EUROPEAN DATA PROTECTION SUPERVISOR

Stanovisko 4/2015

Směrem k nové digitální etice

Data, důstojnost a technologie“

11. září 2015

Evropský inspektor ochrany údajů (EIOÚ) je nezávislou institucí EU a je zodpovědný podle čl. 41 odst. 2 nařízení 45/2001 „[v] oblasti zpracování osobních údajů... zajistit, aby orgány a instituce Společenství dodržovaly základní práva a svobody fyzických osob, zejména jejich právo na soukromí", a „... je pověřen poradenstvím pro orgány a instituce Společenství a subjekty údajů pro všechny otázky, které se týkají zpracování osobních údajů". Byl jmenován v prosinci 2014 společně se zástupcem inspektora s konkrétním posláním, aby byl více konstruktivní a proaktivní. EIOÚ zveřejnil v březnu 2015 pětiletou strategii, v níž uvádí, jak hodlá naplnit toto poslání a jak bude zodpovědný za její plnění.

Toto stanovisko navazuje na předchozí stanovisko EIOÚ k obecnému nařízení o ochraně osobních údajů, jehož cílem bylo pomoci hlavním institucím EU při dosažení správné shody o funkčním, na budoucnost orientovaném souboru pravidel, který posílí práva a svobody jednotlivce. Podobně jako stanovisko k mobilnímu zdraví z počátku roku 2015 se zabývá výzvou pro ochranu dat v rámci „go digital (digitalizace)", což je třetí cíl strategie EIOÚ, „přizpůsobení stávajících zásad ochrany údajů tak, aby vyhovovaly globální digitální aréně", a to i ve světle plánů EU na digitální jednotný trh. Je v souladu se stanoviskem článku 29 pracovní skupiny k aspektům ochrany údajů při využívání nových technologií, jako je například „internet věcí", ke kterému EIOÚ přispěl jako plnoprávný člen skupiny.

Dignity	Důstojnost
Future-oriented rules and enforcement	Pravidla a jejich prosazování se zaměřením na budoucnost
Accountable controllers	Zodpovědní správci
Empowered individuals	Silnější jednotlivci
Innovative privacy engineering	Novátorské inženýrství soukromí
Ethics	Etika

„Lidská důstojnost je nedotknutelná. Musí být respektována a chráněna.“

Článek 1, Listina základních práv Evropské Unie

Základní práva na soukromí a na ochranu osobních údajů jsou důležitější pro ochranu lidské důstojnosti než kdykoliv předtím. Jsou zakotvena ve smlouvách EU i v Listině základních práv Evropské unie. Umožňují jednotlivcům rozvíjet svoji vlastní osobnost, vést samostatný život, inovovat a uplatňovat další práva a svobody. Zásady ochrany údajů stanovené v Listině základních práv EU - nezbytnost, přiměřenost, spravedlnost, minimalizace údajů, omezení účelu, souhlas a transparentnost - platí pro zpracování údajů v celém jeho rozsahu, pro shromažďování stejně tak jako pro používání.

Technologie by neměla diktovat hodnoty a práva, ale ani by se tento vztah neměl omezovat na falešnou dichotomii. Digitální revoluce slibuje přínos pro zdraví, životní prostředí, mezinárodní rozvoj i ekonomickou efektivitu. Podle plánů EU na digitální jednotný trh jsou cloud computing, „internet věcí“, data velkého objemu i další technologie považovány za klíčové pro konkurenceschopnost a růst. Obchodní modely využívají nové možnosti pro masivní sběr, okamžitý přenos, kombinaci a opětovné používání osobních informací pro nepředvídané účely na základě neproniknutelných zásad pro ochranu soukromí. Tím vzniká nový tlak na zásady ochrany údajů, což vyžaduje inovativní přístup k tomu, jak jsou uplatňovány.

V dnešním digitálním prostředí dodržování právních předpisů nestačí; musíme brát do úvahy i etický rozměr zpracování dat. Předpisový rámec EU již poskytuje prostor pro pružné rozhodování a záruky, případ od případu, pro zacházení s osobními informacemi. Reforma předpisového rámce bude dobrým krokem vpřed. Ale existují hlubší otázky, pokud jde o dopad trendů ve společnosti řízené daty na důstojnost, svobodu jednotlivce a fungování demokracie.

Tyto problémy mají technické, filozofické, právní a morální důsledky. Toto stanovisko poukazuje na některé hlavní technologické trendy, které mohou zahrnovat nepřijatelné zpracování osobních údajů nebo mohou zasahovat do práva na soukromí. Nastiňuje čtyřstupňový „ekosystém ochrany velkých údajů“ reagující na digitální výzvu: kolektivní úsilí, podpořené etickými úvahami.

(1) Na budoucnost zaměřená regulace zpracování údajů a respektování práv na soukromí a ochranu údajů.

(2) Zodpovědní správci, kteří určují zpracování osobních informací.

(3) Ohled na ochranu soukromí již při navrhování a vývoji produktů a služeb souvisejících se zpracováním údajů.

(4) Silnější jednotlivci.

Evropský inspektor ochrany údajů chce podpořit otevřenou a informovanou diskusi v EU i mimo ni, do které se zapojí občanská společnost, vývojáři, firmy, veřejné orgány i regulační orgány. Nový etický výbor pro ochranu údajů v EU, který založíme v rámci úřadu EIOÚ, pomůže definovat novou digitální etiku, jež umožní lépe realizovat přínosy technologií pro společnost a hospodářství, a to způsoby, které posílí práva a svobody jednotlivců.

OBSAH

1. Data všude kolem nás: Trendy, příležitosti a výzvy

Stále se zvyšující množství osobních informací je shromažďováno a zpracováváno stále neprůhlednějšími a složitějšími způsoby. S pokračujícím zaváděním počítačů do podniků i veřejné správy v 80. letech 20. století vznikl široce rozšířený dojem, že postupy mocných vlád a korporací při zpracování osobních údajů redukují jednotlivce na pouhé subjekty údajů a ohrožují základní práva a svobody. To, čím se odlišuje současná vlna integrovaných informačních a komunikačních technologií, je její všudypřítomnost a síla.

V loňském roce se objevila zpráva, že na planetě je více připojených zařízení než lidí[1]. Nárůst výkonu procesorů[2], kapacity pamětí i šířky přenosového pásma znamená, že postupně existuje stále méně technických omezení pro zpracování osobních údajů. Analýza „internetu věcí" a dat velkých objemů očekává, že se budou sbližovat s umělou inteligencí, zpracováním přirozeného jazyka a biometrickými systémy, aby společně poskytly aplikacím schopnost učit se a dosáhnout tak pokročilé inteligence. Vlády i firmy mohou přejít od „vytěžování údajů" k „vytěžování reality", které pronikne do každodenní zkušenosti, komunikace a dokonce i myšlení[3]. Jak se společnost přizpůsobuje požadavkům digitálního trhu, opět se objevují obnovené snahy učit programování malé děti[4]. Využití těchto trendů v odvětví, ve kterém je EU předním spotřebitelem, ale opozdilcem při poskytování služeb, je vracejícím se tématem pro strategii jednotného digitálního trhu Komise[5].

Tyto trendy a mnohé z dnes používaných pojmů jsou i přes všeobecné rozšíření vágní a překrývají se. Abychom přispěli k podnícení debaty, chtěli bychom upozornit na určité trendy, které - samozřejmě mimo jiné - podle našeho názoru přinášejí nejdůležitější etické a praktické otázky pro uplatňování zásad ochrany údajů.

1.1 Data velkého objemu

Pojem „Big Data - data velkého objemu"[6] označuje postupy při kombinování obrovských objemů informací z různých zdrojů a při jejich analýze, kdy se často používají učící se algoritmy pro kvalifikovaná rozhodnutí. Tyto informace nejsou vždy osobní údaje: mohou to být data získaná ze snímačů pro sledování přírodních nebo atmosférických jevů, jako je počasí nebo znečištění, nebo pro monitorování technických aspektů výrobních procesů, která se nevztahují k „identifikované nebo identifikovatelné osobě"[7]. Ale jedna z největších hodnot dat velkého objemu pro podniky i vlády je odvozena ze sledování *lidského* chování, a to kolektivně i jednotlivě, a spočívá v jejich prediktivním potenciálu[8].

Jedním z výsledků je vznik příjmového modelu pro internetové firmy, které spoléhají na sledování on-line aktivit při optimalizaci ekonomické hodnoty transakcí vůči poskytovatelům služeb, a to nejen v oblasti cílené reklamy, ale také podmínek a sazeb pojištění, úvěrů a dalších smluvních vztahů. Na konkurenčním trhu s pozorností uživatelů si většina lidí neuvědomuje široký rozsah tohoto sledování[9]. Taková „data velkého objemu" by měla být považována za osobní údaje i tam, kde byly použity anonymizační techniky: je stále snazší odvodit totožnost osoby kombinací údajně „anonymních" dat s jinými soubory dat, včetně veřejně dostupných informací, například v rámci sociálních médií[10]. Tam, kde se s údaji obchoduje zejména mezi státy a jurisdikcemi, se odpovědnost za zpracování informací stává mlhavou a obtížné zjistitelnou nebo prosaditelnou v rámci práva na ochranu údajů, a to zejména při absenci mezinárodních norem.

1.2 „Internet věcí“

Mnohá zařízení připojená k internetu jsou dnes již samozřejmostí, jako například chytré telefony, tablety, bankomaty a odbavovací automaty na letišti. Předpokládá se, že do roku 2020 se konektivita stane standardem a připojeno bude 25 miliard zařízení (ve srovnání s 4,8 miliard v roce 2015) - od telemedicíny po auta, od inteligentních měřičů po celou řadu nových stacionárních i mobilních zařízení potřebných pro chytrá města [11].

Tyto snímače budou poskytovat okamžité a podrobné informace, které statistické úřady a průzkumy nemohou dnes získat, ale které nemusí nutně být přesnější a mohou být dokonce potenciálně zavádějící[12]. Odhadovaných 1,8 miliard spojení uskutečněných mezi automobily do roku 2022 by mohlo snížit počet nehod i znečištění životního prostředí, zvýšit produktivitu a samostatnost seniorů i osob se zdravotním postižením[13]. „Nositelná elektronika“ jako oblečení a hodinky bude zpracovávat osobní údaje jako jiná připojená zařízení. Bude schopna detekovat krevní sraženiny a monitorovat kondici či hojení ran; připojené textilie by mohly chránit v extrémním prostředí, například při hašení požárů. Tato zařízení budou nahrávat osobní údaje přímo do cloudového úložiště spojeného se sociálními sítěmi a popřípadě je vysílat veřejně, což bude umožňovat identifikaci uživatelů i sledování chování a pohybů jednotlivců i davů[14].

To, jak bude s těmito informacemi nakládáno, může mít vliv na soukromí nejen uživatelů těchto zařízení, včetně těch, která se používají na pracovišti, ale i na práva ostatních lidí, jež jsou tímto zařízení pozorováni a zaznamenáni. Ačkoliv existuje málo důkazů o skutečné diskriminaci, je jasné, že obrovské množství osobních informací shromážděných „internetem věcí“ je velmi zajímavé jako prostředek k maximalizaci výnosů prostřednictvím cen více personalizovaných na základě sledovaného chování, a to zejména v oblasti zdravotního pojištění[15]. Další pravidla tohoto odvětví budou také ohrožena, například tam, kde zařízení zahrnující zpracování údajů o zdravotním stavu nejsou technicky kategorizována jako zdravotnické prostředky a tudíž nespadají do oblasti působnosti nařízení[16].

1.3 Ambient computing

Ambient neboli neviditelný computing je označení pro klíčovou technologii umožňující „internet věcí“. Jednou z jejích nejvýraznějších aplikací jsou „chytré domácnosti“ a „chytré kanceláře“ zahrnující zařízení s vestavěnými možnostmi propracovaného zpracování informací, které slibují vyšší energetickou účinnost a informovanější jednotlivce, jež jsou schopni ovlivnit svoji spotřebu na dálku (i když to bude záviset na nezávislosti rezidenta na pronajímateli nebo správci budovy). Bude muset být jasné, kdo je odpovědný za účel a prostředky zpracování osobních údajů použitých v rámci aplikací ambient computingu, a to nejen pro ochranu základních práv jednotlivců, ale také pro odpovídající určení odpovědnosti za zajištění dodržování požadavků zabezpečovacích systémů.

1.4 Cloud computing

Cloud computing je známý jako centrální technologie umožňující jak pokročilou analytiku, tak těžení, sběr a analýzu velkých objemů dat i záplavy dat z „internetu věcí“, kterou v současné době používá zhruba pětina občanů a firem v EU[17]. Umožňuje koncentraci dat z nesčetných zařízení v rámci „internetu věcí“ a je s ní spojena dostupnost a konektivita obrovských objemů dat ve velkoobjemových skladovacích a zpracovatelských zařízeních po celém světě[18]. Odhaduje se, že širší použití cloud computingu[19] v soukromém i veřejném sektoru přispěje celkově 449 miliardami EUR k HDP EU28 (0,71% celkového HDP EU).

Kontrolu nad osobními údaji spolu často sdílejí zákazník a poskytovatel cloudových služeb a odpovědnost za povinnosti v oblasti ochrany osobních údajů není vždy jasná. To by mohlo znamenat, že v praxi je poskytována nedostatečná ochrana. Tyto povinnosti platí bez ohledu na **fyzické umístění datového úložiště. Navíc,** i když se jedná jen o technologické zázemí podporující podnikové aplikace, může se infrastruktura pro cloud computing sama o sobě stát kritickou infrastrukturou a zvýšit nerovnováhu v tržní síle. 30 % podniků se v poslední době vyjádřilo, že mají potíže se zrušením služby nebo se změnou poskytovatele[20].

1.5 Obchodní modely závislé na osobních údajích

Tyto technologie umožnily nové obchodní modely, které spoléhají na informace zjištěné nejen při poskytování služeb, ale také z jiných zdrojů, jako je přítomnost na sociálních médiích, při posuzování rizik a bonity i pro maximalizaci příjmů. Prominentní obchodní model dneška je reprezentován platformami, které spojují prodávající a kupující a umožňují sdílení a přerozdělování výrobků, služeb, dovedností a aktiv. Tyto platformy se často nazývají „ekonomikou sdílení“, „kolaborativní spotřebou“ nebo on-line a mobilními platformami peer-to-peer[21] a mohou nabídnout klasickou hospodářskou efektivitu, povzbudit konkurenceschopnost trhů a snížit množství odpadu. Odhaduje se, že jejich celosvětová hodnota se v následujících letech zečtyřnásobí z 26 na 110 bilionů USD[22]. Takové obchodní modely řízené daty již přinášejí obrovské výnosy při sdílení automobilů a pronájmu domů i ve finančních technologiích a sociálních půjčkách. Průzkumy ukazují, že spotřebitelé oceňují jejich očividnou větší dostupnost a pohodlí[23].

„Měnou“ na těchto platformách je obvykle pověst uživatele, vzájemná hodnocení a ověření identity. To by mohlo potenciálně znamenat zvýšení průhlednosti a odpovědnosti, ovšem ne nutně ve vztahu k poskytovateli platformy samotnému. Velcí hráči na těchto trzích byli kritizováni, že údajně odepírají poskytnutí údajů o pověsti uživatelům, na které se informace vztahují. Existuje obrovské riziko, že by jednotlivci mohli být vyloučeni ze služeb poskytovaných na základě reputace kvůli nesprávným údajům, které nemohou zpochybnit ani nemohou požadovat jejich odstranění. Spoléhání na údaje z různých zdrojů rovněž zpochybňuje zásadu minimalizace údajů zakotvenou v právních předpisech EU. Rozsah budoucího dopadu těchto a budoucích obchodních modelů umožněných novými technologiemi na jednotlivce a společnosti si zaslouží pečlivé zvážení[24].

1.6 Drony a autonomní vozidla

Drony nebo částečně autonomní letouny v současné době slouží především vojenským účelům, ale stále více se využívají i pro účely sledování, mapování, dopravy, logistiky a veřejné bezpečnosti, jako například při potlačování požárů[25]. Fotografie, videa a další osobní údaje shromážděné drony mohou být přenášeny přes telekomunikační sítě. Jejich použití přináší riziko závažného zásahu do soukromí a neblahý dopad na svobodu projevu. Naskýtá se otázka, jak by jejich návrh a použití mohly být účinně regulovány tak, aby subjekty údajů mohly uplatňovat své právo přístupu k datům pořízeným těmito stroji.

A na zemi autonomní vozidla nebo vozidla bez řidiče změní způsob, jakým bude cestování lidí používáno a organizováno, a také mohou rozostřit rozdíl mezi soukromou a veřejnou dopravou. Odhaduje se, že do roku 2035 bude existovat 12 milionů plně autonomních a 18 milionů částečně autonomních vozidel, přičemž Evropa bude patřit mezi první uživatele[26]. Algoritmy řídicí taková auta budou přijímat rozhodnutí, která se přímo týkají tělesné integrity a dokonce i života nebo smrti jednotlivců, například při volbě činnosti naprogramované pro případ nevyhnutelného nárazu. Vedle zjevné potřeby vyjasnit, kdo je

odpovědný a kdo ručí za kontrolu a bezpečnost údajů, tyto aplikace také vyvolávají řadu etických otázek.

1.7 Trendy s potenciálně větším a dlouhodobějším dopadem

3D bioprinting organických položek, který využívá kopie buněk pacienta a kolagenových „bio obvazů“ (tedy citlivých údajů podle právních předpisů EU) k pokládání postupných řad živých buněk, bude pravděpodobně brzy k dispozici[27]. Usnadnil by získávání konkrétních anatomických částí těl a byl by obzvláště cenný v chudších a post-konfliktních oblastech světa. Bioprinting vyvolává zjevné otázky v oblasti lékařské etiky, ochrany duševního vlastnictví a ochrany spotřebitele, ale vzhledem k tomu, že počítá se zpracováním intimních a citlivých údajů týkajících se zdraví jedinců, také v oblasti uplatňování pravidel ochrany údajů.

Umělá inteligence, jako robotika, označuje technologický požadavek pro autonomní stroje, stacionární i mobilní. Jejich vývoj nabídne obrovský potenciál daleko nad rámec jejich současného využití. Počítače, ve kterých probíhá „hluboké učení (deep learning)“ se učí tak, že zpracovávají velké datové soubory pomocí (mimo jiné) neuronových sítí, které by měly napodobovat mozek. Výzkumní pracovníci a firmy usilují o zlepšení učení bez učitele. Algoritmy již dokáží porozumět jazykům a překládat je, také rozeznávat obrázky, psát novinové články a analyzovat lékařská data[28]. Sociální média dodávají obrovské množství osobních informací, které účinně předem označí samotní jednotlivci. Ty mohou být poslední v řadě kognitivních vylepšení rozšiřujících schopnosti lidského mozku, stejně jako papír nebo počítadlo, nebo integrovaných do autonomních strojů, robotů. Teď je však načase zvážit širší důsledky pro jednotlivce i společnost[29].

2. Ekosystém ochrany údajů velkého objemu

EU má nyní příležitost udávat směr a ukázat, jak vlády, regulační orgány, správci údajů, návrháři, vývojáři a jednotlivci mohou lépe jednat společně, aby posílili práva a řídili, ne blokovali, technologické inovace. Trendy zmíněné v sekci dvě podle jednoho komentátora, „rozšířily propast mezi tím, co je možné, a tím, co je zákonem povoleno“[30]. Oproti některým tvrzením, soukromí a ochrana údajů jsou platformou pro udržitelné a dynamické digitální prostředí, ne jeho překážkou. Nezávislé orgány pro ochranu údajů, jako je EIOÚ, hrají klíčovou roli v rozptýlení takových mýtů a reagování na skutečné obavy jednotlivců ze ztráty kontroly nad svými osobními informacemi[31].

Příští generace osobních údajů bude pravděpodobně ještě méně přístupná jednotlivcům, kterých se týká. Odpovědnost za formování udržitelného jednotného digitálního trhu je nezbytně rozptýlená, ale je také vzájemně závislá, jako ekosystém, což vyžaduje účinnou interakci mezi vývojáři, podniky a regulačními orgány v zájmu jednotlivce. V této části nastíníme přínos, který tito čtyři základní hráči mohou přinést.

2.1 Regulace orientovaná na budoucnost

Nedávno jsme vyzvali EU, aby se chopila své historické příležitosti a zavedla taková jednodušší pravidla pro zpracování osobních údajů, která zůstanou aktuální pro celou generaci[32]. Jednání k obecnému nařízení o ochraně osobních údajů a ke směrnici o ochraně údajů v oblasti policie a spravedlnosti jsou v závěrečné fázi a brzy se pozornost obrátí na budoucnost směrnice o soukromí a elektronických komunikacích (směrnice o e-soukromí) a na nové nařízení upravující to, jak samotné instituce a orgány EU zpracovávají osobní údaje. S tím, jak jsou ekonomické náklady na sběr a uložení dat téměř zanedbatelné, bude záležet na

orgánech pro ochranu údajů, aby důsledně prosadily tato pravidla a předešly tak „morálním nebezpečím“ spojeným s nadměrným zpracováním dat[33].

Strategie jednotného digitálního trhu uznává souvislost mezi kontrolou nad daty velkého objemu a tržní silou. Sdílí přesvědčení, vyjádřené v našem předběžném stanovisku k „soukromí a konkurenceschopnosti ve věku dat velkého objemu“ z roku 2014, o potřebě užšího dialogu mezi regulačními orgány. EU již dnes má nástroje k nápravě nerovnováhy sil na digitálním trhu: například probíhající antimonopolní řízení Evropské komise jsou uznáním převahy mobilních zařízení v přístupu na internet. Komplexnější vymáhání je možné ve stávajícím právním rámci, například prostřednictvím informačního střediska EU pro orgány dohledu, při zvážení, zda jednotlivé případy mohou vyvolat otázky o dodržování pravidel hospodářské soutěže, ochrany spotřebitele i osobních údajů. Například:

- vyžadování větší transparentnosti cen - v hotovosti nebo jinak - za službu může informovat a usnadnit analýzu případů v oblasti hospodářské soutěže[34] a
- zjišťování nespravedlivé cenové diskriminace na základě nedostatečné kvality dat a nepoctivého profilování a korelací[35].

Užší dialog mezi regulačními orgány z různých odvětví by mohl vést k reakci na rostoucí výzvy ke globálnímu partnerství, které by mohlo vytvořit „společný stůl“ otevřených údajů, kam by data a myšlenky, jako například statistiky a mapy, mohly plynout, kde by byly k dispozici a kde by se mohly vyměňovat ve veřejném zájmu s menším rizikem sledování tak, aby jednotlivci měli větší vliv na rozhodnutí, která se jich týkají[36].

2.2 Zodpovědní správci

Odpovědnost si vyžaduje zavedení vnitřních politik a kontrolních systémů, které zajistí soulad a poskytnou relevantní důkazy, zejména nezávislým orgánům dohledu.

Prosazovali jsme odstranění byrokracie v oblasti práva na ochranu údajů tak, abychom minimalizovali požadavky na zbytečnou dokumentaci a maximalizovali tak prostor pro zodpovědnější podněty ze strany podniků, které budou podpořeny radami orgánů pro ochranu údajů. Zásada, že osobní údaje by měly být zpracovávány pouze způsobem kompatibilním s konkrétním účelem (účely), pro který byly shromážděny, je zásadní pro respektování legitimních očekávání jednotlivců. Například kodexy chování, audity, certifikace i nové generace smluvních doložek a závazných podnikových pravidel mohou přispět k vybudování robustní důvěry v digitální trh. Osoby zodpovědné za zacházení s osobními informacemi, by měli být mnohem dynamičtější a proaktivní a upustit od tak zvané tendence „černé skříňky“, pokud jde o mlčenlivost a neprůhlednost obchodních praktik, a zároveň by měli vyžadovat stále větší transparentnost zákazníků[37].

2.3 Inženýrství berouc ohled na soukromí

Lidské inovace byly vždy produktem činností konkrétních sociálních skupin ve specifických kontextech obvykle odrážejících společenské normy své doby[38]. Nicméně rozhodnutí, pokud jde o technologický návrh, by neměla diktovat naše sociální interakce a strukturu našich komunit, ale spíše by měla podporovat naše hodnoty a základní práva.

EU by měla vyvíjet a podporovat inženýrské techniky a metody, které umožní zavedení takových technologií zpracování dat, jež budou plně respektovat důstojnost a práva jednotlivce. Systémoví a softwaroví inženýři musí porozumět zásadám ochrany soukromí již

od návrhu a lépe je uplatňovat v nových produktech a službách ve všech fázích vývoje a u všech technologií. Odpovědnost musí být podporována větším výzkumem a vývojem metod a nástrojů pro zajištění přesných auditů a pro stanovení dodržování pravidel ze strany správců a zpracovatelů údajů, jako například „označování“ každé jednotky osobních údajů tzv. „metadaty“, která popisují požadavky na ochranu údajů.

Inženýrská řešení by měla posilovat jednotlivce, kteří si chtějí zachovat své soukromí a svobody prostřednictvím anonymity. EU by měla podporovat navrhování a zavádění algoritmů, které skrývají identitu a souhrnné údaje, aby ochránily jednotlivce, společně s využitím prediktivních schopností údajů[39].

Musíme dnes položit základy pro řešení těchto úkolů tím, že spojíme vývojáře a odborníky na ochranu údajů z různých oblastí do širokých sítí, jako je například Internet Privacy Engineering Network (IPEN), které přispějí k plodné interdisciplinární výměně nápadů a přístupů.

2.4 Silnější jednotlivci

Prostředí „profesionálních konzumentů“

Jednotlivci nejsou jen pasivními objekty, které potřebují ochranu zákona před zneužíváním. Digitální trendy popsané výše představují pozitivní příležitosti pro posílení role jednotlivce. Například, lidé nyní vytvářejí i konzumují obsah a služby a stále mohou být považováni za spoluzodpovědné společně s poskytovateli služeb za zpracování osobních údajů, pokud to je pro čistě „domácí“ účely [40] (vznikl pojem „profesionální konzument“, který popisuje tento vývoj[41]). Mezitím, virtuální měny nabízejí uživatelům anonymitu a obejití ověření transakcí třetí stranou, což snižuje transakční náklady při placení za zboží a služby do zahraničí. Na druhé straně, anonymita a mezi-jurisdikční (nebo možná i *mimo-jurisdikční*) povaha těchto virtuálních měn způsobuje, že jednotlivci nejsou chráněni před podvodem a kriminální trhem, který se obtížně odhaluje a vyšetřuje. Vedle existujících povinností regulačních orgánů, podniků a inženýrů, také občané mají povinnost být bdělí, ostražití, kritičtí a informovaní, když se rozhodují on-line i off-line[42].

Souhlas

Navíc, v rozporu s tradičním myšlením, ne všechno lidské chování lze vysvětlit ekonomickými principy, které předpokládají, že lidské bytosti jsou zcela racionální a citlivé na ekonomické pobídky[43]. To je důležité pro budoucí úlohu souhlasu, který jednotlivec poskytuje se zpracováním svých osobních údajů. Podle právních předpisů EU, souhlas není jediným legitimním základem pro většinu zpracování. Dokonce i tam, kde souhlas hraje důležitou roli, nezbavuje správce údajů jejich odpovědnosti za to, co s údaji dělají, zejména tam, kde byl získán všeobecný souhlas se zpracováním pro širokou škálu účelů.

Kontrola a „vlastnictví“ údajů

Jednotlivci musí mít možnost zpochybnit chyby a nekalé zaujatosti plynoucí z logiky, kterou používají algoritmy při určování domněnek a předpovědí. Pro ilustraci, v USA bylo prověřeno téměř 3 000 úvěrových zpráv o 1000 spotřebitelích a bylo zjištěno, že 26 procent z nich mělo problémy s „podstatnými“ chybami, které byly natolik závažné, že ovlivnily kreditní skóre spotřebitele a tím i jeho náklady na získání úvěru[44].

Data jsou často považována za zdroje, jako je ropa, se kterými se obchoduje, v ideálním případě mezi stejně dobře informovanými účastníky transakce[45]. Zákazníci nedostávají spravedlivou kompenzaci za své osobní informace, se kterými se obchoduje, a někteří argumentují ve prospěch modelu vlastnictví údajů. Absolutní kontrolu nad osobními údaji je však obtížné zajistit - existují další obavy, jako je veřejný zájem a práva a svobody druhých. Kontrola je nutná, ale ne dostačující[46]. Nicméně lidská důstojnost je vždy konstantní a podle právních předpisů EU analogie vlastnictví nemůže být použita jako taková na osobní informace, které mají vnitřní vazbu na jednotlivé osoby. Neexistuje žádné ustanovení zákonů EU o ochraně údajů umožňující, aby se jednotlivec vzdal tohoto základního práva.

Jednou alternativní metodou, jak poskytnout jednotlivcům lepší kontrolu nad jejich údaji i nad tím, kdo k nim může přistupovat a za jakým účelem, může být použití úložišť osobních údajů nebo „datových trezorů“[47]. Koncepce takového „osobního úložiště“ si vyžaduje bezpečnostní mechanismy, které zajistí, že pouze osoby oprávněné subjektem údajů budou mít přístup k datům a navíc pouze k těm částem, pro které mají oprávnění. Úložiště osobních údajů by byla nejúčinnější tam, kde by se týkala aktuálních a neustále aktualizovaných informací, jako jsou geoprostorová data nebo životní funkce. Kromě technických záruk by uživatelé údajů byli povinni dodržovat pravidla pro sdílení a použití údajů. Hospodářská soutěž a možnost změnit službu, již člověk používá, je jediným nejúčinnějším nástrojem spotřebitele, kterým může ovlivnit trh služeb, jež má k dispozici. Zajištění přenositelnosti připojení, včetně identifikátorů a kontaktních informací, se ukázalo být účinným prostředkem pro hospodářskou soutěž a účinné snížení spotřebitelských cen, když došlo k liberalizaci telekomunikačního trhu. Přenositelnost údajů, tedy věcná a praktická možnost převést většinu vlastních údajů od jednoho poskytovatele služeb k jinému, je účinným východiskem pro vytvoření podmínek pro skutečnou možnost volby pro spotřebitele.

3. Důstojnost v centru nové digitální etiky

Etický rámec musí podpořit stavební kameny tohoto digitálního ekosystému. Evropský inspektor ochrany údajů se domnívá, že lepší dodržování a zajištění lidské důstojnosti by mohly být protiváhou všudypřítomného sledování a asymetrie moci, které nyní jednotlivci čelí. Musí stát v centru nové digitální etiky.

3.1 Důstojnost a data

Bezprostředně po průmyslové revoluci v 18. a 19. století se hnutí za lidská práva snažila zajistit širší společenské dobro tím, že omezí překážky pro respektování jednotlivce. EU si nyní ve své Listině základních práv, která vychází ze Všeobecné deklarace lidských práv a Evropské úmluvy o lidských právech, vzala za výchozí bod nedotknutelnost lidské důstojnosti. Důstojnost lidské bytosti není jen základním právem jako takovým, ale také základem pro následné svobody a práva, včetně práv na soukromí a na ochranu osobních údajů[48]. Mezi porušení důstojnosti může patřit objektifikace, kdy je s člověkem zacházeno jako s nástrojem sloužícím pro účely někoho jiného[49]. Soukromí je nedílnou součástí lidské důstojnosti a právo na ochranu údajů bylo původně koncipováno v 70. a 80. letech 20. století jako způsob, jak kompenzovat možné narušování soukromí a důstojnosti zpracováním osobních údajů ve velkých objemech. V Německu právo na „informační sebeurčení“ vycházelo z práva na lidskou důstojnost a svobodný rozvoj osobnosti, jak jsou stanovena v článcích 1 a 2 německé ústavy[50].

Nicméně na počátku 21. století jednotlivci stále častěji musí poskytovat mnohem více osobních údajů prostřednictvím internetu, aby se mohli účastnit na sociálních,

administrativních a obchodních záležitostech, a při tom mají stále omezenější prostor pro odhlášení. Vzhledem k tomu, že veškeré aktivity jsou potenciálně vždy on-line, pojem svobodného a informovaného souhlasu je vystaven obrovskému tlaku. „Digitální drobky“ jsou sbírány každou minutu a kombinovány, aby klasifikovaly jednotlivce v reálném čase a vytvářely různé profily, které jsou však někdy protichůdné. Tyto profily mohou být rozeslány v mikrosekundách, aniž by o tom jednotlivci věděli, a slouží jako základ pro důležitá rozhodnutí jich se týkající.

Profily používané k předpovídání chování přinášejí riziko stigmatizace, posilování stávajících stereotypů, sociální a kulturní segregace a vyloučení[51], přičemž taková „kolektivní inteligence“ rozvrací individuální volbu a rovné příležitosti. Takové „filtrovací bubliny“ nebo „osobní dozvukové komory“ by nakonec mohly udusit samotnou kreativitu, inovace i svobody projevu a sdružování, které umožnily rozkvět digitálních technologií.

Mezitím se pokračující výjimky z důvodu „bezpečnosti“ používají k ospravedlnění vícenásobného vrstvení dotěrných technik pro monitorování aktivity jednotlivců[52]. Pochopení této „spirály sledování“ vyžaduje dlouhodobější perspektivu, co se týče celkových dopadů na společnost a chování.

Společně se třetími zeměmi musí EU intenzivně pracovat na tom, jak zajistit, aby tyto hodnoty byly respektovány nejen na papíře, zatímco v kyberprostoru jsou ve skutečnosti neutralizovány. Zejména EU má nyní „kritické okno“, než nastane masové rozšíření těchto technologií, aby zabudovala tyto hodnoty do digitálních struktur, které budou definovat naši společnost[53]. To vyžaduje nové posouzení, zda potenciální přínosy nových technologií skutečně závisí na sběru a analýze osobně identifikovatelných údajů miliard jednotlivců. Takové posouzení by mohlo donutit vývojáře, aby navrhovali produkty, které budou depersonalizovat v reálném čase obrovské objemy neorganizovaných informací a tím ztíží nebo znemožní identifikaci jednotlivce.

Již jsme uznali, že zpracování určitých údajů, například genetických údajů, musí být nejen regulováno, ale také musí být předmětem posouzení širších společenských problémů, například ze strany etických komisí. Ze své podstaty se genetická data netýkají pouze jedné osoby, ale také jejích předků a potomků. Genetické údaje slouží nejen k identifikaci rodinných vztahů, ale prvky nalezené v genech jedné osoby mohou také poskytnout informace o jejích rodičích a dětech a vést k takovým rozhodnutím správců, která ovlivní jejich šance v životě ještě před jejich narozením. Potenciální koncentrace genetických osobních údajů v rukou několika obrovských hráčů na trhu má dopad na tržní ekonomiku, stejně jako na subjekty údajů. Rostoucí závislost na globálním systému sběru a analýzy konstantního toku dat by mohla způsobit, že společnost i hospodářství budou více ohroženy bezprecedentními bezpečnostními chybami a nebezpečnými útoky.

Stávající rámec by mohl selhat, pokud nebudeme přistupovat k budoucnosti s novátorským myšlením. Existuje rostoucí poptávka a je třeba brát subjekt údajů jako jednotlivce a ne pouze jako spotřebitele nebo uživatele. Skutečně nezávislé orgány pro ochranu údajů mají klíčovou roli v prevenci budoucnosti, kde jednotlivci budou určeni algoritmy a jejich neustálými variacemi. Musí být dostatečně vybaveny, aby mohly plnit „povinnost péče“ o jednotlivce a jejich on-line důstojnost. Tradiční pojmy a principy ochrany soukromí a údajů již obsahují etické nuance na ochranu důstojnosti, jako je zaměstnanost a zdraví. Ale dnešní trendy otevřely zcela novou kapitolu a je třeba prozkoumat, zda jsou tyto zásady dostatečně robustní pro digitální věk[54]. Pojem osobních údajů sám o sobě se pravděpodobné radikálně změní s tím, jak technologie stále více umožňují znovu identifikovat jednotlivce z údajně

anonymních dat. Navíc, strojové učení a sloučení lidské a umělé inteligenci podkopou pojetí práv a odpovědnosti jednotlivce.

3.2 Evropská etická poradní skupina

Naším cílem není malovat alarmující obraz dystopie. Již probíhají diskuse v právních, politických, ekonomických, sociálních, vědeckých a dokonce i náboženských kruzích[55]. Zjednodušující postupy, které dávají jednostrannou výhodu ekonomickému zisku či sledování pro zajištění bezpečnosti, nejsou pravděpodobně o nic užitečnější než příliš restriktivní uplatňování stávajících zákonů, které brzdí inovace a pokrok. Evropský inspektor ochrany údajů proto navrhuje důkladnou, širokou a multidisciplinární analýzu, která by poskytla doporučení a přispěla do společenské diskuse o tom, jak by svobodná, demokratická společnost mohla dostát technologickým výzvám.

Strategie evropského inspektora ochrany údajů [56] je zaměřena na vývoj etického přístupu k ochraně údajů, který uznává, že „možné, užitečné nebo ziskové neznamená nutně udržitelné“ a která upřednostňuje „odpovědnost před mechanickým dodržováním litery zákona“. Máme v úmyslu oslovit osobnosti mimo obec úředníků, právníků a IT specialistů EU, a to významné osobnosti, které jsou vybaveny schopností posoudit střednědobé až dlouhodobé dopady technologických změn a regulačních reakcí. V následujících měsících založíme ve své nezávislé instituci externí poradní skupinu k etickým aspektům ochrany údajů, která bude zkoumat vztahy mezi lidskými právy, technologiemi, trhy a obchodními modely v 21. století.

Naše etická poradní skupina bude složena z vybrané skupiny významných osobností z oblasti etiky a filozofie, sociologie, psychologie, techniky a ekonomie a podle potřeby bude podporována dalšími odborníky s odbornými znalostmi a zkušenostmi v oblastech jako je zdravotnictví, doprava a energetika, sociální interakce a média, hospodářství a finance, správa věcí veřejných a demokracie a bezpečnost a policie. Budou vyzváni, aby zvážili širší etické důsledky toho, jak jsou osobní údaje koncipovány a používány, a jejich uvažování bude poskytnuta maximální transparentnost.

4. Závěr: Je čas prohloubit diskusi

Ochrana soukromí a osobních údajů je součástí řešení, nikoli problém. V současné době jsou technologie kontrolovány lidmi. Není snadné jednoduše zhodnotit tento potenciální vývoj jako dobrý nebo špatný, žádoucí nebo škodlivý, výhodný či zhoubný, zejména i proto, že v kontextu je třeba vidět řadu potenciálních trendů. Tvůrci politik, vývojáři technologií i obchodních modelů a my všichni musíme důkladně zvážit, zda a jak chceme ovlivnit vývoj technologií a jejich použití. Ale stejně důležité je, aby EU naléhavě zvážila etiku a místo pro lidskou důstojnost v technologiích budoucnosti.

Zásady ochrany údajů prokázaly schopnost chránit jednotlivce a jejich soukromí před riziky nezodpovědného zpracování dat. Ale dnešní trendy si mohou vyžadovat zcela nový přístup. Proto otevíráme novou debatu o tom, do jaké míry je dostačující uplatňování zásad, jako je spravedlnost a legitimita. Orgány pro ochranu údajů mohou hrát novou roli s využitím stávajících nástrojů, jako je předběžná kontrola a schválení - protože žádné jiné orgány nejsou vybaveny pravomocí ke zkoumání takového zpracování dat. Díky technologiím, globální inovaci a lidské sounáležitosti, které se rozvíjejí překotným tempem, máme příležitost, jak přilákat pozornost, vyvolat zájem a vybudovat konsensus.

Doufám, že tímto stanoviskem poskytneme rámec pro širší a hlubší diskusi o tom, jak může EU zajistit integritu svých hodnot současně s tím, jak přijímá přínosy nových technologií.

V Bruselu dne 11. září 2015

(**podpis**)

Giovanni BUTTARELLI
Evropský inspektor ochrany údajů

Poznámky

[1] Zdroj: Zpráva GSMA.

[2] „Moorův zákon“, že počet tranzistorů, které se mohou umístit na jeden mikročip, se zdvojnásobí přibližně jednou za 18 let, se ukázal jako poměrně přesný; Moore, Gordon E. (19.4.1965). „Cramming more components onto integrated circuits“, Electronics. 22. 8.2011

[3] Nathan Eagle, Alex (Sandy) Pentland, „Reality mining: sensing complex social systems“, Journal Personal and Ubiquitous Computing svazek 10, vydání 4, březen 2006, s. 255–268. Shoshana Zuboff v článku „Big Other: surveillance capitalism and the prospects of an information civilization“ uveřejněném v Journal of Information Technology (2015) 30 na stranách 75-89 píše „V důsledku všudypřítomné počítačové mediace je téměř každý aspekt světa vykreslen v nové symbolické dimenzi jako události, objekty a procesy a lidé se stávají viditelnými, poznatelnými a sdílitelnými novým způsobem“. Zuboff předpokládá „vzestup nové univerzální architektury“, kterou nazývá „Big Other“, jako „všudypřítomného systému zasíťovaných institucí, jež zaznamenává, upravuje a mění na komoditu každodenní zkušenosti od topinkovačů k tělům, od komunikací k myšlenkám, to vše s cílem vytvořit nové cesty ke zpeněžení a zisku“; s. 77, 81.

[4] „BBC Micro Bit computer's final design revealed“ 7.7.2015, http://www.bbc.com/news/technology-33409311(accessed 10.09.2015); „No assembler required: How to teach computer science in nursery school“, The Economist, 1.8.2015.

[5] Žádná z deseti největších společností v technologickém sektoru podle tržní kapitalizace nemá sídlo v Evropské unii (osm z nich jsou americké společnosti, zbývající dvě jsou z Číny a Tchaj-wanu) podle žebříčku PWC Global Top Ten Companies by Market Capitalisation vydaného 31. března 2015.

[6] „Data velkého objemu souvisí s exponenciálním růstem jak dostupnosti, tak automatizovaného využití informací: označují se tak obrovské soubory digitálních dat, které jsou v držení podniků, vlád a dalších velkých organizací a které jsou následně důkladně analyzovány (proto název: analytika) pomocí počítačových algoritmů“; stanovisko 3/2013 pracovní skupiny zřízené podle článku 29 o účelovém omezení. Zpráva Bílého domu z roku 2014 popsala data velkého objemu jako „rostoucí technologickou schopnost zaznamenávat, sdružovat a zpracovávat údaje stále většího objemu, rychlosti a rozmanitosti“, viz Big Data: Seizing Opportunities, Preserving Values, Executive Office of the President (‘Podesta-report’), květen 2014.

[7] Podle právních předpisů EU jsou „osobní údaje“ definovány jako „jakékoli informace o identifikované nebo identifikovatelné fyzické osobě („subjektu údajů“); identifikovatelnou osobou se rozumí osoba, jejíž totožnost lze přímo či nepřímo zjistit, zejména s odkazem na identifikační číslo nebo na jeden či více zvláštních prvků její fyzické, fyziologické, psychické, ekonomické, kulturní nebo sociální identity“; čl. 2 písm. a) směrnice 95/46/ES. Tato definice je v podstatě srovnatelná s definicí přijatou Radou Evropy v Úmluvě o ochraně osob se zřetelem na automatizované zpracování osobních dat (známé jako Úmluva 108) a definicí ve Směrnici OECD o ochraně soukromí a přeshraničních tocích osobních údajů. Pro podrobnější analýzu viz pracovní skupina zřízená podle článku 29: stanovisko k pojetí osobních údajů, WP136.

[8] Viz například projev předsedkyně Federální obchodní komise USA z roku 2014: „Rozrůstání připojených zařízení, padající náklady na shromažďování, ukládání a zpracování informací a schopnost datových makléřů i jiných kombinovat off-line a on-line data znamená, že společnosti mohou hromadit prakticky neomezené množství informací o spotřebitelích a uchovávat je na dobu neurčitou. S využitím prediktivní analýzy se z nich mohou dozvědět překvapivé množství informací o každém z nás“ úvodní slovo předsedkyně FTC Edith Ramirezové, „Big Data: A Tool for Inclusion or Exclusion?“, Washington, DC 15. září 2014. Podle Sandy Pentland „sociální fyzika je kvantitativní sociální věda, která popisuje spolehlivé, matematické spojení mezi informacemi a myšlenkovým tokem na jedné straně a chováním lidí na straně druhé ... umožňuje nám předpovídat produktivitu malých skupin, oddělení v rámci společností a dokonce i celých měst“. To „je to, co potřebujeme,

abychom vytvořili lepší sociální systémy“ (s. 4, 7) a aby „mohli (vládní úředníci, ředitelé podniků i občané) využívat nástrojů pobídek sociálních sítí k *vytvoření nové normy chování“* (s. 189) (naše kurzíva); Pentland, *Social Physics: How Good Ideas Spread: The Lessons from a New Science*.

[9] Zvláštní průzkum Eurobarometru 431 o ochraně údajů, červen 2015 a panelový průzkum Pew Research Center z ledna 2014 „Public Perceptions of Privacy and Security in the Post-Snowden Era“. Podle jedné studie jediná průměrná návštěva jedné webové stránky má za následek 56 případů sběru dat, jak říká Julia Angwin *Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance*, 2012). Zpráva Bílého domu z roku 2014 k datům velkého objemu tvrdí, že „bezprecedentní výpočetní výkon a sofistikovanost ... vytvářejí asymetrii moci mezi těmi, kdo data mají, a těmi, kdo je úmyslně nebo neúmyslně poskytují“; „některé z nejhlubších problémů zjištěných během tohoto přezkumu se týkají toho, jak analytika dat velkého objemu může ... vytvořit tak neprůhledné prostředí pro rozhodování, že se individuální autonomie ztrácí v neproniknutelné sadě algoritmů“.

[10] S využitím veřejných anonymních dat ze sčítání lidu v roce 1990 může být 87 % americké populace pravděpodobně identifikováno prostřednictvím jejich pětimístného PSČ v kombinaci s pohlavím a datem narození; viz Paul Ohm „Broken promises of privacy: responding to the surprising failure of anonymisation“, UCLA Law Review 2010 a „Record linkage and privacy: issues in creating new federal research and statistical info“, duben 2011. DNA je unikátní (s výjimkou identických dvojčat) a stabilní po celý život. Obsahuje informace o etnickém původu, náchylnosti k onemocnění a může identifikovat ostatní členy rodiny. V lednu roku 2013 byli vědci schopni identifikovat jednotlivce a rodiny z anonymních údajů o DNA z veřejně přístupných genealogických databází; Gymrek, M., McGuire, A. L., Golan, D., Halperin, E. & Erlich, Y. *Science* 339, 321–324 (2013). Viz také „Poorly anonymized logs reveal NYC cab drivers' detailed whereabouts“, 23.6.2014 http://arstechnica.com/tech-policy/2014/06/poorly-anonymized-logs-reveal-nyc-cab-drivers-detailed-whereabouts/ (přístup ověřen 10.9.2015). Viz pracovní skupina zřízená podle článku 29: stanovisko 04/2007 k pojetí osobních údajů, stanovisko 03/2013 k omezení účelu, stanovisko 06/2013 k veřejně přístupným údajům a opakovanému použití 'PSI' a stanovisko 05/2014 k anonymizaci.

[11] Zdroj: Gartner.

[12] Viz například panelová diskuse „What is the future of official statistics in the Big Data era?“ Royal Statistical Society, Londýn. 19. ledna 2015; http://www.odi.org/events/4068-future-official-statistics-big-data-era (přístup ověřen 10.9.2015).

[13] Ten technologies which could change our lives: potential impacts and policy implications, Scientific Foresight Unit, Výzkumná služba Evropského parlamentu, leden 2015.

[14] Pracovní program programu EU „Horizont 2020“ na léta 2016–2017 podporuje tento vývoj včetně rozsáhlých pilotních programů, které se budou zabývat záležitostmi soukromí a etiky.

[15] Pojištění bylo popsáno jako „přirozený obchodní model pro internet věcí“; „From fitness trackers to drones, how the 'Internet of Things' is transforming the insurance industry“, Business Insider 11.6.2015. Pojem cenové diskriminace v soutěžním právu, jak vyplývá z článku 102 Smlouvy o fungování EU, který zakazuje podnikům v dominantním postavení na trhu, aby „přímo či nepřímo vynucovaly nepřiměřené nákupní nebo prodejní ceny anebo jiné nerovné obchodních podmínky“, je vysoce diskutabilní, viz například Damien Gerardin and Nicolas Petit Price Discrimination Under EC Competition Law: Another Antitrust Theory in Search of Limiting Principles (červenec 2005), Global Competition Law Centre Working Paper Series č. 07/05. Pokud jde o data velkého objemu a jejich (podle autorů dosud nerealizovaný) potenciál k urychlení personalizovaného určování cen, viz Výkonný úřad prezidenta Spojených států: Big Data and Differential Pricing, únor 2015 a nedávná analýza, která dochází k závěru, že individuální stanovení ceny obecně zahrnuje zpracování osobních údajů, a proto musí respektovat zásadu transparentnosti obsaženou v zákoně o ochraně údajů, která vyžaduje, aby společnosti informovaly lidi o účelu zpracování jejich osobních údajů: firmy musí informovat, že personalizují ceny. A v případě, že společnost používá soubory cookie k rozpoznání uživatele, směrnice o e-soukromí požaduje, aby společnost informovala osobu o účelu souborů

cookie; pracovní návrh Frederika Borgesiuse „Online Price Discrimination and Data Protection Law“. K dispozici na http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2652665 (přístup ověřen 10.9.2015).

[16] Zdravotnické prostředky jsou definovány v rámci právních předpisů EU ve směrnici Rady 93/42/EHS o zdravotnických prostředcích ve znění směrnice 2007/47/ES Evropského parlamentu a Rady ze dne 5. září 2007. Více o dopadech „mobilního zdraví“ na ochranu údajů viz stanovisko EIOÚ 1/2015.

[17] Podle údajů Eurostatu 21 % fyzických osob a 19 % podniků v EU využívá služeb cloudových úložišť.

[18] „Pokud by světový internet byl státem, byl by 12. největším spotřebitelem elektrické energie na světě, někde mezi Španělskem a Itálií. To představuje zhruba 1,1 až 1,5 procenta celosvětové spotřeby elektřiny (k roku 2010) a produkci skleníkových plynů odpovídající každý rok 70 až 90 velkým (500megawattovým) uhelným elektrárnám“. Natural Resources Defense Council, Data Centre Efficiency Assessment: Scaling Up Energy Efficiency Across the Data Centre Industry: Evaluating Key Drivers and Barriers 2014.

[19] Zpráva ze studie „SMART 2013/0043 - Uptake of Cloud in Europe“.

[20] Zdroj: Eurostat.

[21] Pojem „ekonomika sdílení“ byl kritizován jako zavádějící: „The Sharing Economy Isn't About Sharing at All“, Giana M. Eckhardt a Fleura Bardhi, Harvard Business Review, 28.01.2015.

[22] Rachel Botsman a Roo Rogers, *What's Mine Is Yours: How Collaborative Consumption is Changing the Way We Live*, 2011.

[23] Fórum Future of Privacy, „User Reputation: Building Trust and Addressing Privacy Issues in the Sharing Economy“, červen 2015.

[24] Viz seminář Federální obchodní komise USA konaný 9. června 2015 na téma „Competition, Consumer Protection, and Economic Issues Raised by the Sharing Economy“, https://www.ftc.gov/news-events/events-calendar/2015/06/sharing-economy-issues-facing-platforms-participants-regulators/ (přístup ověřen 10.9.2015).

[25] Více o dopadech dronů nebo dálkově řízených letounů na ochranu údajů viz stanovisko EIOÚ ke sdělení Komise Evropskému parlamentu a Radě s názvem „Nová éra letectví – Otevření leteckého trhu pro bezpečné a udržitelné civilní využití dálkově řízených letadlových systémů“’, listopad 2014.

[26] Zdroj: Boston Consulting Group.

[27] Gartner.

[28] Algoritmus pro rozeznávání obličejů DeepFace na Facebooku dosáhl 97% úspěšnosti - lepší než lidé; DeepFace: Closing the Gap to Human-Level Performance in Face Verification, zveřejněno ve zprávě na konferenci IEEE Conference on Computer Vision and Pattern recognition, červen 2014.

[29] Robot byl definován jako „stroj nacházející se ve světě, který vnímá, myslí a jedná“; Bekey, G, Current trends in robotics: technology and ethics, in Robot Ethics - The ethical and social implications of robotics, The MIT Press 2, 2012, s. 18. Odhaduje se, že mezi lety 2013 a 2016 bude prodáno 22 milionů servisních robotů; IFR World Robotics Report, 2013. Více k umělé inteligenci viz Rise of the Machines, Economist, 9.5.15 a internetový projekt Pew Research Centre 2014. Společnost zabývající se umělou inteligencí podmínila v roce 2014 své získání technologickou společností založením komise pro etiku a bezpečnost a zákazem používat umělou inteligenci pro vojenské nebo zpravodajské účely; Forbes, Inside Google's Mysterious Ethics Board, 03.02.2014.

[30] Pentland, *Social physics*, s. 147.

[31] Viz poznámka 9 výše. Pentland *Social Physics* , s.153: „Velké pokroky ve zdravotnictví, dopravě, energetice a bezpečnosti jsou všechny možné... hlavními překážkami pro dosažení těchto cílů jsou

obavy týkající se soukromí a skutečnost, že jsme dosud nedošli ke shodě ohledně kompromisu mezi osobními a společenskými hodnotami“. Debata kolem pandemie eboly v roce 2014 v západní Africe je příkladem toho, jak tato falešná dichotomie mezi individuálními soukromými a společenskými potřebami vzniká. Existuje tendence sledovat nemoci a měřit jejich trvání prostřednictvím výzkumů a sčítání, aby bylo možné předpovědět, kde nemoc udeří příště. Avšak výsledky takových výzkumů a sčítání snadno zastarají a obtížně se extrapolují. Zde jsou některé příklady použití „dat velkého objemu“ ke sledování ohnisek malárie v Namibii a v Keni a v roce 2009 ke sledování účinnosti vládních zdravotních výstrah během krize s mexickou prasečí chřipkou. Jedním zdrojem dat jsou záznamy o volání z mobilních telefonů, které obsahují základnovou stanici, jež hovor zpracovala, a které tak mohou dávat v reálném čase hrubý odhad polohy lidí i toho, kam jdou. Shromažďování všech těchto záznamů není cílené - nelze rozlišit mezi těmi, kdo mají ebolu, a těmi, kdo ji nemají. Švédská nezisková organizace mapovala mobilitu populace v Západní Africe, ale údaje nebyly použity, protože mobilní operátoři je neposkytli schváleným externím výzkumníkům s prohlášením, že potřebují pokyny od vlád, které naopak vyslovily obavy o ochranu osobních údajů, jež nemohla být podle právních předpisů EU zaručena; http://www.pri.org/stories/2014-10-24/how-big-data-could-help-stop-spread-ebola. (přístup ověřen 10.9.2015)

[32] Stanovisko evropského inspektora ochrany údajů 3/2015.

[33] Předpoklad dat velkých objemů, že „N=všechno“, znamená sledování všech datových bodů, ne jen vzorku, Viktor Mayer-Schönberger a Kenneth Cukier, *The Rise of Big Data: How it's changing the way we think about the world*, 2013. Organizace Lisbon Council a Progressive Policy Institute argumentovaly, že prosperita vzroste, když se maximalizuje „digitální hustota“- „množství dat použitých v ekonomice na jednoho obyvatele“ http://www.lisboncouncil.net/component/downloads/?id=1178 (přístup ověřen 10.9.2015). Mezinárodní pracovní skupina pro ochranu údajů v telekomunikacích (známá jako „Berlínská skupina“) navrhla pro data velkých objemů výjimku ze zásad ochrany údajů; http://www.datenschutz-berlin.de/attachments/1052/WP_Big_Data_final_clean_675.48.12.pdf. (přístup ověřen 10.9.2015). Světové ekonomické fórum vyzvalo k zaměření se na použití a ne na shromažďování údajů a ustoupení od požadavku na souhlas se shromažďováním osobních údajů; Unlocking the Value of Personal Data: From Collection to Usage, 2013.

[34] Viz předběžné stanovisko EIOÚ k soukromí a konkurenceschopnosti ve věku dat velkého objemu.

[35] Článek 21 Listiny základních práv zakazuje „jakoukoliv diskriminaci z jakýchkoli důvodů, zejména z důvodů jako jsou pohlaví, rasa, barva pleti, etnický nebo sociální původ, genetické rysy, jazyk, náboženské vyznání nebo víra, politický nebo jakýkoli jiný názor, příslušnost k národnostní menšině, majetkové poměry, původ, zdravotní postižení, věk nebo sexuální orientace“. Mnohým z těchto kategorií údajů („odhalující rasový či etnický původ, politické názory, náboženské nebo filozofické přesvědčení, členství v odborech a zpracování údajů týkajících se zdraví nebo sexuálního života“) je poskytována zvýšená ochrana podle článku 8 směrnice 95/46/ES.

[36] Více k myšlence „společných digitálních prostorů (digital commons)“ viz Ambition numérique: Pour une politique française et européenne de la transition numérique, French Digital Council, červen 2015, s. 276; Bruce Schneier podporuje vytváření „nikomu nepatřících veřejných prostorů“ na internetu, podobných veřejným parkům, *Data and Goliath*, s. 188-189; Sandy Pentland propaguje „veřejné společné datové prostory“, *Social Physics*, s. 179. Více k hodnocení bezpečnosti zveřejňování agregovaných datových souborů jako veřejně přístupných údajů viz stanovisko skupiny zřízené podle článku 29 č. 06/2013 k veřejně přístupným údajům a opakovanému použití informací veřejného sektoru.

[37] „Während die Einzelnen immer transparenter werden, agieren viele Unternehmen hochgradig intransparent“ http://crackedlabs.org/studie-kommerzielle-ueberwachung/info. Více ke kvalifikované průhlednosti viz např. Frank Pasquale: *The Black Box Society: The Secret Algorithms that Control Money and Information*.

[38] „Za technologiemi, které ovlivňují sociální vztahy, vězí tytéž sociální vztahy“, David Noble, ‘Social Choice in Machine Design: The Case of Automatically Controlled Machine Tools’, v *Case Studies in the Labor Process*, vyd. Andrew Zimbalist, 1979. Viz také Judy Wacjman, *Pressed for Time: The Acceleration of Life in Digital Capitalism*, 2014 s. 89-90; a Zuboff, ‘Big Other’ (citováno v poznámce 3 výše).

[39] Stanovisko 05/2014 k technikám anonymizace přijaté 10. dubna 2014 (WP 216.)

[40] Více k úzce interpretované výjimce z pravidel pro ochranu údajů pro čistě osobní nebo domácí účely, viz rozsudek SDEU v případě C-212/13 *František Ryneš v Úřad pro ochranu osobních údajů.*

[41] Termín profesionální konzument vymyslel Alvin Toffler v knize *The Third Wave*, 1980. Diskuse k „prostředí profesionálních konzumentů“ a jak by mělo být regulováno, viz Ian Brown a Chris Marsden, *Regulating Code*, 2013.

[42] Stanovisko Evropské skupiny pro etiku ve vědě a nových technologiích pro Evropskou komisi: Etika technologií pro zabezpečení a sledování, stanovisko č. 28, 20.5.2015, s. 74.

[43]Viz například, Homer Economicus: The Simpsons and Economics, vyd. Joshua Hall, 2014.

[44] I při nejkonzervativnější definici chyby by to znamenalo, že 23 milionů Američanů má závažné chyby ve své zprávě o spotřebiteli. Pět procent účastníků studie mělo takové chyby, že po jejich opravě se jejich kreditní skóre zlepšilo natolik, že mohli získat úvěr za nižší cenu; Federální obchodní komise, zpráva pro kongres podle článku 319 zákona o poctivých a přesných úvěrových obchodech z roku 2003, prosinec 2012; Chris Jay Hoofnagle, How the Fair Credit Reporting Act Regulates Big Data (10. září 2013). Seminář fóra Future of Privacy k datům velkého objemu a soukromí: Making Ends Meet, 2013. K dispozici na SSRN: http://ssrn.com/abstract=2432955.

[45] WEF postuluje data jako cenný majetek jednotlivce, jehož práva na vlastnictví, používání a likvidaci mohou být poskytnuta společnostem a vládám výměnou za služby. Viz nedávné projevy také vice-prezidenta Komise Ansipa, například 7.9.2015 na každoročním setkání v Bruegelu s názvem „Produktivita, inovace a digitalizace - které výzvy pro globální politiku?“: „Vlastnictví a řízení datových toků, použití a opakované použití údajů. Řízení a uchovávání údajů. Tyto jsou základem důležitých vznikajících odvětví jako je cloud computing, internet věcí a data velkého objemu“.

[46] „Kdo má tedy právo používat informace a údaje, které opravdu nepatří danému jednotlivci? Je to problém, který přesahuje hranice obchodu, etiky a morálky, což vede k otázkám soukromí a ochrany soukromí“; Al-Khouri, listopad 2012, http://www.academia.edu/6726887/Data_Ownership_Who_Owns_My_Data_036. Viz také Margaret Jane Radin, Incomplete Commodification in the Computerized World, v The Commodification of Information 3, 17, Niva Elkin-Koren & Neil Weinstock Netanel vyd. 2002: „Je velký rozdíl mezi tím, zda je soukromí považováno za lidské právo připadající osobám na základě jejich osobnosti nebo za vlastnické právo, tedy něco, co může být ve vlastnictví a pod kontrolou osob. Lidská práva jsou podle všeho na trhu nezcizitelná, zatímco vlastnická práva jsou podle všeho na trhu převoditelná“.

[47] Cílem projektu Crosscloud laboratoře Computer Science and Artificial Intelligence Lab MIT, který je podporován několika společnostmi se sídlem v EU, je „1) usnadnit vývoj víceuživatelského („sociálního“) softwaru při využití pouze vývoje na straně klienta (front-end) a při respektování práv a soukromí uživatelů. A 2) poskytnout uživatelům svobodu, aby mohli snadno přecházet mezi aplikacemi, hardwarovými platformami a sociálními sítěmi při zachování svých údajů a sociálních kontaktů“; http://openpds.media.mit.edu/#architecture (přístup ověřen 10.9.2015).

[48] Viz vysvětlení článku 1 Listiny základních práv.

[49] Martha Nussbaum, Objectification, in Philopsophy and Public Affairs 24, 4, 1995.

[50] Rozsudek z 15. prosince 1983, BVerfGE 65, 1-71, Volkszählung.

[51] Viz Evropská skupina pro etiku ve vědě a nových technologiích, stanovisko k etice a sledování, s. 75. Studie naznačila, že algoritmus vybírající cílenou reklamu byl diskriminační, protože při návštěvě

stránek s nabídkou pracovních míst vyhledávání průměrně nacházelo reklamy na lépe placená pracovní místa pro muže než pro ženy; Carnegie Mellon University and the International Computer Science Institute. K tendenci dávat ve výchozím nastavení digitálním asistentkám ženský hlas viz například Judy Wajcman, Feminist theories of technology. Cambridge Journal of Economics, 34 (1), s. 143-152, 2010.

[52] Giorgio Agamben, *State of Exeption, 2005.*

[53] Neil Richards, Neil a Jonathan King, Big Data Ethics (19. května 2014), Wake Forest Law Review, 2014.

[54] BBC, Information watchdog investigates 'charity data sales', 1.9.2015.

[55] Viz dopis od organizace Future of Life Institute. Papežská encyklika *Laudato Si:* „K tomu přistupuje dynamika médií a digitálního světa, který, stane-li se všudypřítomný, nepodporuje rozvoj schopnosti moudře žít, hloubavě přemýšlet a velkodušně milovat. Velkým mudrcům minulosti by v tomto kontextu hrozilo, že spatří svoji moudrost, jak se dusí uprostřed rozvratného hluku informací. Vyžaduje to od nás snahu, aby tyto prostředky přispívaly k novému kulturnímu vývoji lidstva, a nikoli k úbytku jeho nejhlubšího bohatství. Pravou moudrost, plod reflexe, dialogu a velkodušného setkání mezi lidmi, nelze dosáhnout pouhou akumulací dat, která zahlcují a matou na způsob mentálního znečistění. Reálné vztahy s druhými a všechno, co s sebou přinášejí, zároveň tíhnou k tomu, aby se nahradily typem komunikace zprostředkované internetem. To umožňuje selekci či eliminaci vztahů podle naší libovůle, čímž nezřídka vzniká nový typ umělých emocí, které se váží spíše k přístrojům a obrazovkám než k lidem a k přírodě. Nynější prostředky umožňují, abychom vzájemně komunikovali, sdíleli poznatky i pocity. Nicméně, někdy nám také brání navázat přímý kontakt s úzkostí, chvěním a radostí druhého a se složitostí jeho osobní zkušenosti. Proto by neměla udivovat skutečnost, že dotěrnou nabídku těchto produktů provází hluboké a melancholické neuspokojení v meziosobních vztazích či škodlivá osamělost".

[56] Viz Aktivita 4 v rámci strategie EIOÚ na léta 2015-2020, rozvoj etického rozměru ochrany údajů.