Brian W. Kernighan

JAK POROZUMĚT DIGITÁLNÍMU SVĚTU

Vše, co potřebujete vědět o internetu, bezpečnosti a soukromí

argo / dokořán

Brian W. Kernighan

JAK POROZUMĚT DIGITÁLNÍMU SVĚTU

Vše, co potřebujete vědět o internetu, bezpečnosti a soukromí

ARGO / DOKOŘÁN

Brian W. Kernighan

JAK POROZUMĚT DIGITÁLNÍMU SVĚTU

Vše, co potřebujete vědět o internetu, bezpečnosti a soukromí

Druhé vydání v českém jazyce (první elektronické).
Z anglického originálu *Understanding the Digital World. What You Need to Know about Computers, the Internet, Privacy, and Security* přeložil Petr Holčák.
Odpovědný redaktor Zdeněk Kárník.
Redakce Marie Černá.
Obálka a sazba Michal Puhač podle návrhu Pavla Růta.
Vydalo v roce 2020 nakladatelství Dokořán, s. r. o.,
Holečkova 9, Praha 5, dokoran@dokoran.cz, www.dokoran.cz,
jako svou 1037. publikaci (318. elektronická).

ISBN 978-80-7363-977-8

Věnováno Meg

OBSAH

PŘEDMLUVA

Od podzimu 1999 učím na Princetonské univerzitě studijní předmět nazvaný „Počítače v našem světě". Název kurzu je trapně mlhavý, musel jsem ho ale vymyslet během pěti minut a pak už jej bylo těžké měnit. Vedení kurzu se pro mě stalo velkou zábavou a takřka vždy mi přináší potěšení.

Můj kurz je založen na skutečnosti, že počítače a výpočetní technologie jsou všude kolem nás. Některé počítačové technologie vidíme kolem sebe na první pohled: každý student má daleko výkonnější počítač, než byl sálový počítač IBM 7094, který stál několik milionů dolarů, zabíral celou jednu velikánskou klimatizovanou místnost a v roce 1964, kdy jsem na Princetonu zahájil doktorské studium, sloužil celému kampusu.[1] Každý student má také mobilní telefon, jehož výpočetní výkon je rovněž mnohem vyšší než výkon počítače z roku 1964. Každý ze studentů, stejně jako významný podíl světové populace, má i vysokorychlostní přístup k internetu. Každý z nich na internetu vyhledává informace, nakupuje a k udržování kontaktu s rodinou a přáteli používá elektronickou poštu, textové zprávy a sociální sítě.

To je však jen část počítačového ledovce, jehož většina se nalézá pod povrchem. Nevidíme a obvykle nemyslíme na počítače, které se ukrývají v různých spotřebičích, automobilech, letadlech a všudypřítomných elektronických přístrojích, které už bereme jako samozřejmost – fotoaparátech, hudebních přehrávačích, tabletech, navigacích GPS, herních konzolích. Ani se příliš nepozastavujeme nad tím, do jaké míry na výpočetních technologiích závisí naše infrastruktura: telefonní sítě, televizní vysílání, řízení letového provozu, energetické sítě, bankovnictví a finanční služby.

Většina lidí do tvorby těchto systémů přímo zapojena není, počítačové technologie ale mají velký vliv na každého z nás a někteří o nich musí činit významná rozhodnutí. Nebylo by lepší, kdybychom počítačům rozuměli lépe? Vzdělaný člověk by o nich měl znát alespoň základní věci: co počítače umí a jak to dělají; co dělat vůbec neumí a co je pro ně dnes nesmírně těžké; jak vzájemně komunikují a co se při tom děje; měl by také znát celou řadu způsobů, jimiž počítačové technologie a komunikace ovlivňují svět kolem nás.

Všudypřítomná povaha počítačových technologií nás zasahuje nečekanými způsoby. Čas od času se sice dovídáme o nárůstu sledování pomocí elektronických systémů, na vpády do našeho soukromí a nebezpečí krádeže identity, zřejmě si ale neuvědomujeme, do jaké míry šíření těchto praktik umožňují počítačové a komunikační technologie.

V červnu 2013 spolupracovník americké Národní bezpečnostní agentury (NSA) Edward Snowden vynesl a předal novinářům dokumenty, které odhalovaly, že NSA rutinně monitoruje a shromažďuje obrovské množství údajů o elektronické komunikaci – telefonických hovorech, elektronické poště, používání internetu – takřka každého na světě, zvláště však amerických občanů, včetně těch, kteří pro svou zemi žádnou hrozbu nepředstavují. Snowdenovy dokumenty rovněž ukázaly, že své občany špehují i ostatní země, v Británii například agentura zvaná Vládní komunikační ústředí (GCHQ), což je tamní obdoba NSA. Zpravodajské agentury spřátelených zemí si své informace sice obvykle vzájemně vyměňují, neplatí to ale o všech datech, takže německé zpravodajce tak trochu zaskočilo, když se dozvěděli, že NSA odposlouchávala mobilní telefon německé kancléřky Angely Merkelové.

Rovněž firmy pilně monitorují, co děláme na síti i ve skutečném světě, a každému z nás tím dál zužují možnost zůstat v anonymitě. Dostupnost ohromného množství dat umožnila rapidní pokrok v rozpoznávání řeči a jejím převádění na text, v rozpoznávání obrazu a překladech mezi jazyky, stálo nás to ale hodně z našeho soukromí.

Také zločinci se v útocích na data a databáze výrazně zlepšili. Rozmohla se vloupání do elektronických systémů firem a vlád a ve velkých množstvích se odcizují informace o zákaznících a zaměstnancích, které se pak často používají k podvodům a krádežím identity. Běžné jsou i útoky na jednotlivce. Byly doby, kdy stačilo ignorovat e-maily od údajných nigerijských princů či jejich příbuzných a mohli jsme zůstat na síti vcelku v bezpečí, nyní jsou ale cílené útoky mnohem rafinovanější a staly se jedním z nejobvyklejších způsobů napadání firemních počítačů.

Komplikované jsou i otázky jurisdikce čili soudní pravomoci a příslušnosti. Evropská unie rozhodla, že velké internetové vyhledávače musí zajistit „právo být zapomenut“, to znamená, že obyčejní lidé mohou po provozovatelích těchto vyhledávačů požadovat, aby byli vyloučeni z výsledků vyhledávání. EU to nařídila firmám, které ukládají data o jejích občanech na serverech v EU, nikoli však v USA. Tato pravidla samozřejmě platí jen v EU, v jiných částech světa je to jinak.

Další vrstvu složitosti přidává rychlé rozšíření modelu cloud computing, kdy si jednotliví uživatelé a firmy nechávají ukládat svá data na serverech vlastněných společnostmi Amazon, Google, Microsoft a řadou dalších a tyto servery jim také dodávají výpočetní operace, které potřebují. Data už nejsou přímo u svých majitelů, ale u některé z třetích stran, které mají jiné cíle, jinou odpovědnost a zranitelnost, a v různých jurisdikcích mohou čelit různým právním požadavkům.

Nastává také překotný růst „internetu věcí“, trendu připojovat k internetu všechny možné typy zařízení. Nejvýmluvnějším příkladem jsou samozřejmě mobilní telefony, k síti se ale připojují i automobily, bezpečnostní kamery, domácí

spotřebiče a různé ovladače, lékařské přístroje a velká část infrastruktury, jako je řízení letového provozu nebo energetické soustavy. Tendence připojovat k internetu všechno, co je kolem nás, bude díky neoddiskutovatelným výhodám této praxe pokračovat, je s ní však bohužel spojena i řada rizik, protože zabezpečení většiny těchto zařízení je mnohem slabší než bezpečnost vyspělých počítačových systémů.

Jedním z mála účinných nástrojů obrany proti tomu všemu je kryptografie, která nám umožňuje udržovat data a komunikace v bezpečí a soukromí. Silná kryptografie ale čelí ustavičným tlakům. Vládám se nelíbí, že by jednotlivci, firmy nebo teroristé mohli komunikovat zcela v soukromí, takže se často objevují návrhy na to, aby kryptografické mechanismy měly povinně otevřená „zadní vrátka", která by úřadům umožňovala prolamovat šifry, samozřejmě s „patřičnými zárukami" a jen „v zájmu národní bezpečnosti". I kdyby to bylo motivováno dobrými úmysly, je to velmi špatný nápad, protože slabá kryptografie pomáhá nejen našim přátelům, ale i našim protivníkům.

To všechno jsou některé z problémů a otázek kolem počítačových technologií, o něž by se měli zajímat všichni, včetně mých univerzitních posluchačů nebo příslovečných mužů a žen z ulice, bez ohledu na jejich zázemí či vzdělání.

Studenti v mém kurzu nestudují technické obory – nejsou to inženýři, fyzici ani matematici. Jsou to angličtináři, politologové, historici, klasičtí filologové, ekonomové, muzikologové i teoretici umění, takže jde o úžasný průřez humanitními obory. Na konci kurzu by měli být schopni přečíst a pochopit novinový článek o počítačové technologii, získat z něj více než dosud a možná i poznat, kde není příliš přesný. Obecně vzato bych chtěl, aby moji studenti a čtenáři přistupovali k technologiím s poučenou skepsí, aby věděli, že jsou často velmi užitečné, nejsou ale lékem na všechno; na druhé straně by měli vědět, že technologie mohou mít někdy neblahé následky, že ale žádným vysloveným zlem nejsou.

Pozoruhodná kniha Richarda Mullera *Physics for Future Presidents*[2] (Fyzika pro budoucí prezidenty) se pokouší vysvětlovat vědecké a technické pozadí významných problémů, s nimiž se musí potýkat političtí vůdci – jaderné hrozby, terorismu, energetiky, globálního oteplování a dalších podobných věcí. Něco o těchto tématech by měli vědět i dobře informovaní občané bez ambicí vstoupit do velké politiky. Mullerův přístup je dobrou metaforou toho, čeho bych zde chtěl dosáhnout i já: „Výpočetní technologie pro budoucí prezidenty."[3]

Co by měl budoucí prezident vědět o výpočetních technologiích? Co by měl o počítačích znát slušně informovaný člověk? Nějakou představu o tom má každý: zde je ta moje.

Výpočetní technologie sestávají ze tří základních technických oblastí – hardwaru, softwaru a komunikací. Na tomto rozdělení je vystavěna také struktura naší knihy.

Hardware je fyzická, hmatatelná část technologií; jsou to počítače, které vidíme a můžeme se jich dotýkat, máme je ve svých domovech a kancelářích a nosíme si je ve svých telefonech. Co je uvnitř počítače, jak to funguje, jak je to postaveno? Jak počítač ukládá a zpracovává informace? Co jsou to bity a bajty a jak je používáme, aby se z nich stala hudba, filmy a cokoli dalšího?

Software, což jsou instrukce, které počítačům říkají, co mají dělat, je naopak v podstatě nehmotný. Co můžeme vypočítat a jak rychle? Jak počítačům sdělíme, co mají dělat? Proč je tak těžké je přimět, aby fungovaly správně? Proč je často tak těžké je používat?

Komunikace spočívají v tom, že počítače, telefony a další zařízení spolu rozmlouvají, a někdy pak nechávají přes internet, web, e-mail a sociální sítě spolu mluvit i nás. Jak všechny tyto komunikační prostředky fungují? Jejich výhody jsou jasné, jaká jsou ale rizika, zvláště pro naše soukromí a bezpečnost, a jak můžeme tato rizika zmírnit?

K této trojici bychom měli připojit *data*, což jsou všechny informace, které jsou hardwarem a softwarem shromažďovány, ukládány a zpracovávány a jež jsou komunikačními systémy posílány kolem světa. Něco z nich jsou data, jimiž přispíváme do těchto systémů dobrovolně – ať už si rizika uvědomujeme, nebo ne – když na web posíláme texty, fotografie nebo videa. Zbytek jsou osobní informace o nás, a ty se obvykle shromažďují a sdílejí bez našeho vědomí, natož pak souhlasu.

Ať prezident či kdokoli jiný, o světě počítačových technologií by něco měl vědět každý, protože tyto technologie se dotýkají nás osobně. I kdybychom žili a pracovali jakkoli daleko od technických vymožeností, s technologiemi a lidmi, kteří s nimi umí pracovat, vždy nějak přijdeme do styku. Vědět něco o tom, jak tyto přístroje a systémy fungují, je velká výhoda, i kdyby měla spočívat jen v tom, že poznáme, kdy nám prodejce nebo servisní linka neříká celou pravdu. Nevědomost zde může dokonce přímo uškodit. Kdo neví, co jsou viry, phishing a podobné hrozby, podlehne jim snadněji. Pokud nevíte, jak ze sociálních sítí unikají, nebo se dokonce cíleně vysílají informace, o nichž jste si mysleli, že jsou soukromé, pravděpodobně budete o sobě na síti odhalovat mnohem více, než byste chtěli. Pokud nevíte nic o honbě komerčních subjektů za využitím všeho, co se dozvěděly o vašem životě, vzdáváte se svého soukromí v podstatě zadarmo. Pokud nevíte, proč je riskantní přistupovat ke svému osobnímu bankovnímu účtu v kavárně nebo na letišti, hrozí vám krádež peněz nebo totožnosti. A ignorovat narušování našeho osobního soukromí vládou přináší velká nebezpečí.

Kniha se obvykle čte od začátku do konce, možná ale raději zalistujete dopředu k tématům, která vás zajímají nejvíc, a zpět se vrátíte později. Můžete třeba začít pasážemi o sítích, mobilních telefonech, internetu, webu a otázkách soukromí, které začínají kapitolou 8; možná se budete muset podívat o něco

zpět, abyste plně porozuměli detailům, většina výkladu je ale srozumitelná i bez toho. Můžete přeskakovat cokoli, kde se vyskytuje příliš mnoho čísel, například pasáže o fungování binárních čísel v kapitole 2, nebo ignorovat detaily programovacích jazyků v několika dalších kapitolách. V poznámkách na konci uvádím svoji oblíbenou literaturu a jsou tam i odkazy na zdroje a užitečné dodatky. Na závěr přikládám slovníček, který podává stručné definice a vysvětlení důležitých technických termínů a zkratek.

Každá kniha o počítačích může rychle zastarat a tato není žádnou výjimkou. Její první vydání vyšlo dlouho předtím, než jsme se dozvěděli o rozsahu sledování NSA. Nejnovější vydání jsem aktualizoval zejména v částech týkajících se soukromí a bezpečnosti, jelikož tato témata prošla v posledních letech prudkým vývojem. Také jsem se snažil vyjasnit některé méně srozumitelné části a vypustil jsem či nahradil zastaralé pasáže. I přesto se může stát, že v době, kdy knihu budete číst, už některé věci platit nebudou. Stejně jako u prvního vydání jsem se i zde snažil jasně označit to, co má trvalejší hodnotu; zbytek si můžete ověřovat na webové stránce knihy kernighan.com, která nabízí aktualizace, opravy, dodatečný materiál a podobně.

Mým cílem je, aby čtenář této knihy plně ocenil úžasné možnosti výpočetních technologií a pochopil, jak fungují, odkud přicházejí a kam by mohly v budoucnu směřovat. Během čtení by si rovněž mohl osvojit užitečný způsob uvažování o světě. Pevně v to doufám.

PODĚKOVÁNÍ

Jsem hluboce zavázán všem svým přátelům a kolegům, kteří mi při psaní knihy poskytli velkorysou pomoc a rady. Jon Bentley stejně jako u prvního vydání přepečlivě pročetl několik pracovních verzí a každou stránku okomentoval; kniha je nyní díky jeho příspěvkům mnohem lepší. Cenné návrhy, kritické postřehy a upozornění na chyby v celém rukopisu mi poskytovali i Swati Bhattová, Giovanni De Ferrari, Peter Grabowski, Gerard Holzmann, Vickie Kearnová, Paul Kernighan, Eren Kursun, David Malan, David Mauskop, Deepa Muralidharová, Madeleine Planeix-Crockerová, Arnold Robbins, Howard Trickey, Janet Vertesiová a John Wait. Pomohly mi také rady, které mi dali David Dobkin, Alan Donovan, Andrew Judkis, Mark Kernighan, Elizabeth Linderová, Jacqueline Mislowová, Arvind Narayanan, Jonah Sinowitz, Peter Weinberger a Tony Wirth. Bylo mi potěšením spolupracovat s pracovní skupinou nakladatelství Princeton University Press – Markem Bellisem, Lorraine Donekerovou, Dimitrim Karetnikovem a Vickie Kearnovou. Všem jim za to děkuji.

Jsem vděčný rovněž princetonskému interdisciplinárnímu středisku Center for Information Technology Policy, kde jsem si mohl užívat dobrou společnost,

zajímavé debaty a každý týden obědy zdarma. A děkuji báječným studentům svého kurzu, jejichž talent a nadšení mě stále překvapují a inspirují.

PODĚKOVÁNÍ K PRVNÍMU VYDÁNÍ

Jsem hluboce zavázán všem svým přátelům a kolegům, kteří mi při psaní knihy poskytli velkorysou pomoc a rady. Zvláště jsem vděčen Jonu Bentleymu, který podrobně okomentoval takřka každou stránku několika mých pracovních verzí. Clay Bavor, Dan Bentley, Hildo Biersma, Stu Feldman, Gerard Holzmann, Joshua Katz, Mark Kernighan, Meg Kernighanová, Paul Kernighan, David Malan, Tali Moreshetová, Jon Riecke, Mike Shih, Bjarne Stroustrup, Howard Trickey a John Wait velmi pečlivě pročetli konečné pracovní verze, poskytli mi mnoho užitečnách návrhů a ušetřili mě některých velkých chyb. Za cenné komentáře děkuji také Jennifer Chenové, Dougu Clarkovi, Stevu Elgersmovi, Avi Flamholzovi, Henrymu Leitnerovi, Michaelu Liovi, Hughovi Lynchovi, Patricku McCormickovi, Jacqueline Mislowové, Jonathanu Rochellovi, Coreymu Thompsonovi a Chrisu Van Wykovi. Doufám, že poznají místa, kde jsem jejich rady poslechl, a nevšimnou si těch několika, kde jsem to neudělal.

David Brailsford mi díky svým těžce nabytým zkušenostem dodal mnoho prospěšných rad k formátování textu. Greg Doench a Greg Wilson mi velkoryse radili s publikováním. Za fotografie jsem zavázán Gerardu Holzmannovi a Johnu Waitovi.

V akademickém roce 2010–2011, kdy jsem psal první pracovní verze této knihy, byl mým hostitelem na Harvardu Harry Lewis. Jeho rady a zkušenosti s vedením obdobného kurzu byly pro mě neocenitelné, stejně jako jeho poznámky k řadě hrubých náčrtů. Škola inženýrských oborů a aplikovaných věd při Harvardově univerzitě a Berkmanovo centrum pro internet a společnost mi poskytly kanceláře a další zařízení, přívětivé a podnětné prostředí a také (ano, to existuje!) pravidelné obědy zdarma.

Zejména jsem vděčný stovkám studentů, kteří se přihlásili do kurzu „Počítače v našem světě“. Jejich zájem, nadšení a přátelství jsou pro mě stálým zdrojem inspirace. Doufám, že až budou za pár let řídit celý svět, bude se jim hodit něco z toho, čemu jsem je naučil.

ÚVOD

„Dostatečně pokročilou technologii nelze odlišit od magie."
Arthur C. Clarke: *Zpráva o třetí planetě*, 1972

V létě 2015 jsme si se ženou vzali dlouhou dovolenou a téměř tři měsíce jsme strávili cestováním po Anglii a Francii. Pronajali jsme si auto, koupili si jízdenky na vlak a zamluvili hotely ve velkých městech i chalupy na samotách, a to vše pouze prostřednictvím internetu. Před dokončením rezervací jsme si vždy prohlédli okolí a místní zajímavosti na on-line mapách a službě Google Street View. Na neznámých místech jsme se orientovali pomocí map a navigace v mobilních telefonech, kontakt s příbuznými a přáteli jsme udržovali přes e-mail a Skype, často jsme posílali fotografie a tu a tam i videa; pomocí mobilních telefonů jsem takřka denně několik hodin pracoval na jedné knize se svým spoluautorem v New Yorku. E-mail jsem si párkrát zkontroloval i v době, kdy jsme pluli lodí a nacházeli se uprostřed Atlantiku.

Na to si asi řeknete: „No a co? Nedělá to snad každý?" A až na neobvykle dlouhou dovolenou a plavbu lodí asi budete mít pravdu. V dnešním světě je to úplně běžné. Je téměř magické, jak snadné a pohodlné je zařizovat si své věci bez prostředníků a udržovat kontakt s blízkými i daleko od domova. Všechny tyto technologické systémy jsou už tak samozřejmé, že na ně často ani nemyslíme, přestože se naše životy díky nim výrazně a velmi rychle změnily.

Na naší dovolené jsme k pronájmům ubytování nepoužívali webovou službu Airbnb, i když bychom mohli. Airbnb byla založena v roce 2008, nyní působí ve 190 zemích a uživatelé přes ni inzerují kolem jednoho a půl milionů nabídek. Airbnb měla velký dopad na hotelové podnikání v řadě měst – ceny jsou na ní často nižší a její technologie obchází zavedený regulační rámec, který se něčemu takovému ještě nestihl přizpůsobit.

Nepoužívali jsme ani přepravní službu Uber, protože jet taxíkem jsme potřebovali jen párkrát, ale využívat jsme ji také mohli (a náš londýnský taxikář si přivydělával jako řidič Uberu). Uber vznikl v roce 2009 a své služby nyní provozuje ve více než 60 zemích. Podnikání Uberu má významný dopad na odvětví taxislužby v mnoha velkých městech – stejně jako Airbnb má často nižší ceny než běžné taxislužby a jeho technologie rovněž obchází stávající regulaci, která se tomu přizpůsobuje jen velmi pomalu.

K udržování kontaktu s blízkými jsme nepoužívali ani aplikaci WhatsApp, i když i tu jsme využívat mohli, ale Skype, který byl pro nás lepší. WhatsApp byla

rovněž založena v roce 2009 a o pět let později ji koupil Facebook za 19 miliard dolarů. Má více než 900 milionů uživatelů a je to největší mobilní aplikace pro zasílání zpráv a multimediálních souborů. Ke konci roku 2015 a v roce 2016 jí brazilský soud několikrát nařídil pozastavit, protože odmítala vyhovět soudním nařízením na předání dat, která byla součástí trestního vyšetřování. Odvolací soud toto nařízení pokaždé zvrátil, a 100 milionů brazilských uživatelů tak může znovu používat WhatsApp místo služeb zavedených mobilních operátorů.

To všechno nám připomíná, jak rozsáhlý záběr počítačové technologie mají, jak rychle se mění, jak rozkladně mohou působit na stávající struktury, jak hluboko mohou pronikat do našich životů a kolika způsoby je mohou měnit k lepšímu.

Všechny tyto novinky mají ale i svou temnější stránku, zdaleka ne tak radostnou a optimistickou. Každou z uvedených interakcí tiše sleduje a ukládá nespočet počítačových systémů – sledují, s kým vy a já vstupujeme do transakcí, kolik jsme zaplatili a kde jsme v té době byli. Velká část těchto dat se shromažďuje pro komerční účely, jelikož čím více o nás firmy vědí, tím přesněji na nás mohou zacílit své reklamy. Většina čtenářů o shromažďování takových dat ví, myslím ale, že mnohé by překvapilo, o jak velký rozsah jde a do jakých podrobností tato data zacházejí.

A jak jsme se nepříliš dávno dozvěděli, nesledují nás jen firmy.

E-maily, interní zprávy a powerpointové prezentace NSA, které vynesl Edward Snowden, odhalily o špionáži v digitální éře opravdu hodně, především to, že NSA sleduje velkoplošně v podstatě všechny. Snowden se v obavách o svou bezpečnost podělil o ukradené materiály s malým počtem novinářů v Hongkongu a pak před trestním stíháním v USA utekl do Moskvy, kde ho chrání vláda Vladimira Putina. O muži, jehož jedni označují za zrádce a jiní ho velebí jako hrdinu, se bude mluvit zřejmě ještě dlouho. Jeho příběh vypráví kniha Glenna Greenwalda *No Place to Hide* (Není se kam ukrýt) z roku 2014 a film Laury Poitrasové *Citizenfour: Občan Snowden*, který v roce 2015 získal Oscara za nejlepší dokument.

Snowdenova odhalení ohromila svět. Všeobecně se sice tušilo, že NSA sleduje více lidí, než sama přiznávala, rozsah sledování byl ale větší, než si kdokoli byl schopen představit. NSA rutinně shromažďovala metadata o všech telefonických hovorech na americkém území – tedy záznamy o tom, kdo, kdy, s kým a jak dlouho mluvil – a zřejmě nahrávala i obsahy hovorů.[1] Zaznamenala tedy i moje hovory přes Skype, moje e-mailové kontakty a možná i obsahy mých e-mailů. (A samozřejmě i vašich.) Odposlouchávala mobilní telefony předních světových politiků. Zachycovala rozsáhlé objemy internetového provozu pomocí nahrávacích zařízení na různých místech. Přesvědčila nebo donutila velké telekomunikační a internetové společnosti, aby shromažďovaly a předávaly jí informace o uživatelích. Ukládala si nadlouho velká množství dat a některá z nich sdílela se zpravodajskými agenturami jiných zemí.

Když se vrátíme do firemní sféry, sotva mine den, v němž bychom se nedozvěděli o dalším prolomení počítačových systémů některé firmy nebo instituce, které neznámí hackeři ukradli data ve formě jmen, adres a čísel kreditních karet milionů lidí. Obvykle jde o aktivity zločinců, někdy ale i tajných služeb jiných zemí. Občas se otevře přístup k soukromým datům kvůli hlouposti jejich správce. Ať tak či onak, data, která se o nás shromažďují, až příliš často unikají ven nebo jsou odcizena a mohou být použita proti nám.

Není tedy všechno tak báječné a kouzelné, jak by se mohlo zdát.

Tato kniha by chtěla všem čtenářům srozumitelně vysvětlit základy počítačových a komunikačních technologií, které za tím vším stojí. Jak je možné, že se dají ve zlomku sekundy poslat kolem světa fotografie, hudba, filmy a intimní podrobnosti našeho osobního života? Jak funguje e-mail a posílání textových zpráv a do jaké míry jsou tyto služby soukromé? Proč se dají tak snadno rozesílat spamy a proč je tak těžké se jich zbavit? Opravdu mobilní telefony neustále hlásí, kde jsme? Jak se liší iPhony od telefonů na platformě Android a proč jsou oba systémy v principu zcela stejné? Kdo nás sleduje na síti a na našem telefonu a proč na tom záleží? Mohou hackeři přebrat řízení našeho vozu? Jak je to se samořízenými automobily? Můžeme vůbec ochránit naše soukromí a bezpečnost? Na konci knihy by čtenáři měli mít solidní povědomí o fungování počítačových a komunikačních systémů, o tom, jak nás ovlivňují a jak najít rovnováhu mezi používáním užitečných služeb a ochranou svého soukromí.

Proto probereme do podrobností několik málo základních principů.[2]

Prvním z nich je *univerzální digitální reprezentace informací*. Komplikované a důmyslné mechanické systémy uchovávání dokumentů, fotografií, hudby a filmů, které jsme používali po většinu 20. století, nahradil jediný a jednotný mechanismus. Bylo to možné proto, že informace je možné reprezentovat i digitálně, nejen na barevných políčkách plastových filmů nebo magnetických strukturách vinylového pásku. Papírová pošta přenechala místo své digitální verzi. Papírové dokumenty jsou nahrazovány databázemi na síti. Různé analogové reprezentace informací nahrazuje jediná digitální reprezentace.

Druhou takovou myšlenkou je *digitální procesor* jako *univerzální* nástroj na zpracování informací. Všechny informace je možné zpracovávat jediným víceúčelovým zařízením, digitálním počítačem. Digitální počítače, které pracují s jednotnou digitální reprezentací informací, nahradily řadu složitých mechanických přístrojů, jež se zabývaly reprezentací analogovou. Jak uvidíme později, počítače jsou co do výpočetní činnosti všechny stejně způsobilé a liší se jen rychlostí a množstvím dat, která mohou uložit. Chytrý telefon je už značně pokročilý počítač a má podobný výpočetní výkon, jaký má několik let starý notebook. To, co dříve mohly zpracovávat jen stolní počítače a notebooky, se tak stále více přemisťuje na telefony a tento proces konvergence se zrychluje.

Třetím principem je *univerzální digitální síť*. Internet propojuje digitální počítače, které zpracovávají digitální reprezentace; napojuje počítače a telefony na elektronickou poštu, vyhledávače, sociální sítě, weby pro nakupování, bankovnictví, zpravodajství, zábavu a cokoli dalšího. Můžeme si vyměňovat e-maily s kýmkoli, bez ohledu na to, kde je nebo jak se ke své poště dostává. Můžeme vyhledávat, srovnávat ceny a nakupovat přes telefon, laptop nebo tablet. Sociální sítě nás udržují v kontaktu s přáteli a příbuznými a k dispozici je máme opět přes telefon nebo počítač. Všechny tyto služby fungují díky rozsáhlé infrastruktuře.

Neustále se také sbírá a analyzuje ohromné množství *digitálních dat*. Díky tomu máme volně dostupné mapy, letecké záběry a pohledy do ulic ve většině světa. Webové vyhledávače neúnavně prohledávají internet, aby co nejlépe zodpověděly kladené dotazy. Máme k dispozici miliony knih v digitální podobě. Sociální a výměnné sítě udržují rozsáhlé objemy dat pro nás a o nás. On-line prodejny a služby si při poskytování přístupu ke svým produktům nenápadně nahrávají všechno, co děláme, když je navštívíme; v tom jim dopomáhají a k tomu je navádějí provozovatelé vyhledávačů a sociálních sítí. Poskytovatelé internetového připojení zaznamenávají při každé naší interakci na síti všechna uskutečněná připojení – a možná i něco více. Vlády nás celou dobu sledují v míře, jaká by byla před desetiletím či dvěma zcela nemyslitelná.[3]

To všechno se překotně rozvíjí – systémy digitálních technologií se exponenciálním tempem zmenšují, zrychlují a zlevňují: každý rok až dva se jejich výkon za stejnou cenu zdvojnásobí. Na trh nepřetržitě přicházejí nové mobilní telefony se stále atraktivnějšími prvky, lepšími displeji a zajímavějšími aplikacemi. Neustále se objevují digitální novinky a funkce těch nejužitečnějších se často obratem stanou součástí telefonů. Je to přirozený vedlejší produkt digitálních technologií, kdy každá prospěšná novinka vede ke zlepšení v celém spektru digitálních zařízení: pokud určitá změna umožní nakládat s daty levněji, rychleji nebo ve větším množství, mají z toho prospěch všechna zařízení. V důsledku toho digitální systémy pronikají všude a stávají se integrální součástí našeho života, nejen viditelně, ale i za scénou.

Tento pokrok jistě působí na pohled báječně a ve většině ohledů takový i je. Má to ale i své stinné stránky. Jednou z nejzjevnějších a nejznepokojivějších je dopad technologií na naše osobní soukromí. Když používáme telefon, abychom vyhledali určité zboží a navštívili web jeho prodejců, uchovávají všechny zúčastněné strany záznamy o tom, co jsme navštívili a na co jsme klikli. Vědí, kdo jsme, protože nás identifikuje náš telefon. Vědí, kde jsme, protože telefony hlásí *celou dobu* naši polohu. Pomocí GPS, globálního polohovacího systému, nás mohou telefonní operátoři zaměřit s přesností na pět až deset metrů, a i bez GPS znají naši polohu na zhruba stovky metrů. A všechny tyto informace pak mohou prodávat. Stále více nás sledují i kamenné prodejny. Technologie rozpoznávání

tváří nás může identifikovat na ulici nebo v obchodě. Dopravní kamery snímají poznávací značky našich vozů, a vědí tak, kudy jezdíme. Sledování z románu *1984* od George Orwella vypadá vedle toho, co dnes bez většího přemýšlení dovolujeme, jako náhodné a ledabylé.

Záznamy o tom, co kde děláme, mohou klidně vydržet navěky. Digitální archivování je tak levné a data tak cenná, že se informace odstraňují jen zřídkakdy. Jakmile na internet umístíme něco trapného nebo pošleme e-mailem něco, čeho vzápětí litujeme, je už pozdě. Informace o nás z více zdrojů se mohou spojit a vytvořit podrobný obraz našeho života, který mohou bez našeho vědomí a svolení získat komerční subjekty, vládní úřady i zločinci. Tyto informace pravděpodobně zůstanou dostupné neomezeně dlouho a v budoucnu se mohou kdykoli vynořit, aby nám zkomplikovaly život.

Univerzální síť a univerzální digitální informace nás vystavily rizikům od cizích lidí v míře, jaká byla před jedním či dvěma desetiletími nepředstavitelná. Expert na počítačovou bezpečnost Bruce Schneier ve své knize *Data and Goliath* (Data a Goliáš) z roku 2015 napsal: „Naše soukromí je pod náporem neustálého sledování. Máme-li pochopit, co je v sázce, musíme vědět, jak se to děje."

Společenské mechanismy, které chrání naše soukromí a majetky, nedokážou s tak rychlým technologickým pokrokem držet krok. Před 30 lety jsem se se svou bankou a dalšími finančními institucemi stýkal prostřednictvím klasické pošty a občasných osobních návštěv. Dostat se ke svým penězům nějakou dobu trvalo a zůstávala za tím značná papírová stopa; ukrást peníze z mých účtů bylo hodně obtížné. Dnes se s finančními institucemi stýkám převážně přes internet. Ke svým účtům mám sice snadný přístup, bohužel je ale docela dobře možné, že kvůli nějaké chybě na straně mé nebo těchto institucí mi může někdo na druhém konci světa vybrat účet, ukrást identitu, zničit můj úvěrový rating a kdoví co ještě – stane se to během chvilky a já mám jen malou šancí tomu předejít.

Naše kniha se zabývá tím, jak tyto systémy fungují a jak mění naše životy. Je to ale nevyhnutelně jen momentka – je jisté, že za deset let se budou dnešní systémy zdát obstarožní a nemotorně velké. Technologická změna není izolovaná událost, ale trvalý proces – překotný, nepřetržitý a stále rychlejší. Základní principy digitálních systémů však naštěstí zůstávají stále stejné, a jestliže jim porozumíme, pak snáze pochopíme i technologie zítřka a lépe zvládneme problémy a příležitosti, které přinesou.