme jako kontrolu a sebeurčení. Pokud je to možné, lidé by měli mít možnost sdělovat jakékoli informace, které chtějí, komukoli si přejí a kdykoli, a musí mít také možnost tato rozhodnutí zvrátit. Pak bude ochrana osobních údajů něco jako ručička na ciferníku, nejen visací zámek.

Směna hodnot v praxi

Dáme-li lidem kontrolu nad jejich daty, získají také právo s nimi obchodovat. Soukromí se stane měnou, něčím, co lidé mohou vyměnit za pohodlí. Jde o důležitou směnnou hodnotu. Pokud tuto výměnu chápou obě strany a je-li oboustranně spravedlivá, teoreticky může vyvolávat jen málo etických pochybností; tak by koneckonců měl obchod probíhat. Proběhne-li dobře, miliardy lidí dostanou inovativní technologii výměnou za dohodnuté množství osobních údajů. Jenže je tento obchod spravedlivý dnes?

Popravdě řečeno mají uživatelé pouze malou moc na to, aby si vyjednali odškodné nebo se obchodu nezúčastnili. Technologické společnosti si výměnou za přístup k datům kladou neměnné požadavky: berte, nebo nechte být. Obhajoba volného trhu, podle níž mohou spotřebitelé prostě přejít ke konkurenci, zní nepřesvědčivě. Konkurenční sociální sítě jsou k ničemu, pokud na nich nejsou vaši přátelé, a chcete-li cenově dostupný chytrý telefon nebo hlasového asistenta, vyhnout se ekosystémům technologických

[76] Richard A. Posner, „Privacy, Secrecy, and Reputation", 28 *Buffalo Law Review* 1 (1979).

gigantů je dnes těžké. Některé digitální služby jsou pro moderní život natolik zásadní, že prakticky jde o veřejné služby: buď musí uživatelé odevzdat své údaje, nebo je čeká zbídačená digitální existence.

Podmínky výměny dat bývají neprůhledné. Neproniknutelné zásady ochrany osobních údajů a strohá vyskakovací okna operačních systémů se nevyjadřují jasně: i jednoduchý požadavek jako „Udělit přístup k historii prohlížení?" může mít řadu výkladů. Jak daleko může taková historie sahat? Zapisuje jen domény, nebo konkrétní stránky? Zaznamená moje vyhledávací dotazy prostřednictvím parametrů URL?

Veřejnost se navíc o to, jak agregace mění datovou krajinu, do značné míry nestará. Firmy mohou kombinováním datových souborů získávat nové poznatky; algoritmy ve čtení mezi řádky vynikají. Aplikace Tinder ví nejen to, kdo se vám líbí, ale i to, jak atraktivní vám přijdou různé rasové skupiny. Facebook dokáže z chování v aplikaci odvodit vaše politické názory. Pokud se správně vytěží zdánlivě neškodné žádosti o informace, lze získat vysoce citlivé inference druhého řádu.

A konečně, rozhodování o ochraně osobních údajů často ovlivňuje okolí. Spousta uživatelských dat se týká mnoha lidí: v kalendáři máte zapsané narozeniny členů rodiny; přátele máte označené v knihovně fotek. Také e-maily mají odesílatele i příjemce. Celkem 320 000 lidí si nainstalovalo nechvalně známý facebookový osobnostní test Dr. Aleksandra Kogana, který později společnost Cambridge Analytica využila pro politické cílení; každý „seeder" (zdroj dat) dal navíc aplikaci přístup průměrně ke sto šedesáti přátelům. Nejmenovaná psychiatrička zase zjistila, že facebookový algoritmus „Lidé, které můžete znát" navrhoval, aby se vzájemně spřátelili její pacienti.[77] Nejpravděpodobnější vysvětlení? Každý z nich si ji přidal do adresáře v telefonu. Facebook pak předpokládal, že jelikož mají společného přítele, mohou se znát navzájem; pro pacienty psychiatričky, z nichž někteří přežili sebevraždu nebo se snažili uniknout z násilných vztahů, to znamenalo vážné ohrožení soukromí. Prostřednictvím identifikace dalších osob zmíněných v uživatelských údajích mohou technologické firmy dokonce vytvářet stínové profily lidí, kteří se k jejich službě nepřihlásili.

[77] Kashmir Hill, „Facebook recommended that this psychiatrist's patients friend each other", *Splinter*, 29. srpna 2018, splinternews.com.

Zpráva Světového ekonomického fóra v roce 2011 označila osobní údaje za „novou třídu aktiv". Počet technologických společností, jež se obchodu s daty účastní, sice roste, uživatelé si však hodnotu tohoto nového bohatství musí teprve uvědomit. Vyhledávače a sociální software jsou dnes do značné míry stejné jako před deseti lety, a třebaže několik platforem, například YouTube, se snaží o tržby dělit, skutečný zisk mají jen nejvlivnější uživatelé. Na rozdíl od utopického snu o obchodování s údaji však již uživatelé žádnou spravedlivou kompenzaci nedostávají.

Nové vymezení veřejného a soukromého

Má-li být obchod s údaji spravedlivý, musí mít obě strany podobné názory na to, co má být soukromé a co veřejné. To není snadné: hranice probíhá napříč kulturami a generacemi.

> Pojetí soukromí ve smyslu, v jakém je používáme dnes, je západní kulturní artefakt. Představa, že by mohlo být příjemné existovat mimo veřejné jeviště, ve společnosti nedávala velký smysl. [...] Soukromí bývalo údělem páriů.[78]

Ochrana osobních údajů se opírá o komplexní síť společenských konvencí. Spotřebitelé, kteří technologie označují za „děsivé", si stěžují, že jejich očekávání, pokud jde o hranici mezi veřejným a soukromým, se nesplnila a že technologie vědí víc, než by podle nich měly. Tato hranice je však nestabilní a neustále se překresluje a narušuje. Z předefinování soukromých informací na veřejné obvykle těží technologické společnosti; jakmile se data zveřejní, je jednodušší je využít. Řadě nových technologií je navíc vlastní tendence narušovat soukromý prostor a vytvářet to, co bychom mohli označit za *posun ke zveřejňování*. Hlasová rozhraní dávají interakci člověka s počítačem dosah vysílání, do vysokých oken nakukují drony a technologie odezírání ze rtů dokáže z úst mluvčího vyrvat soukromý rozhovor. Zařízení sdílená uživateli nebo nainstalovaná na veřejných prostranstvích – což

78 Richard A. Posner, „Privacy, Secrecy, and Reputation", *Buffalo Law Review*, sv. 28, č. 1 (1979).

je předpoklad inteligentního města – tento trend jen urychlují. Autonomní vozy budou například nepřetržitě zaznamenávat ulici ze stovek úhlů a vytvářet záznam, který bude neocenitelným přínosem pro výrobce i pro policii, jež ho bude vyžadovat pro všechny druhy vyšetřování, nejen u silničních dopravních nehod. Tato plíživá kolonizace našich měst přiměla časopis *The Economist* – který lze stěží prohlásit za odpůrce technologií či korporátní moci – k tomu, aby autonomní vozy označila za „pantoptikony na kolech".[79]

Nerovnováha moci, jež je dnešním technologiím vlastní, někdy firmám umožňuje zmocnit se soukromých informací silou. Řada neustále zapnutých produktů vyžaduje, aby se uživatelé smířili s novými požadavky na údaje, a otevřeli tak dveře jejich zneužívání. Společnost Sonos v roce 2017 prosadila nevyváženou aktualizaci ochrany osobních údajů a její odpůrce varovala, že nedostanou budoucí aktualizace softwaru, a jejich drahá zařízení proto postupem času přestanou fungovat. Uživatelé se tedy na datové ekonomice v nejhorším případě podílejí jen jako výchozí surovina.

Nepolevující narušování soukromí by mohlo způsobit skutečné škody. Tento druh *argumentu šikmou plochou* – tvrzení, že menší ústupek může uspíšit nebezpečnější kompromisy – je v etice běžný. Někteří aktivisté v oblasti ochrany soukromí tvrdí, že pokud si technologické firmy říši soukromí přivlastní, dospějeme postupně k post-soukromé budoucnosti, v níž bude mlčenlivost projevem nepoctivosti a mocní budou na požádání smět sledovat kohokoli. (Tuto konkrétní dystopii si probereme v šesté kapitole.) Argumenty šikmou plochou vycházejí z řetězců příčin a následků, které sice nenastanou vždy, přesto si zasluhují pozornost. Připomínají cvičení s kolem budoucností: někdy i sebemenší riziko vyžaduje preventivní opatření.

Před škodami způsobenými šikmou plochou se lze chránit dvěma účinnými způsoby: nastavením zákonných omezení – můžete zajít jen potud, dál už ne – a vytvářením technologií, jež působí proti gravitačním silám. Ve světě dat jsou známé jako *technologie na podporu ochrany soukromí* (PET).

79 „Self-driving cars offer huge benefits – but have a dark side", *The Economist*, 1. března 2018, economist.com.

De-identifikace a re-identifikace

Nejsamozřejmějším přístupem ke zvýšení ochrany soukromí je odstranění osobních identifikovatelných údajů. Tuto de-identifikaci lze však čím dál snadněji zvrátit. V roce 2006 dva vědci využili údaje společnosti Netflix a databáze IMDb ke zpětné identifikaci uživatelů obou služeb a k odvození jejich politických preferencí[80] a profesorka Latanya Sweeneyová dokázala prostřednictvím křížových referencí z amerického sčítání lidu a seznamů voličů identifikovat více než polovinu obyvatel USA, a to jen s údaji o jejich pohlaví, datu narození a bydlišti.[81]

Zdánlivě neškodné údaje se v kombinaci s jinými soubory dat často stávají mnohem nebezpečnějšími. Mnoho uživatelů ochotně sděluje svou polohu, historii kreditních karet a srdeční frekvenci a každý, kdo si umí všechny tři údaje spojit dohromady, snadno shromáždí důkazy o závažných zdravotních problémech nebo milostném poměru dotyčných. De-identifikované údaje proto musí být v bezpečí nejen před současnými re-identifikačními technologiemi, ale i před všemi soubory dat a budoucími algoritmy, jež by se daly použít ke křížovým referencím a k analýze. Prostřednictvím dnes neškodných metadat vás zítra mohou sledovat. Tyto alarmující vyhlídky některé zasvěcence z technologických firem vedly k tomu, že de-identifikaci prohlásili za strategii odsouzenou k záhubě.

> Společnost Uber poskytuje anonymizovaná data o dvou miliardách výjezdů. Chcete-li soubor neanonymizovaných dat, počkejte si půl roku až rok. – Maciej Cegłowski[82]

Vlády, které si tuto hrozbu uvědomují, se nyní proti zpětné identifikaci snaží vydávat zákony. Británie navrhuje, aby „úmyslná či nedbalostní zpětná identifikace osob z anonymizovaných či pseudonymizovaných dat" byla trestným činem. To zní sice slibně, ovšem chybí detailnější informace:

80 Arvind Narayanan a Vitaly Shmatikov. „Robust Deanonymization of Large Datasets (How to Break Anonymity of the Netflix Prize Dataset)", 2006.

81 Latanya Sweeney, „Simple Demographics Often Identify People Uniquely", Carnegie Mellon University, pracovní verze textu, Data Privacy, 2000.

82 Pinboard (@pinboard), Twitter, 8. ledna 2017.

Bude například nezákonné odhalit, kdo stojí za pseudonymním účtem na Twitteru?

Bezchybné fungování a důvěra

I veřejné údaje lze používat způsoby, jež porušují soukromí. Kontroverzní vědec Emil Kirkegaard si v roce 2016 vytvořil na seznamce OkCupid falešný účet a pak z ní pomocí bota vyškrábl 68 000 profilů. Soubor údajů včetně uživatelských jmen zveřejnil a pokusil se na něm ukázat spojitost mezi inteligencí a náboženským přesvědčením. Proti výslednému rozruchu se bránil neomaleným tvrzením: Údaje už přece veřejné byly, tak v čem je problém? Časopis *WIRED*, který Kirkegaardův prohřešek pozoruhodným způsobem bagatelizoval, upozornil na „závážné etické otázky, jimiž se musí zabývat analytici tzv. velkých dat [...], aby neúmyslně nepoškodili ty, kteří uvíznou v datové síti".[83]

Není žádným překvapením, že hlavním bitevním polem, na němž se boj o ochranu soukromí odehrává, jsou technologie: veřejnost obvykle nemá ponětí, co moderní zařízení potají dělají.

> Pokud stroj efektivně funguje, pokud je skutečnost dána, stačí se zaměřit pouze na jeho vstupy a výstupy, nikoli na jeho vnitřní složitosti. Paradoxně tak platí, že čím jsou věda a technologie úspěšnější, tím neprůhlednějšími a nevysvětlitelnějšími se stávají. – Bruno Latour[84]

Latour má pravdu v tom, že technologie přirozeně inklinují k neprůhlednosti, ovšem jestliže technologické firmy skrývají vnitřní fungování, jde také o důsledek vědomého rozhodnutí designérů. Ve jménu bezchybného fungování přesvědčili uživatele, aby se nedívali pod kapotu. S výměnou údajů se zachází jako se složitostí, s něčím, co je nejlépe nějakým trikem

83 Michael Zimmer, „OkCupid Study Reveals the Perils of BigData Science", *WIRED*, 14. května 2016, wired.com.

84 Bruno Latour, *Pandora's Hope: Essays on the Reality of Science Studies* (Harvard University Press 1999).

zakrýt. Technologický průmysl proto musí silně spoléhat na důvěru. Uživatelé musí věřit slibům technologů, že hlasoví asistenti nic nenahrávají, dokud neuslyší dané slovo, že kamery se nespustí bez souhlasu, že nikdo neprochází jejich soukromé zprávy. Čím nižší úroveň v oblasti technologií – představte si operační systémy či prohlížeče –, tím nebezpečnější může potenciální porušení důvěry být.

Důvěra je důležitá etická hodnota a pro zdravou společnost je zásadní. Svěřit někomu údaje znamená mít jistotu, že je nezveřejní; důvěra je tedy konsensuální slabé místo v zabezpečení. Většina firem ji má, třebaže neexistuje prostý způsob, jak si to uživatel může ověřit. Některé firmy však důvěru zrazují tím, že soukromé údaje tajně využívají pro svůj zisk. Společnost Verizon pokoutně modifikovala webový provoz tak, aby zahrnoval sledovací program, který nezisková organizace Electronic Frontier Foundation popsala jako „nesmazatelný soubor supercookie".[85] Rozhodnutí americké agentury FCC z roku 2017 o tom, že poskytovatelé internetových služeb již nepotřebují k prodeji uživatelských údajů souhlas, k podobnému chování nepochybně vybídne.

Možná bychom se neměli ptát, zda je firma důvěryhodná; otázkou by mělo být i to, co by s důvěryhodnými informacemi mohl udělat zloduch. Firmy koneckonců rychle vznikají a krachují, někdo je koupí nebo se do nich naboural, a osobních údaje se tak často dostanou do rukou nedůvěryhodných či neznámých skupin.

Regulace údajů

Vzhledem k tomu, jak velké zneužití údajů hrozí, a vzhledem neprůhlednosti, jež brzdí spravedlivou výměnu dat, se o věc přirozeně zajímají regulační orgány. Zákon o ochraně údajů musí být vyvážený: musí hájit osobní práva a zároveň vycházet vstříc potřebám inovací a tomu, co je pro společenost prospěšné. Demokracie například potřebuje seznam voličů, i když jednotlivci by dali přednost tomu, kdyby jejich údaje v centrální databázi nebyly.

[85] Jacob Hoffman-Andrews, „Victory: Verizon Will Stop Tagging Customers for Tracking Without Consent", 7. března 2016, eff.org.

V různých právních a společenských kulturách podle očekávání vznikly rozdílné přístupy. Spojené státy jako obvykle nechaly průmysl, aby se reguloval sám, poněvadž vládní intervenci vnímají až jako poslední možnost. Přestože mají stovky zákonů na ochranu soukromí, mnohé z nich jsou omezené a zbytečné a neplatí ve všech státech. Jiné země mají přísnější požadavky. Indie v roce 2017 prohlásila ochranu osobních údajů za ústavní právo, a urychlila tak úspěšné zrušení tamního dlouholetého zákazu homosexuality. Aktivisté tvrdili, že sexuální orientace a aktivita jsou soukromou záležitostí, a jsou proto nově chráněny. Nezamýšlené důsledky tedy mají i regulace: v tomto případě to dopadlo dobře.

Nejpřísnější režimy pro ochranu údajů jsou dnes v EU. Německo zakazuje prodej chytrých hodinek dětem s tím, že jde o „zakázaná odposlouchávací zařízení"; poté, co v minulém století zažilo dva totalitní režimy, má vůči sdílení osobních údajů silný kulturní odpor. Obecné nařízení o ochraně osobních údajů (GDPR) z roku 2018 znamenalo v celé EU nový mezník a týká se všech firem na světě, jež zpracovávají údaje evropských občanů. Nařízení GDPR rozšiřuje rozsah osobních údajů, stanovuje přísné nové normy pro poskytování souhlasu (což pro temné datové mechanismy, například předvyplněná políčka, znamená trest smrti), nabízí nová individuální datová práva a omezuje automatizované rozhodování. Na rozdíl od svých předchůdců může mít také dopady: pokuty za závažná porušení mohou dosahovat až 4 % celosvětového obratu firmy nebo 20 milionů euro.

Nařízení GDPR je pravděpodobně prvním krokem ke globálnímu utahování datových opasků. Brzy možná budeme svědky sladění sankcí za úniky údajů se sankcemi za průmyslové havárie a se zákony, jež poženou technologické firmy k odpovědnosti za bezpečnostní rizika. S cílem udržet průmysl na své straně budou vlády pravděpodobně nabízet i pobídky, například daňové úlevy za bezpečné sdílení údajů, z nichž budou těžit nová průmyslová odvětví.

Zvláště sporná právní a etická debata se vede o *právu být zapomenut*. Digitální údaje mají ve zvyku nemizet a zachycovat pomíjivé okolnosti a přesvědčení v neosobním snímku. Je to vzhledem k přirozenému lidskému sklonu zapomínat spravedlivé? Měli by mít lidé možnost zatajit svou minulost? Právní a morální precedens pro stažení informací z veřejného prostoru již existuje. Například britský Zákon o rehabilitaci pachatelů (Rehabilitation of Offenders Act) lidem umožňuje neuvádět méně závažné

trestné činy, pokud se jich už znovu nedopustili. Oběti sexuálních trestných činů získávají podle britského práva automaticky anonymitu, což je z hlediska morálky vítané rozhodnutí, může však vyžadovat nepříjemné úpravy údajů. Když v roce 2012 patnáctiletá Britka zmizela i se svým učitelem, tamní noviny ji vyzývaly, že pokud se vrátí, nic jí nehrozí. Jakmile vyšlo najevo, že dotyční spolu měli (trestný) sexuální vztah, jméno dívky se už nesmělo v tisku objevit.

Evropský soudní dvůr v roce 2014 rozhodl, že Evropané mohou žádat vyhledávače, aby z výsledků vyhledávání vyřadily webové stránky, které se jich týkají, což už není ani tak zapomínání jako spíše mazání mapy. Etik Luciano Floridi sice rozhodnutí chválil jako „dospívání naší informační společnosti",[86] bylo však sporné a dodnes se o něm pochybuje. Novináři je odsoudili s tím, že z očí veřejnosti by mizely exkluzivní zprávy a šejdíři by vymazávali historii. Některé noviny se od té doby brání tím, že zveřejňují vlastní seznamy stránek, které Google vyřadil. Navzdory počátečním obavám se ovšem právo být zapomenut používá nejen k utajování prohřešků. Mezi žadateli byli také lidé, kteří se chtěli zřeknout dřívějších politických názorů, oběti trestné činnosti, jež chtěly zapomenout na minulost, a transgender osoby, které chtějí ze záznamů odstranit původní jména.

K právu být zapomenut by mohl být skeptický také deontolog s tím, že lidé mají morální povinnost žít s následky svých činů. Kdyby o vyřazení žádali všichni, zmizelo by naše sdílené poznání i důvěra. Kritizovat někoho na základě velmi přísných deontologických důvodů se zdá nicméně kruté, pokud se chce pouze zbavit emočního traumatu. Právo být zapomenut také pěkně odpovídá představě soukromí jako sebeurčení. Zapomínání lidem umožňuje žít bez stigmatu menších chyb. Sheilla Janasoffová ve své knize *The Ethics of Invention* (Etika invence) tvrdí, že právo být zapomenut je důležitou součástí existence „pohyblivého, měnícího se, sledovatelného a svéhlavého subjektu".[87]

V praxi stojí úřady na straně vyhledávače, který může žádost odmítnout na základě svobody projevu, veřejného zájmu a pokud je to právně

[86] Luciano Floridi, „Google ethics adviser: The law needs bold ideas to address the digital age", *The Guardian*, 4. června 2014, theguardian.com.

[87] Sheila Janasoff, *The Ethics of Invention: Technology and the Human Future* (W. W. Norton & Company, 2016).

nezbytné. Během tří let společnost Google vyhověla jen 43 % žádostí.[88] Nedávné případy konečně vrhly určité světlo i na to, jak k těmto rozhodnutím dochází. Google má k dispozici právní tým pro odstraňování záznamů a poradní sbor, podle portálu *The Register* však někdy spolurozhodují softwaroví inženýři, či jim dokonce patří poslední slovo.[89] Ačkoli žadatelé mají možnost se odvolat k národním agenturám pro ochranu údajů, je s podivem, že soukromá firma může mít na datová práva jednotlivců takový vliv – byť je pravděpodobné, že Google má nesmírnou moc i bez ohledu na právo být zapomenut.

Právo být zapomenut je stále převážně evropským fenoménem. Jeho americkou verzi by bylo obtížné sladit například s prvním dodatkem Ústavy o právu na svobodu projevu, výsledek má proto velmi teritoriální podobu: odkazy skryté v Evropě jsou stále viditelné jinde. Nové technologie mohou vést ještě k dalším výrazným změnám. Pokud jste již údaje předali nezměnitelnému blockchainu, nezbývá než vám při vyřizování požadavku na právo být zapomenut popřát hodně štěstí.

Přizpůsobit se nařízení zjevně není snadné. Budoucí zákony o ochraně údajů budou firmy nutit ke změnám algoritmů, rozhraní, procesů i zásad: k nákladným změnám, jež mohou malé firmy postihnout více než velké provozovatele. Technologické firmy si zřejmě budou muset vystačit s méně častými statistikami zákazníků a s horšími tréninkovými daty a některých inovací se budou muset nepochybně zbavit, protože budou nepoužitelné. Kvůli nařízení GDPR nemůže Facebook Evropanům nabídnout nástroj, který iniciativně odhaluje riziko sebevraždy, což vede ke škodolibým stížnostem bojovníků proti EU a za volný trh. Vždy však existuje i jiné rámování: novinář deníku *Guardian* Alex Hern dospěl k závěru, že tato facebooková funkce „je doslova nelegální [...], protože její funkčnost vyžaduje bezuzdné porušování ochrany osobních údajů".

Datové normy budoucnosti mohou být přísnější, pokud je však zvládneme, budou také jasnější a zlepší se jejich vymahatelnost. Firmy si už nebudou konkurovat v tom, kolik dat nepozorovaně ukradnou a zpeněží;

[88] Michee Smith, „Updating our "right to be forgotten" Transparency Report", blog *Google in Europe*, 26. února 2018, www.blog.google.

[89] Gareth Corfield, „Here is how Google handles Right To Be Forgotten requests", *The Register*, 19. března 2018, theregister.co.uk.

prvořadá bude důvěra uživatele. Nejvíce se to dotkne těch, které fungují s pochybným souhlasem mimo zraky veřejnosti. Digitální sledování, celé roky utajované, konečně nutně vyplave na povrch, což způsobí panickou konsolidaci. Dobrá legislativa by měla poškodit především ty firmy, kvůli nimž byl tvrdý zásah nutný: skončí-li ti, kteří drancují data z reklamy, nikdo pro ně plakat nebude.

Úvod do utilitarismu

Právní předpisy by měly být spíše záchrannou sítí, nikoli etickým východiskem. Technologický průmysl zabrání vzniku předpisů nejlépe tím, že bude v současnosti činit lepší rozhodnutí. Podívejme se tedy na další teorii etiky: *utilitarismus*.

Utilitaristé se neobávají morálního zákona ani povinnosti; zajímají je jedině výsledky. Proto se utilitarismu říká *konsekvencionalistický* přístup. Navrhli ho empirici Jeremy Bentham a John Stuart Mill, kteří měli pocit, že deontologie je zbytečně abstraktní, a tvrdili, že činy bychom měli raději soudit podle toho, zda přinášejí štěstí. Pro utilitaristy představuje štěstí nejvyšší dobro, hlavní cíl společnosti a života. Neznamená to sice, že bychom měli usilovat jen o požitkářská vzrušení, nicméně zejména Mill se zápalem zdůrazňoval, že štěstí by mělo zahrnovat intelektuální a emocionální naplnění. Utilitaristé ani neusilují o umocnění vlastního pocitu štěstí – tomuto přístupu se říká *egoismus*, a ten se samozřejmě všeobecně považuje za závadný –, zajímá je spíše štěstí celé společnosti. Etická rozhodnutí utilitaristů vycházejí z prosté, ale působivé otázky: *Dosahuji co největšího štěstí pro co největší počet lidí?* A minimalizuji tak bolest?

Tento přístup se jeví jako intuitivní; s tím, že svět by ocenil více štěstí a méně bolesti, by souhlasil každý a díky svému zaměření na výsledek je utilitarismus konkrétnější než pravidla a povinnosti deontologie. Vzhledem k tomu, že podle utilitarismu máme brát v úvahu celkovou sumu štěstí, nejen to naše, potřebují utilitaristé globální a inkluzivní pohled na svět. Řečeno slovy filozofa Henryho Sidgwicka, utilitarista musí brát v úvahu „úhel pohledu celého vesmíru". Utilitaristé se také musí přizpůsobovat okolnostem každého rozhodnutí. Čin, který zvyšuje štěstí v jednom kontextu, může v jiném kontextu způsobovat škodu; utilitarista musí každý případ posoudit

podle významu. Utilitaristé jsou proto přizpůsobiví a ochotní ohýbat tradiční morální pravidla, pokud tím zvýší bilanci štěstí, a zřejmě s nimi budete vycházet lépe než s jejich striktními deontologickými bratranci.

Zatím to tedy zní slibně, jenže jsou tu i problémy. Nutnost posuzovat budoucí štěstí a bolest každého člověka u každého jednotlivého činu – *utilitarismus konání* – zní naprosto neprakticky. Bentham navrhoval „kalkul prospěšnosti", rovnici, do níž by se přidávaly hodnoty štěstí. Odsuzuje nás tedy morálka k věčným výpočtům? Nenechají lidé aritmetiku aritmetikou a nespolehnou se na intuici, a nepopřou tak smysl celé záležitosti? Jak se vlastně štěstí měří?

Utilitaristé proto navrhli několik vylepšení. *Zásadoví utilitaristé* se s deontology shodují na tom, že nějaká morální pravidla potřebujeme, tvrdí ovšem, že si je máme spíše vybírat podle toho, kolik štěstí přinášejí, než vycházet z nějaké mytické morální pravdy. I zásadoví utilitaristé tedy zvažují štěstí a škodu, ovšem jen aby rozhodovali o pravidlech chování. Jakmile prý postavíme mimo zákon podvod, který poškozuje oběť i společnost, nemusíme už morálně posuzovat každý jednotlivý podvodný čin. *Preferenční utilitaristé* naproti tomu říkají, že štěstí je příliš požitkářské; lepší je jednat v souladu s preferencemi každého z nás. (Jak uvidíme v osmé kapitole, preferenční utilitarismus představuje cenný způsob, jak se dívat na etiku robotů.)

Někdy se utilitarismus potýká s potížemi, jak před útlakem ochránit jedince a menšiny. Chce-li 99 % obyvatel poslat do vyhnanství nebo popravit 1% menšinu, je mnohem snazší použít deontologický protiargument než ten utilitární. Tato „tyranie většiny" může pro utilitaristy představovat ošemetný problém. Podobně může být pro utilitaristu konání těžké argumentovat proti zabití jednoho člověka, pokud by jeho orgány zachránily pět lidí, nebo proti vyhození zločince ze záchranného člunu, pokud by se tak zachránil lékař.

Utilitarismus také podle všeho nechává bez povšimnutí pochybné chování, které nepůsobí škodu. Jestliže si školáci vyměňují kompromitující fotografie spolužačky bez jejího vědomí, je to špatně? Podle deontologů rozhodně ano: s dívkou se jedná jako s prostředkem dráždivosti, nikoli jako se samostatným účelem, a naší povinností je respektovat soukromí druhých. Jenže pokud to dívka nezjistí, pro utilitaristu může být odsouzení tohoto činu těžší: chlapcům se to líbí, bilance štěstí je tedy přece pozitivní, ne?

Typická utilitární obhajoba v těchto případech říká, že upírání spravedlnosti jednotlivci je celkově škodlivé, a jako společnost jsme pak méně šťastní. Přesto je zřejmé, že utilitarismus nás někdy přivádí k závěrům, jež se zdají morálně kontraintuitivní.

Vědecká mravnost

Technologická obec má utilitarismus obvykle v oblibě, částečně proto, že se zdá poněkud kvantifikovatelná. Proč ve světě, kde se většina rozhodnutí podřizuje datům, nekvantifikovat mravnost? Myšlence kvantifikace a dokazování lidských hodnot – „vědecké etice" – se v posledních letech daří. Sam Harris v knize *The Moral Landscape* (Morální krajina)[90] tvrdí, že díky pokrokům v neurovědě a ve výpočetní technice můžeme mít Benthamův kalkul prospěšnosti na dosah. Podle Harrise je věda spasitelkou etiky: velká data a několik dobře umístěných elektrod nám brzy s jistotou řeknou, které zákony a životní styly přinášejí lidem největší štěstí.

Myšlenka racionálního, vědeckého přístupu k etice není nic nového a mnoho etiků Harrise kritizovalo coby diletanta. Největší chybou v jeho uvažování je Humeova gilotina: morální poučení nelze odvodit z pohledu na data o tom, co *existuje*, což je přesně Harrisův záměr. Podle mě však chápání etiky jako další rovnice, kterou je třeba vypočítat, představuje smutné hledisko někoho, kdo jen řeší příklady. Toto hledisko totiž ignoruje nejdůležitější části etiky: dialog, konsensus, rozhodnost. Představa, že skener používaný při funkční magnetické rezonanci je nějakým nástrojem morálního osvícení, vědě i etice křivdí.

Utilitarismus, nebo deontologie?

Přestože utilitarismus má některé nepraktické slabiny a je náchylný k pseudovědeckým mylným výkladům, jde o důležitý etický model. Myšlenka maximalizace štěstí je mnohem přístupnější než vznešené představy o morální povinnosti a utilitarismus je obvykle zvláště užitečný při přemýšlení

[90] Sam Harris, *The Moral Landscape* (Simon & Schuster 2010).

o důsledcích toho, co je nové. Vládou podporované etické komise se k utilitárním hlediskům často uchylují například při posuzování dopadů inovací.

> Právní předpisy musí být při pohledu do budoucnosti víceméně utilitární. [...] Ve snaze rozhodnout, co by bylo nejlepší, musí být zákonodárci konsekvencionalisty [...] v úvahu je třeba brát každého člena společnosti a žádnému se nesmí věnovat zvláštní pozornost. – Mary Warnocková[91]

Chceme-li ukončit významné porušování etických pravidel u komunit, které již překročily hranice, může být vhodnější deontologický postoj. Deontologové i za cenu, že je občas budeme považovat za umíněnce, nakreslí do písku čáru, a stanoví tak jasná základní pravidla.

Uveďme obě tyto etické teorie do praxe na příkladu zařízení z blízké budoucnosti řízeného daty. Představte si inteligentní domácí hub, který se připojí k vašim domácím spotřebičům a zařízením vaší rodiny, bude sledovat například využití energie, vaše mediální návyky, polohy a zdravotní biometrii a umožní vám tyto údaje vizualizovat a využít je k automatizaci domácnosti, nastavení upozornění, rozsvěcení světel a podobně. Předpokládejme, že hub funguje s vaším plným souhlasem: přesně víte, jaké údaje shromažďuje a kam odcházejí. Výrobce toto zařízení rozdává zadarmo. Na oplátku se vám na displeji občas zobrazují cílené reklamy a inzerenti výrobci platí, kdykoli na reklamu zareagujete.

Zjistíte, jak se do zařízení nabourat a reklamy v domácím hubu vypnout. Vyžaduje to určité odborné znalosti – zařízení budete muset přepnout do privilegovaného režimu (rootovat) –, ale jste si jisti, že je pak dokážete zprovoznit. Je etické se do něj nabourat? Nabízí se určitá podobnost s dnešním blokováním webových reklam, o kterém se přehnaně diskutuje. Jedna strana tvrdí, reklamní technologie jsou tak nepřátelské, že jde prakticky o malware; reklamní průmysl kontruje tvrzením, že blokování reklam je krádež: „Každým blokováním reklamy ve skutečnosti odtrháváte dítěti sousto

[91] Mary Warnock, *An Intelligent Person's Guide to Ethics* (Gerald Duckworth & Co 2001).

od úst."[92] Použijme naše etické teorie k prohlédnutí této směšné rétorické mlhy.

Z utilitárního pohledu musíme zvážit pravděpodobné štěstí a bolest všech zúčastněných. Zaměřme se na tři zúčastněné strany: na vás (uživatele), na inzerenty a na výrobce hubu. Pro vás jako uživatele je hlavním ziskem soukromí: svůj osobní život můžete lépe skrývat a chránit před narušováním a pravděpodobně se ve výsledku budete cítit šťastnější. Vzhledem k tomu, že blokujete jen reklamy, nikoli sběr dat, je tento efekt většinou iluzorní, cenný však může být i pocit soukromí. Těžit budete též z toho, že vás nic nerozptyluje.

> V krátkodobém horizontu nám mohou rozptýlení bránit v tom, co chceme dělat. V dlouhodobém horizontu se však mohou nakupit a bránit nám žít tak, jak bychom chtěli. [...] To má na svobodu, blahobyt, a dokonce i na integritu našeho já silné etické dopady. [...] Otázkou by nemělo být, zda je blokování reklam etické, ale zda jde o morální povinnost. – James Williams[93]

Podle Williamse je blokování reklam sebeobrana, tedy téměř povinnost, máme-li znovu získat kontrolu nad tím, čemu věnujeme pozornost, a nad svým životem.

Co možné negativní dopady na uživatele? Jelikož jde o složité nabourání do systému, realizace může být frustrující a v případě neúspěchu můžete všechno pokazit. Existuje sice nebezpečí, že z toho budou mrzutosti, ovšem pro uživatele jde o čistě utilitární pozitivum.

Nabouráním do hubu sice inzerentům možná ušetříte pár dolarů – pokud reklamy nevidíte, nemůžete podle nich jednat –, ale jinak je to pro ně čisté negativum. Přijdou o povědomí o značce a o potenciální prodej, i když pokud jste blokování reklam nakloněni, nejspíše byste na ně stejně neklikli.

Dopad na výrobce je smíšený. Zařízení už máte a jeho nabouráním zlepšíte svou uživatelskou zkušenost a možná se tím zvýší i vaše loajalita

92 Opravdu. Viz Avram Piltch, „Why Using an Ad Blocker Is Stealing (Op-Ed)", *Tom's Guide*, 22. května 2015, tomsguide.com.

93 James Williams, „Why It's OK to Block Ads", blog *Oxford University Practical Ethics*, practicalethics.ox.ac.uk.

ke značce. Výrobci zůstanete jako zákazník a on vaše cenné údaje může s vaším souhlasem využívat i nadále. Přijde však o možnost získat kompenzaci. Pravděpodobně jde o čistou ztrátu, která však není tak zřejmá jako u inzerentů.

Nezapomeňte, že utilitaristé se ptají, zda čin maximalizuje čisté štěstí celé společnosti, což znamená vyvažování neslučitelných zájmů. To obvykle bývá politické téma. Pokud se zvýší štěstí veřejnosti, ale utrpí příjmy firem, jde o čisté dobro? V našem případu blokování reklamy to není jasné, ale protože si na náročné nabourání do hubu troufne jen málo lidí, škoda způsobená inzerentům a výrobci je zanedbatelná. Kvůli hrstce lidí, kteří se vyhýbají reklamě, zaměstnanci společnosti ve skutečnosti o štěstí nepřijdou.

Složitost podnikání a kapitalismu mohou při utilitárních diskusích působit jako vyrovnávací paměť: sotva lze tvrdit, že nadnárodní společnost pocítí ztrátu několika set dolarů, ovšem tato ztráta může získat konkrétnější podobu, pokud zaměstnanci začnou přicházet o prémie nebo o práci. Širší otázkou je, zda samotné firmě ubližuje rozhodnutí lidí vyvázat se z obchodních smluv; ať tak či onak, utilitarista by nejspíše dospěl k závěru, že toto nabourání je vcelku eticky přípustné. Pokud by bylo snadné, situace by zřejmě byla jiná. Pokud by reklamy blokovala polovina uživatelské základny, škody by prudce vzrostly: použitelnost technologie může změnit její utilitární dopad.

Deontologický argument zní poněkud jinak. Je v sázce nějaká morální povinnost? Ano: pravděpodobně máte povinnost dostát daným slibům. Souhlasili jste, že při instalaci zařízení inzerentům a výrobci poskytnete svá data a pozornost, ale teď se chcete odpíráním pozornosti z této dohody vykroutit. Co kdyby to, co se chystáte udělat, udělal každý? Kdyby reklamy blokovali všichni, výrobce by musel hub stáhnout, nebo ho spotřebitelům účtovat přímo, a potenciálně tak zvyšovat technologickou nerovnost. Ještě horší by bylo, že byste tak vytvořili precedens, že je v pořádku za spravedlivý podíl neplatit.

Co naše další deontologická zkouška: Jednáme s lidmi jako s prostředkem, nebo jako s účelem? Nabouráte-li se do hubu, zřejmě s druhými jinými lidmi jednáte jako s prostředky – technologii výrobce využíváte pro vlastní zisk a inzerenti vám ji jako prostředek umožňují získat zdarma, aniž byste jim to měli v úmyslu oplatit. Někteří aktivisté by správně namítli,

že reklamní průmysl jednal se spotřebiteli spíše jako s prostředkem než účelem celé roky, to je však pro tento konkrétní čin sotva relevantní. Podle deontologa je nabourání do hubu pravděpodobně neetické.

Máme tedy dvě etické perspektivy a každá se na vaše rozhodnutí dívá docela jinak. Utilitaristé zdůrazňují důsledky – v tomto případě dost malé –, zatímco deontology více zajímá podstata samotného činu a jeho rozpor s morální povinností. Oba pohledy mají samozřejmě své opodstatnění, i když jeden se vám může zdát přesvědčivější než druhý. Pokud to tak je, učinili jste první kroky k tomu, abyste pochopili, jakému etickému postoji dáváte přednost. S mými argumenty a závěry nemusíte dokonce ani souhlasit. Taková je totiž složitá a často frustrující podstata etiky: často existuje hned několik věrohodných odpovědí. Etické teorie nejsou nástroje do té míry jako objektiv, kterým se můžeme dívat na svět. Nelze jednoduše otočit klikou a zobrazit výsledky; podstatou etiky je spíše kladení správných otázek a diskutování o odpovědích. Cesta často bývá stejně důležitá jako cíl.

Spravedlivější výměna dat

Vraťme se k naší datové utopii: ke spravedlivé směně, při které lidé souhlasí s výměnou menšího množství údajů za cenné technologie. Jak by se dala uskutečnit?

Zaprvé musí mít technologický průmysl realistickou představu o skutečné hodnotě své práce. Je neudržitelné, aby firmy požadovaly větší množství údajů, aniž by nabízely skutečně užitečnější technologie. Přeceňování hodnoty technologií bude vyhlídky na spravedlivou směnu ohrožovat vždy; firma, která věří, že nabízí něco opravdu revolučního, bude pravděpodobně výměnou vyžadovat velké oběti na poli soukromí. Realismus, pokora a hluboké porozumění výhod pro reálný svět riziko vzniku nerovnováhy sníží.

Technologové by také měli mít za to, že data a algoritmy spolu nemilosrdně souvisejí. Sběr dat může působit jako abstraktní záležitost odtržená od svých dopadů, ovšem při každém rozhovoru o tom, jak se údaje získávají, musí zaznít otázka, k čemu se budou používat. I když jsem tato dvě témata rozdělil do několika samostatných kapitol, v praxi mají škody způsobené algoritmy původ ve škodách způsobených daty.

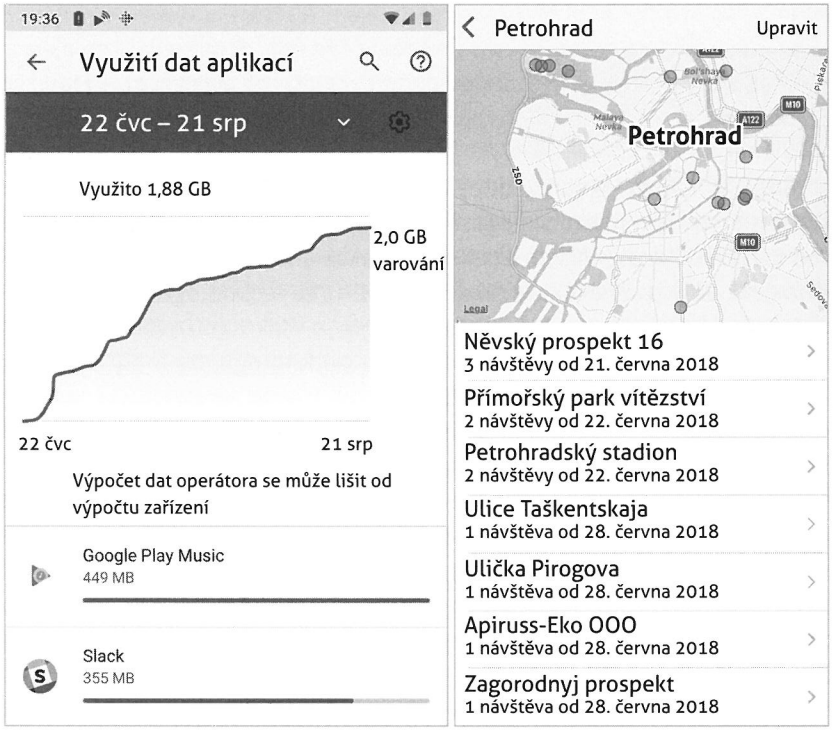
> Když slyším, že „je etické vytvářet aplikace AI, které u některých masivně agregovaných databází provádějí činnost X", mám chuť se zeptat, zda je vůbec etické danou databázi masivně agregovat. – Matt Blaze[94]

Snad je klíčem ke spravedlivé výměně dat snaha zacházet s nimi jako s materiálem, nikoli jako s magií. Magie představuje pro technologie lákavou metaforu; designéři jsou celí žhaví zákazníka potěšit a minimalizovat jeho úsilí, až je pro ně lákavé dospět k závěru, že technologie by měly fungovat téměř nadpřirozeně. Podstatou magie je však zamlčování informací, skrývání mechanismů triku. Představa, že technologie by měly být něco jako magie, lidi odrazuje od toho, aby zkoumali jejich fungování; ve výsledném informačním vakuu pak nemohou činit informovaná rozhodnutí. Jak řekl výtvarník James Bridle: „Ti, kteří síť nevnímají, na ní nemohou efektivně jednat a jsou bezmocní."

Při spravedlivé výměně údajů by uživatelé měli vědět, jak jejich technologie údaje získávají a přenášejí sítí. Zásady ochrany osobních údajů nestačí: jde o právní, nikoli komunikační nástroje. Určitě je lepší upozornit na datové toky v rámci samotných produktů. Někteří to označují za „datovou transparentnost", ale myslím, že právě tohle je špatné rámování. Místo zprůhledňování bychom data měli *zhmotnit*. Jen když je přetáhneme do viditelného spektra, když dáme jejich přízračnosti podobu, umožníme uživatelům, aby jim porozuměli. Zhmotnění údajů také lidem usnadňuje zasáhnout, pokud systém shromažďuje nežádoucí nebo nesprávné informace.

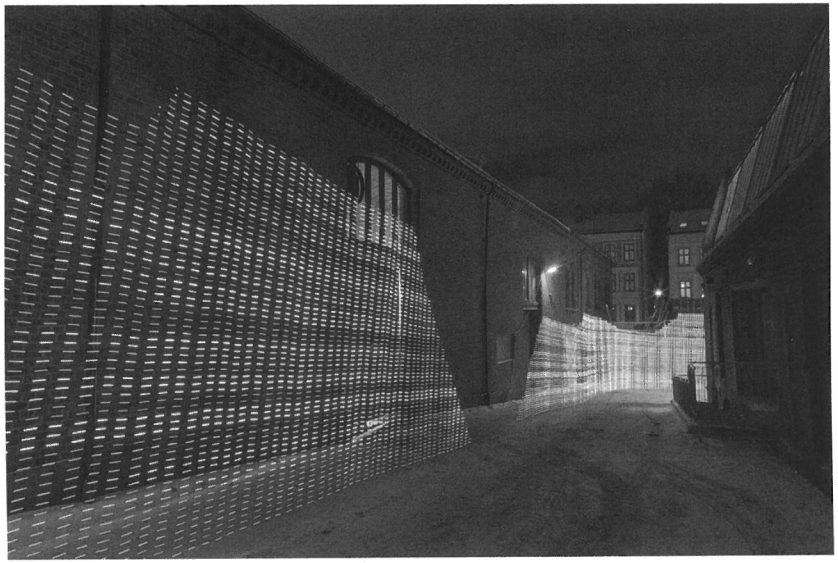
Technologie dnes data zhmotňuje špatně. Hlasoví asistenti tápou i u přímočarých otázek na ochranu soukromí typu: „Co o mně víš?" nebo „Kde ukládáš moje data?" Prosté shrnutí s odkazem na podrobnější vysvětlení by zvýšilo důvěru a datovou gramotnost. Valná část dnešních grafických vizualizací je uhlazená a složité datové toky redukuje na jednu ikonu či graf nebo přináší hrubé zobrazení údajů až po akci.

[94] Matt Blaze (@mattblaze), Twitter, 3. února 2018.



Obrazovka využití dat v systému Android Oreo (vlevo) ukazuje čistou spotřebu v megabytech, což je užitečné pro předpověď účtu za telefon, ovšem o tom, zda se s danými údaji obchoduje spravedlivě, vám nic neřekne. Obrazovka historie poloh v systému iOS 11 (vpravo) přináší hrubější rozpis dat, ale samozřejmě pouze zpětně.

Timo Arnall, Jørn Knutsen a Einar Sneve Martinussen v projektu *Immaterials* (Nehmotnosti) zhmotnili městskou síť Wi-Fi pomocí „malování světlem". Obraz vznikl připojením dlouhé tyče s diodami LED k detektoru Wi-Fi a pečlivým měřením signálu v pravidelných intervalech. Fotografie pořízené při dlouhé expozici zachycují intenzitu pole podél městských ulic, a vytvářejí tak snímek odhalující složitou neviditelnou datovou infrastrukturu, jejíž vrcholy, mrtvé zóny a přechody prostupují náš svět. Tyto fotografie nám umožňují pochopit, že digitální a fyzický



Immaterials: WiFi Light Painting (Nehmotnosti: Wi-Fi malování světlem, 2011) autorů Tima Arnalla, Jørna Knutsena a Einara Snevea Martinussena. Přetištěno s laskavým svolením autorů.

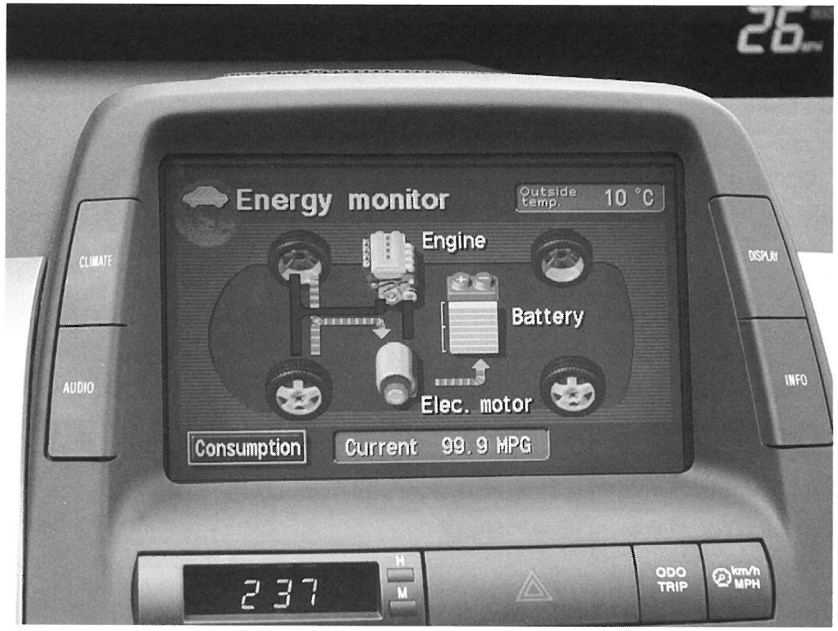
prostor jsou jedno a totéž, a podněcují naši touhu zjistit, co se ještě děje za našimi prahy vnímání.

> Vzhledem k tomu, že čím dál víc obýváme technické systémy a jejich prostřednictvím ustanovujeme společnost a kulturu, se zdá nebezpečné, že o jejich fungování víme tak málo. Zviditelnění materiálu technologické infrastruktury je prvním krokem k porozumění. To, co nevidíme, nelze kriticky zhodnotit. – Timo Arnall[95]

Mohli bychom z tohoto díla čerpat inspiraci, na jeho základě vytvořit hrubý rozpis poloh v systému iOS, a nabídnout tak v reálném čase přehled

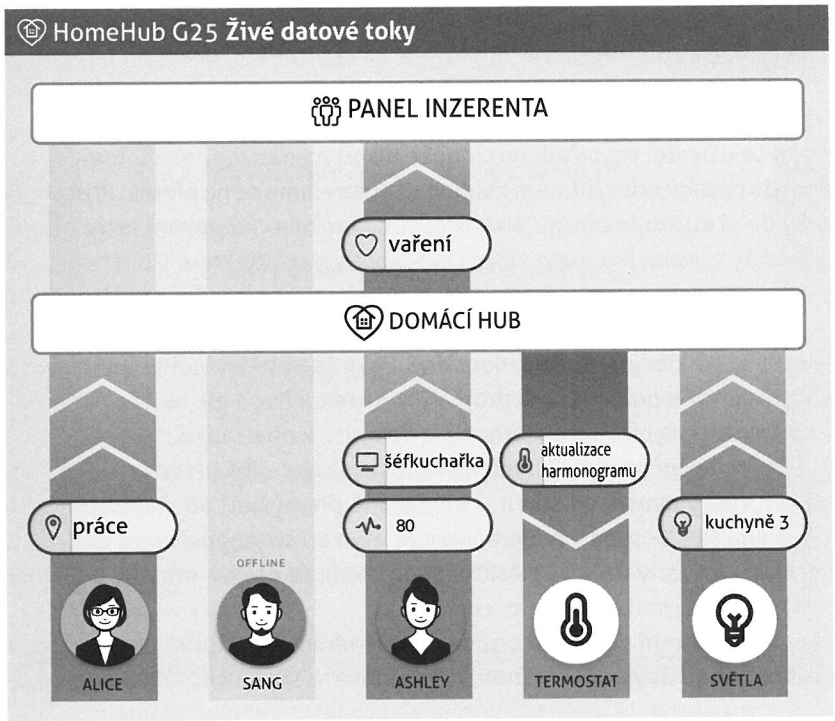
95 „Immaterials artist Timo Arnall on seeing the invisible", *Lighthouse*, 9. června 2015, lighthouse.org.

o stavu a pohybu dat? Kdyby uživatelé měli kdykoli možnost zobrazit data kroužící kolem nich – nebo přehled výměny údajů, jíž se chystají zúčastnit –, své kroky by si lépe spojovali s jasnými důsledky a činili by informovanější rozhodnutí.



Monitor spotřeby energie ve voze Toyota Prius, 2003.

V analogovém světě se dnes takovému snímku snad nejvíce blíží monitor spotřeby energie na přístrojové desce hybridního vozu. Tento náhled šikovně ukazuje, jak se jiná neviditelná entita – energie – pohybuje automobilem, a udává směr jejího toku, rychlost změny a rezervy. Monitor poskytuje okamžitou zpětnou vazbu na základě kroků řidiče, umožňuje mu lépe pochopit, jak auto spotřebovává energii, a podporuje styl jízdy zvyšující hospodárnost. Pokusme se o podobný grafický návrh pro náš imaginární inteligentní domácí hub.



Tento panel zobrazuje, jak se data prokousávají systémem, a našim hypotetickým uživatelům tak umožňuje se dozvědět, jaké údaje systém shromažďuje, k jakým závěrům hub dospěl a které datové toky jsou v současné době aktivní. Zobrazuje také, která zařízení s hubem komunikují – a umožňují mu ladění chyb (debugging), pokud vše nefunguje podle očekávání –, a rodinným příslušníkům dává možnost přejít na jednotlivé datové toky a ty pak rychle opravit nebo odstranit. Panel se tedy do jisté míry snaží zajistit spravedlivější výměnu dat: uživatelé přesně vidí, které údaje vyměňují za užitečnost hubu. Hub si nemůže zkrátka urvat tolik dat, kolik chce; spoléhá spíše na pochopení a souhlas.

Obrazovka nemusí být pro toto zhmotnění tím nejlepším plátnem; jako vhodnější možnost se jeví převést údaje do skutečného světa pomocí rozšířené reality. Bez ohledu na rozhraní by však etická hodnota zobrazení

datových toků měla být jasná. Nejenže uživatelé lépe porozumí dohodě, kterou uzavírají, ale snadněji také odhalí potenciální rizika.

Někdy je vhodné na tato rizika upozornit. Řečeno terminologií Martina Heideggera,[96] designéři obvykle usilují o technologii *příručnosti*. V tomto stavu se uživatel soustředí na činnost, nikoli na nástroj. Technologie ustupuje do pozadí: odmyslíme si kladivo a soustředíme se na hřebík. Přístup na základě příručnosti odvádí pozornost od vnitřního fungování technologií; pokud by však technologie mohly být škodlivé, což ty, které slouží ke sběru dat, někdy jsou, rámování příručností toto nebezpečí ještě zamlží zevnitř.

Oproti tomu nástroj, který se *vyskytuje* (parafrázujeme-li Heideggera), je nástroj, na který narazíme mentálně. Pokud se hlava kladiva uvolní, jsme nuceni věnovat pozornost nástroji. Výskytové technologie nejsou prostředkem činnosti: vybízejí k pozornosti, a dokonce k opatrnosti.

Projektování analyzující tok uživatelských dat – jež přechází od příručnosti k výskytovosti, od stavu „nenuťte mě přemýšlet" ke stavu „přinuťte mě přemýšlet" – představuje důležitou etickou strategii. Pokud designéři nechtějí, aby uživatelé náměsíčně vstupovali na datové minové pole, neměli by napětí snižovat, ale zvyšovat.

Toto rozhraní souhlasu odporuje základním principům použitelnosti tím, že napětí zvyšuje. Technologie se stává *výskytovou*, vyžaduje pozornost a pro uživatele je těžší ochromeně předat velmi osobní údaje.

Vysoce sporné transakce a snímky dat v reálném čase by mohly narovnat pravidla datové hry, pouhým odhalením datových toků však spravedlnosti nedosáhneme. Systém sice může odkrýt, jak údaje shromažďuje, tato činnost přesto může být stále nepokrytě nespravedlivá. Je přitom pozoruhodné, kolik škodlivých postupů se již v technologickém průmyslu rozšířilo. Doufat ve spravedlivou výměnu údajů ovšem nelze, dokud aplikace nonšalantně vyžadují celé adresáře či sdílení polohy, i když jsou vypnuté. Sběrači

[96] Martin Heidegger, *Being and Time* (Max Niemeyer Verlag Tübingen, 1927). (Česky: Martin Heidegger: *Bytí a čas.* Přel. Ivan Chvatík, Pavel Kouba, Miroslav Petříček, Jiří Němec. Praha: Oikoymenh, 2008 – pozn. překl.) Žádná kniha o etice nemůže Heideggera zmínit, aniž by se zabývala jeho fašismem a antisemitismem. Heidegger byl řadu let členem nacistické strany a podle všeho toho do své smrti nikdy nelitoval. Zapeklitý problém, zda by jeho odporná politika měla snižovat význam jeho filozofického náhledu, mohu jen vzít na vědomí, nikoli ho vyřešit; inteligentní kritiku nabízí článek Joshuy Rothmana „Is Heidegger Contaminated by Nazism?" v časopise *New Yorker.*

dat vždy nedává etické rozhřešení ani předchozí souhlas. Skandál společnosti Cambridge Analytica ukázal, že postupy, které se u aplikací kdysi tolerovaly – například udělení přístupu k celé síti přátel –, mohou v pozdějších letech šokovat. S nárůstem datové gramotnosti veřejnosti a s tím, jak jsou datová rizika zřejmější, se posunulo také očekávání v oblasti ochrany soukromí a dřívější rozhodnutí Facebooku se dnes jeví jako nezodpovědná. Bez ohledu na souhlas s podmínkami použití zřejmě Facebook porušil povinnost dbát na zájmy uživatelů.

Zde může být užitečný Rawlsův závoj nevědění. Chceme-li navrhovat spravedlivé systémy, měli bychom předstírat, že nevíme, jakou roli v systému převezmeme. Byli bychom s dohodou spokojeni stejně v pozici uživatele jako v pozici inzerenta? Co kdybychom byli uživatelem ze skupiny nedostatečně zastoupených obyvatel či uživatelem, který se již setkal s datovou diskriminací a odmítnutím služeb?

Sebevlastnictví a umělá inteligence do kapsy

Přimhouříme-li oči, vývoj výpočetní techniky uvidíme jako oscilaci mezi blízkým a vzdáleným.[97] Mohutný sálový počítač zplodil stolní počítač a přinesl globální internet; díky mobilům se internet stal osobní záležitostí, než převládl takzvaný cloud computing. Cloud je samozřejmě praktický eufemismus, zkrácené označení pro „počítače jiných lidí". Ať vznikají data kdekoli, obvykle se zpracovávají centrálně, v datových centrech zaskládaných servery s výkonnými grafickými procesory.

Tato centralizace dnes přináší řadu rizik souvisejících s ochranou soukromí: jakmile se data ze zařízení uživatele vypaří, mají tendenci mizet v mlze. Snad se kyvadlo znovu zhoupne směrem k lokálním technologiím. Vzhledem k tomu, že výkon přenosných zařízení roste a hardware pro strojové učení zlevňuje, je možné, že výpočetní procesy se znovu začnou decentralizovat. Místo nalévání dat do rozsáhlých soukromých rezervoárů by uživatelé data bezpečně uchovávali ve vlastních zařízeních, spravovali je pomocí uživatelsky přívětivých aplikací typu

[97] Amber Case, „Calm Technology: Design for the Next Generation of Devices", přednáška na konferenci *TNW* 2017.

peněženky a podle potřeby by k nim udělovali licenci. Tak by nevznikala zranitelná centrální datová úložiště a uživatelé by místo toho získali pravomoc udělovat, odebírat a revidovat souhlas dle libosti. Přidáme-li k tomu přístupy *umělé inteligence do kapsy*, jež slibují zvládnutí výcviku a inference umělé inteligence přímo v zařízení, začíná to vypadat jako utopie aktivisty za ochranu osobních údajů. Uživatel má plnou kontrolu při minimálním přenosu dat a menším riziku neviditelného zneužití. Výsledné systémy budou navíc mít nižší latenci a umožní práci v režimu offline.

Vlastnictví dat a jejich zpracovávání v zařízení je krásný sen, který se však nikdy nemůže zcela uskutečnit. Vlastnictví zřídka bývá binární; datové drama se nevyhnutelně týká mnoha subjektů. Některé transakce neumožňují výměnu dat odmítnout – například daňové úřady a lékaři naše informace potřebují, aby s námi mohli správně jednat – a spousta osobních údajů je mimo naši kontrolu v seznamu kontaktů přátel, v záznamech státních kamer nebo ve složkách zaměstnavatelů. I při jednoduchých úkolech vznikají konkurenční nároky na údaje. Dobíjím-li si elektromobil, patří údaje o dobíjení – množství využitých kWh, délka nabíjení, kapacita – mně, výrobci vozu, nebo mému dodavateli energie?

Decentralizace může data také rozkouskovat a snížit jejich užitečnost. Jak podotýká analytik Benedict Evans, data jsou daleko cennější ve velkém měřítku:

> Každý člověk pravděpodobně přispívá jen miliontinou údajů, jež jsou nezbytné pro jakýkoli úkol. [...] Tyto datové body mají význam pouze v souhrnu milionů, a to pro čtyři až pět nesouvisejících firem. Jak bych je mohl „vlastnit"? Co bych s nimi proboha dělal?[98]

Umělá inteligence do kapsy je ještě daleko. I když vývoj v oblasti zpracovávání dat v zařízení povzbudivě pokročil – rozpoznávání obličejů v aplikaci Photos společnosti Apple probíhá výhradně v uživatelských zařízeních a Google má v úmyslu se při svém vývoji umělé inteligence zaměřit především na ně –, úkoly strojového učení, například rozpoznávání řeči a počítačové vidění, jsou výpočetně náročné. Výcvik hluboké neuronové

[98] Benedict Evans (@benedictevans), Twitter, 31. prosince 2017.

sítě může i na výkonném serveru trvat celé dny. Dokud osobní zařízení, omezená velikostí a výkonem baterie, nezvládnou inferenci a výcvik sama, decentralizace může inovacím v oblasti umělé inteligence bránit. Největší nadějí se jeví *federativní učení*, jež vyžaduje, aby zařízení při výcviku spojila síly, i když údaje zůstanou v jednotlivých zařízeních.

Utopie o vlastnictví údajů by také mohla znamenat problémy pro služby financované reklamami. Licencování údajů by některým uživatelům – pravděpodobně těm nejbohatším – umožnilo odhlásit cílenou reklamu, což by zlikvidovalo reklamní sazby a potenciálně ohrozilo životaschopnost celého modelu. Svět BYOD (přines si své zařízení, angl. Bring Your Own Device) by urychlil vznik dvouúrovňové digitální společnosti, ve které by bohatí platili za soukromí a masy by musely odevzdávat své údaje. Tímto směrem se do určité míry ubírá trh s chytrými telefony, přičemž iPhone má postavení zařízení pro náročné, u něhož je soukromí na prvním místě, a Android nabízí cenově dostupnější, ale uvolněnější datový ekosystém. Představa soukromí jako luxusního statku by nás měla znepokojovat, protože napomáhá jen těm, kteří už mocní jsou.[99] Přidáme-li k tomu výzvy decentralizovaného světa související s uživatelskou zkušeností – budou tradiční uživatelé kvůli tak nejasné výhodě tolerovat náklady na skladování a komplikované úkony související s datovou hygienou? –, naprostá decentralizace se zdá nepravděpodobná.

Možná spíše skončíme u nějaké kombinace ukládání a zpracovávání dat v zařízení i mimo ně. Telefony se systémem Android již řeč zhruba rozpoznávají místně a pro vyšší přesnost pak zvuk odesílají do cloudu. Bude-li trénink mobilních zařízení příliš náročný, zařízení podobná stolním počítačům může čekat budoucnost osobních serverů, jež budou zpracovávat data a trénovat umělou inteligenci místo jiných zařízení uživatele. Úkoly budou lépe přizpůsobené pro zařízení, ale všechno zůstane stále pod kontrolou uživatele a žádná data do cloudu odcházet nebudou.

99 Natalie Kane, „Private Data Is the Ultimate Luxury Good", *VICE Motherboard*, 27. září 2016, motherboard.vice.com.

Přenositelnost a diferenciální ochrana soukromí

Zatím se zdá pravděpodobnější, že vsadíme spíše na přenositelnost dat než na jejich vlastnictví. Pokud se uživatelům nabídne možnost stáhnout a znovu použít osobní údaje, mohou opět získat pocit kontroly a rovnováhy, technologickým gigantům se však toto řešení nebude prodávat snadno. Přenositelnost dat spotřebitelům usnadňuje změnu poskytovatele, proto se ji firmy obecně zdráhají nabízet. Na významu pravděpodobně získá, pouze pokud ji bude vyžadovat zákon; základní požadavky na přenositelnost dat například obsahuje nařízení GDPR.

Většina technologických firem by raději uchovávala cenná data centrálně, ale uživatele ujišťovala, že centralizace je bezpečná. Firmy k tomu mohou využívat techniky, jako je *diferenciální ochrana soukromí*, jež k datům přidává měřitelné množství statistického šumu tím, že některé otázky nahrazuje jinými, se známou mírou odezvy („V jakém měsíci jste se narodil/a?"). Uživatelská data se tak předtím, než dorazí na server, zamlží, a protože nelze zjistit, kteří uživatelé dostali které otázky, jejich zpětná identifikace se stává obtížnější.

Velký zájem o diferenciální ochranu soukromí má společnost Apple, která ji nejprve využívá k analýze používání klávesnice a emodži a poté k zabezpečení procházení historie a údajů týkajících se zdraví. Někteří analytici však pochybují, zda Apple slíbenou diferenciální ochranu soukromí poskytuje. Efektivita diferenciální ochrany soukromí totiž závisí na množství detailních informací, které je firma ochotna obětovat a které stručně vyjadřuje „hodnota epsilon", tedy v podstatě míra ztráty soukromí. Vědci zjistili, že společnost Apple využívala nižší hodnoty epsilon, než se očekávalo, a na rozdíl od konkurence je navíc udržuje v tajnosti, což znamená, že je těžké zjistit, jak dobře soukromé údaje zamlžuje.[100] Frank McSherry, jeden z vynálezců diferenciální ochrany soukromí, se k tomu vyjádřil velmi kriticky: „Společnost Apple nakládání s vašimi údaji svázala nějakými

100 Jun Tang et al, „Privacy Loss in Apple's Implementation of Differential Privacy on MacOS 10.12", arxiv.org/abs/1709.02753.

pouty. Ukazuje se však, že ta pouta jsou z hedvábného papíru."[101] Společnost Apple naproti tomu zjištění vědců odmítla jako neúplná.

Apple však podniká dobré kroky na podporu ochrany soukromí alespoň u jiných technologií. Výrobci hardwaru a operačních systémů mají ideální možnost změnit datové a bezpečnostní postupy používané ve světě. Softwarové technologie na podporu ochrany soukromí (PET), jako jsou správci hesel a dvoufaktorového ověřování, sice coby spotřebitelské technologie v podstatě selhávají – například dvoufaktorové zabezpečení údajně používá necelé 1 % uživatelů služby Dropbox –, jejich přenos do zařízení je ale nesmírně efektivní. Dotykové senzory Apple ID umožnily nárůst využití přístupového kódu k systému iOS z mizerných 49 % na 89 %[102] a šifrování typu end-to-end se stalo nezbytnou součástí aplikací iMessage a FaceTime i služeb třetích stran, například Signal.

Téměř každá technologie na podporu ochrany soukromí vyvolává protichůdné reakce. Inteligentní protokoly preventivního sledování prohlížeče Safari omezují soubory cookie třetích stran k radosti věrných uživatelů, ale ke vzteku inzerentů, kteří prskají, že společnost Apple narušila internetovou ekonomiku. Vlády a policejní sbory technologické společnosti opakovaně žádají, aby ve jménu národní bezpečnosti oslabily bezpečnostní opatření, a následovat mohou zákony proti šifrování. V boji o soukromí je obvykle nutné postavit se na jednu stranu.

Zásadní bezdatová alternativa

Zpracovávání dat v zařízení a diferenciální ochrana soukromí jsou slibné techniky, ale stejně jako každý technologický přístup s sebou nesou riziko přikrašlování postupů, jež jsou stále škodlivé. Jathan Sadowski pochmurně předpovídá, že kybernetická bezpečnost „jen odkládá katastrofální selhání". Autorka Zeynep Tüfekçi tvrdí, že smysluplný individuální souhlas

[101] Andy Greenberg, „How One of Apple's Key Privacy Safeguards Falls Short", *WIRED*, 15. září 2017, wired.com.

[102] Ivan Krstić, „How iOS Security Really Works", přednáška na konferenci *Apple Worldwide Developer Conference* 2016.

je zkrátka nemožný, protože lidé netuší, jak firmy s jejich údaji nakládají v současnosti ani jak s nimi budou nakládat v budoucnosti.

Je sice správné se ptát, jak můžeme uživatelské údaje zpracovávat bezpečně, zásadní otázka však zůstává: Měli bychom uživatelské údaje vůbec shromažďovat? Některé firmy se rozhodly, že náklady a rizika jim za to nestojí. Pokud se data stávají toxickým závazkem, nejlepší strategií je vůbec s nimi nemanipulovat. Britský řetězec hostinců Wetherspoons v roce 2017 celou svou e-mailovou databázi smazal. Nemuselo však jít tak docela o ušlechtilý čin: dva roky předtím firma kvůli úniku dat přišla o záznamy 650 000 zákazníků. Někteří analytici spekulovali, že problémy s databází způsobily, že firma Wetherspoons přišla o záznamy souhlasů, což ji přimělo k tomu, že se e-mailového marketingu raději úplně vzdala, než aby se souhlasy snažila náročným způsobem získat znovu.

Zásadní bezdatová alternativa je snazší pro řetězce hostinců než pro technologickou firmu, ovšem rozhodnutí neshromažďovat údaje je nejlepší možnou ochranou proti opětovné identifikaci, a ať už jde o akt bezpečnosti, nebo protestu, má velký politický význam. Eticky smýšlející technologové by měli odmítnutí sběru dat zvážit, pokud si myslí, že by tím mohli způsobit újmu nebo poškodit uživatele v případě, že jim tyto údaje zabaví úřady. Například údaje o rasovém původu lze využít k zachovávání předpojatosti, což může být argument pro to, aby se – stejně jako jiné údaje, jež lze využít k opětovné identifikaci nebo interpolaci rasového původu – neshromažďovaly, pokud by se tím toto riziko snížilo. Nikdo nemůže předat údaje, které nikdy neměl. Snad bychom se na data měli dívat vývojářovou optikou postupného zlepšování: dobrý software by měl dobře fungovat i bez nich a s nimi by měl fungovat ještě lépe.

Odmítači dat v podstatě uplatňují *princip předběžné opatrnosti*. Předběžná opatrnost, tedy formalizovaná podoba úsloví „jistota je jistota", převrací důkazní břemeno a umožňuje nám jednat pouze tehdy, máme-li jistotu, že tím nemůžeme nikomu uškodit. U vysoce rizikových oborů, například ochrany životního prostředí, lékařství a bezpečnosti potravin, bývá předběžná opatrnost běžná, tento princip však jde proti rozvratnému charakteru technologického průmyslu a většinou by zbytečně protahoval rozhodování. Pokud však existuje značná pravděpodobnost, že ke škodě dojde, předběžná opatrnost může být stále na místě.

Ochrana soukromí jako strategie

Datovou etiku je důležité vidět nejen jako věc snižování rizik souvisejících se zabezpečením či s dodržováním předpisů, ale také jako zdroj inovací a konkurenční výhodu. Takový je dnes přístup společnosti Apple, která doufá, že se dlouhodobým zaměřováním na ochranu soukromí a tím, že se technologie PET staly základem její nabídky a marketingu, odliší od společnosti Google a v menší míře od Facebooku a Amazonu.

I když už nastal čas, aby významná technologická firma vystupovala jako zastánce ochrany soukromí, rétorika společnosti Apple částečně končí v opotřebovaných pastech kapitalismu sledování a postoje konkurence spíše zkresluje. Proto není těžké být k tomuto využívání etiky jako zbraně trochu skeptický. Jak naznačuje analytik Ben Thompson, nikoli náhodou etický postoj společnosti Apple prospívá jejímu podnikání, jehož podstatou je spíše prodej hardwaru s vysokou marží než dosah a monetizace dat.

> Mnohem více na mě zapůsobí firma, která dělá něco v souladu se svými „hodnotami" a „zásadami" a která jde proti svému obchodnímu modelu, než firma, jíž obchodní model usnadňuje získávat body v oblasti PR.[103]

Ze skandálů souvisejících s datovou etikou nejvíce těží Apple a podobné společnosti zaměřené na ochranu soukromí; čím větší je odpor veřejnosti a tisku, tím snadnější je prosazovat strategii ochrany osobních údajů. Dnes je společnost Apple vnímána jako ta, která stojí za umělou inteligencí, a musí doufat, že její designové a technologické intervence v dlouhodobém horizontu ukážou, že už je na druhém břehu.

Správná ochrana soukromí a dat má reklamní i marketingové výhody, je to však také dobrá strategie. Je totiž podstatou *ochrany soukromí jako aspektu designu* (privacy by design), který vymyslela Ann Cavoukianová, bývalá komisařka pro ochranu soukromí kanadské provincie Ontario. Ochrana soukromí jako aspekt designu zavádí sedm designových principů pro začlenění etických přístupů k údajům do podnikání:

[103] Ben Thompson, „Facebook's Earnings, Facebook's Strategy Credit (and Apple's), Facebook and the Future", *Stratechery*, 2. listopadu 2017, stratechery.com.

1. iniciativa, nereaktivnost; prevence, nenáprava,
2. ochrana osobních údajů jako výchozí nastavení,
3. soukromí začleněné do designu,
4. plná funkčnost – pozitivní, nikoli nulový součet,
5. zabezpečení typu end-to-end – ochrana během celého životního cyklu,
6. viditelnost a transparentnost – zachovejte otevřenost,
7. respekt vůči soukromí uživatelů – zaměřte se na uživatele.

Ochrana soukromí jako aspekt designu je dobře zavedena coby dobrovolný osvědčený postup; nařízení GDPR vyžaduje, aby firmy podobný proces dodržovaly a dokázaly, že ochranu údajů občanů EU braly v úvahu již ve fázi návrhu. Proto má smysl, aby technologické firmy přijaly ochranu soukromí jako aspekt designu za celosvětový standard. Alternativa – vytváření samostatných systémů pro občany EU a jiných zemí a následné větvení databází kódů a zásad – nepochybně osloví pouze ty firmy, které ochrana soukromí ohrožuje. Není překvapením, že tuto cestu zvolily některé datové zprostředkovatelské firmy, jež se zoufale snaží ochránit část svého podnikání spoléhajícího na laxní regulaci; některé technologické firmy podnikající v reklamě se raději rozhodly ukončit provoz v Evropě úplně, než aby soukromí jako aspekt designu přijaly. Pro etickou technologickou společnost by však soukromí a datová etika měly být jasnou strategickou sázkou na jistotu.

Posílení role veřejnosti

Všechny tyto návrhy se zaměřují na průmysl a samy o sobě nemohou poskytnout všechny odpovědi. Je jen správně, že by o směřování našeho datového světa měla rozhodovat veřejnost. Souhlas spotřebitele bohužel přispívá k tomu, že dochází k těm nejhorším případům zneužití. Bezohledným firmám (a vládám; viz šestá kapitola) zneužívání údajů prochází, protože narážejí na malý odpor široké veřejnosti. Není to však její chyba. Tisk pojednává datová témata tak nezáživně, případy porušování jsou tak časté a možností postihu je tak málo, že veřejnost nad problémem mávla rukou. Přestože přetrvávají obavy, co se s osobními údaji stane, většina lidí možné

důsledky nedohlédne, snad s výjimkou krádeže identity, což je sám o sobě abstraktní pojem zahrnující celou řadu podvodů.

Nemá smysl se domnívat, že veřejnost by měl současný stav dat přivádět k zuřivosti; i když bychom se před zneužitím dat měli mít na pozoru vždy, spravedlivá a konsensuální výměna údajů umožní, aby se cenné technologie dostaly do rukou miliard lidí. Technologové by si jen naběhli, kdyby vyvolávali odpor proti všem inovacím závisejícím na datech. Udělají lépe, budou-li se zabývat tím, proč je veřejnost vůči datům lhostejná.

K hlavním příčinám této lhostejnosti patří nedostatek porozumění; nejúčinněji veřejnost zapojíme tím, že podpoříme její znalosti v oblasti dat a její sebedůvěru. Pomůže nám jak zhmotnění dat, tak nabízení technologií na podporu ochrany soukromí (PET) a vysvětlování jejich hodnoty. Měli bychom se však také pokusit zvýšit informovanost veřejnosti prostřednictvím vzdělávání a zpravodajství. Technologové musí upozorňovat i na jiné problémy s daty než na problémy se zabezpečením; mohou nabídnout více než jen obrázky visacích zámků. Měli bychom se snažit vytvořit přesvědčivý veřejný a politický narativ o roli dat v naší budoucí společnosti a zabývat se jejich rostoucím významem a hodnotou („Dostáváte za ně spravedlivou kompenzaci?"), riziky, jež předpokládané a agregované údaje mohou vytvářet, a hrozbou algoritmické nespravedlnosti způsobené zneužíváním údajů.

Toho lze dosáhnout tím, že využijeme politický proces. Zainteresovaní technologové mohou spoluutvářet státní datovou politiku tím, že se budou podílet na konzultacích, psát voleným zástupcům, či dokonce kandidovat. Ti, kteří k politice tolik netíhnou, mohou vytvářet řadu technologií. Technologie na podporu ochrany soukromí (PET), například blokátory reklam (jsou-li etické!), anonymizéry, jednorázové účty, šifrovací software a nástroje pro automatizaci žádostí podle zákona o ochraně údajů, zvýší informovanost veřejnosti a její odolnost. Vždy budou zapotřebí také alternativy ke službám pro získávání údajů, jež budou sloužit jako zářné příklady toho, jak lze s údaji a se soukromím zacházet spravedlivě.

5

Pohled novýma očima

Donedávna jsme předpokládali, že mají-li stroje porozumět fyzickému světu, svět jim bude muset dobrovolně poskytnout informace. K tomu bychom potřebovali lidské kartografy – informační architekty a další mistry taxonomie a označování – i celou řadu automaticky se popisujících a hlásících se objektů („spimes"), jež by neustále vysílaly informace o svém stavu.

Zdá se však, že to již není nezbytné. Jak naznačuje teorie zprostředkování, každá inovace přináší nové způsoby interpretace světa. Rodící se technologie jsou čím dál schopnější získávat informace z fyzického světa jednostranně tím, že ze stínů vytahují to, co bylo dříve neviditelné.

Počítačové vidění

Nejdůležitějším vstupním zařízením příštího desetiletí budou kamery: ještě levnější a menší, namontované v osobních zařízeních, v našich obývacích pokojích, na dronech i v našich ulicích. Podle odhadů jedné firmy jejich počet do roku 2022 dosáhne 45 miliard, což představuje nárůst o 220 % za pouhých pět let. Za peníze si dnes koupíte denní satelitní záběry odkudkoli na světě, nositelné fotoaparáty budou brzy přenášet miliony tváří