

EUROPEAN DATA PROTECTION SUPERVISOR

Stanovisko 4/2015

Smerom k novej digitálnej etike

Údaje, dôstojnosť a technológia



11. septembra 2015

Európsky dozorný úradník pre ochranu údajov (EDPS) je nezávislou inštitúciou EÚ, zodpovednou v súlade s článkom 41 ods. 2 nariadenia 45/2001 „Vzhľadom na spracovanie osobných údajov... za to, že inštitúcie orgány spoločenstva budú dodržiavať základné práva a slobody fyzických osôb, najmä ich právo na súkromie“... a „... za poradenstvo pre inštitúcie a orgány spoločenstva a dotknuté osoby vo všetkých veciach týkajúcich sa spracovania osobných údajov“. Bol vymenovaný v decembri 2014 spolu s asistentom dozorného úradníka s konkrétnou úlohou, aby bol konštruktívnejší a aktívnejší. EDPS uverejnil v marci 2015 päťročnú stratégiu, v ktorej je stanovené, ako plánuje splniť túto úlohu a ako bude zodpovedný za jej splnenie.

Toto stanovisko nadväzuje na predchádzajúce stanovisko EDPS ku všeobecnému nariadeniu o ochrane údajov, ktorého cieľom je pomáhať hlavným inštitúciám v EÚ pri dosahovaní správneho konsenzu o fungujúcom súbore pravidiel zameranom na budúcnosť, ktorým sa posilňujú práva a slobody jednotlivca. Podobne ako v stanovisku o mobilnom zdravotníctve zo začiatku roka 2015 sa v ňom rieši otázka ochrany údajov pri prechode na digitalizáciu, čiže tretieho cieľa stratégie EDPS, ktorým je prispôbenie existujúcich zásad ochrany údajov, aby vyhovovali globálnej digitálnej úrovni, a to aj v súvislosti s plánmi EÚ týkajúcimi sa jednotného digitálneho trhu. Je v súlade s prístupom pracovnej skupiny podľa článku 29 o aspektoch ochrany osobných údajov v oblasti používania nových technológií, ako je tzv. internet vecí, ku ktorému EDPS prispel ako riadny člen skupiny.



Dignity	Dôstojnosť
Future-oriented rules and enforcement	Súbor pravidiel a presadzovanie zamerané na budúcnosť
Accountable controllers	Zodpovední prevádzkovatelia
Empowered individuals	Oprávnené fyzické osoby
Innovative privacy engineering	Inovatívne inžinierstvo súkromia
Ethics	Etika

„Ľudská dôstojnosť je nedotknuteľná. Musí sa rešpektovať a ochraňovať.“

Článok 1, Charta základných práv EÚ

Základné právo na súkromie a ochranu osobných údajov je v súčasnosti dôležitejšie pre ochranu ľudskej dôstojnosti než kedykoľvek predtým. Je zakotvené v zmluvách EÚ a v Charte základných práv EÚ. Umožňujú jednotlivcom rozvíjať vlastné osobnosti, žiť nezávislý život, inovovať a uplatňovať iné práva a slobody. Zásady ochrany údajov vymedzené v charte EÚ – nevyhnutnosť, primeranosť, spravodlivosť, minimalizácia údajov, obmedzenie účelu, súhlas a transparentnosť – sa vzťahujú na spracúvanie údajov vo svojej úplnosti, na ich zber, ako aj používanie.

Technológia by nemala určovať hodnoty a práva, ale ani vzťah medzi nimi by nemal byť obmedzený na nesprávnu dichotómiu. Digitálna revolúcia sľubuje výhody pre zdravie, životné prostredie, medzinárodný rozvoj a hospodársku efektívnosť. V plánoch EÚ pre jednotný digitálny trh sa za kľúčové pre konkurencieschopnosť a rast považuje cloud computing, internet vecí, veľké dáta (big data) a iné technológie. V obchodných modeloch sa využívajú nové možnosti na hromadný zber, okamžitý prenos, spájanie a opätovné použitie osobných údajov na nepredvídané účely, ktoré sú odôvodnené dlhými a nepreniknuteľnými zásadami ochrany súkromia. Tým sa zásady ochrany údajov dostávajú pod nový tlak, ktorý si vyžaduje nové uvažovanie o spôsobe ich uplatňovania.

V dnešnom digitálnom prostredí nestačí dodržiavanie zákona. Musíme zvážiť etický rozmer spracúvania údajov. Regulačný rámec EÚ už poskytuje priestor na pružné rozhodnutia a ochranné opatrenia podľa individuálnych prípadov pri zaobchádzaní s osobnými informáciami. Reforma regulačného rámca bude dobrým krokom vpred. Existujú však hlbšie otázky týkajúce sa vplyvu trendov na spoločnosť založenej na údajoch v oblasti dôstojnosti, slobody jednotlivca a fungovania demokracie.

Tieto otázky majú technické, filozofické, právne a morálne dôsledky. V stanovisku sa upozorňuje na niekoľko zásadných trendov v technológii, ktoré môžu zahŕňať neprijateľné spracúvanie osobných informácií alebo môžu porušovať právo na súkromie. Zachytáva štvorúrovňový tzv. ekosystém ochrany veľkých dát ako odpoveď na digitálnu výzvu: kolektívne úsilie podporené etickými úvahami.

- (1) Regulovanie spracovania údajov zamerané na budúcnosť a rešpektovanie práv na súkromie a ochranu údajov.
- (2) Zodpovední prevádzkovatelia, ktorí určujú spracovanie osobných informácií.
- (3) Navrhovanie a vývoj produktov a služieb v oblasti spracovania údajov, v ktorých sa zohľadňuje súkromie.
- (4) Oprávnené fyzické osoby.

Európsky dozorný úradník pre ochranu údajov chce podnecovať otvorenú a informovanú diskusiu v EÚ a mimo nej so zapojením občianskej spoločnosti, pôvodcov, spoločností, akademikov, verejných orgánov a regulačných orgánov. Nová etická rada EÚ pre ochranu údajov, ktorú zriadime v rámci EDPS, prispeje k vymedzeniu novej digitálnej etiky umožňujúcej lepšie využívanie technológie pre spoločnosť a hospodárstvo spôsobmi, ktorými sa posilňujú práva a slobody fyzických osôb.

OBSAH

1. Údaje všade: Trendy, príležitosti a výzvy	6
1.1 VEĽKÉ DÁTA.....	6
1.2 INTERNET VECÍ.....	7
1.3 AMBIENTNÉ POČÍTAČOVÉ SLUŽBY.....	7
1.4 CLOUD COMPUTING	7
1.5 OBCHODNÉ MODELY ZÁVISLÉ OD OSOBNÝCH ÚDAJOV	8
1.6 DRONY A AUTONÓMNE VOZIDLÁ.....	8
1.7 TRENDY S POTENCIÁLNE VÄČŠÍM, DLHODOBEJŠÍM VPLYVOM.....	9
2. Ekosystém ochrany veľkých dát.....	9
2.1 REGULOVANIE ZAMERANÉ NA BUDÚCNOSŤ	10
2.2 ZODPOVEDNÍ PREVÁDZKOVATELIA	10
2.3 INŽINIERSTVO ZOHĽADŇUJÚCE SÚKROMIE.....	11
2.4 OPRÁVNENÉ FYZICKÉ OSOBY	11
<i>Prostredie výrobcu-spotrebiteľa</i>	<i>11</i>
<i>Súhlas.....</i>	<i>11</i>
<i>Kontrola a „vlastníctvo“ údajov</i>	<i>12</i>
3. Dôstojnosť ako ústredný prvok novej digitálnej etiky	12
3.1 DÔSTOJNOSŤ A ÚDAJE	12
3.2 EURÓPSKY PORADNÝ VÝBOR PRE ETIKU.....	14
4. Záver: Prišiel čas na hlbšie úvahy	14
Poznámky	16

1. Údaje všade: Trendy, príležitosti a výzvy

Zhromažďujú sa čoraz väčšie množstvá osobných informácií a spracúvajú sa čoraz neprehľadnejšími a zložitejšími spôsobmi. S postupným nástupom využívania počítačov v podnikaní a verejnej správe v 80. rokoch minulého storočia došlo k všeobecnému vnímaniu, že postupy silných vlád a korporácií v spracúvaní osobných údajov obmedzovali jednotlivcov do postavenia obyčajných dotknutých osôb, pričom obmedzovali základné práva a slobody. To, čím sa líši súčasná vlna integrovanej informačnej a komunikačnej technológie, je jej všadeprítomnosť a sila.

Minulý rok bolo zaznamenané, že na planéte bolo viac zapojených zariadení ako ľudí¹. Zvýšenia kapacity procesora², ukladania a šírky pásma prenosu znamená, že postupne existuje čoraz menej technických obmedzení v oblasti spracúvania osobných informácií. Očakáva sa, že internet vecí a analytika veľkých údajov sa spoja s umelou inteligenciou, spracúvaním prirodzeného jazyka a biometrickými systémami na spustenie aplikácií so schopnosťou strojov učiť sa v záujme pokrokovej inteligencie. Vlády a spoločnosti sú schopné posunúť sa nad rámec tzv. hĺbkovej analýzy údajov k tzv. hĺbkovej analýze reality, ktorá sa dotýka každodennej skúsenosti, komunikácie a dokonca myšlienky³. Ako sa spoločnosť prispôbuje požiadavkám digitálneho trhu, v súčasnosti sa obnovujú snahy o výučbu programovania malých detí⁴. Využívanie týchto trendov v odvetví, v ktorom je EÚ vedúcim spotrebiteľom, ale zaostáva v poskytovaní služieb, je opakujúcou sa témou v stratégii Komisie o jednotnom digitálnom trhu⁵.

Tieto trendy a mnohé z pojmov, ktoré sa dnes používajú, sú napriek ich aktuálnosti vágne a navzájom sa prekrývajú. S cieľom podnietiť debatu chceme zdôrazniť osobitné trendy, ktoré, hoci podľa nášho názoru určite nie sú vyčerpávajúce, ale nastoľujú dôležité etické a praktické otázky v oblasti uplatňovania zásad ochrany údajov.

1.1 Veľké dáta

Veľké dáta⁶ sa týkajú postupu spájania obrovských objemov informácií z rôznych zdrojov a ich analýzy, často s používaním adaptívnych algoritmov na tvorbu rozhodnutí. Tieto informácie nie sú vždy osobné: údaje generované senzormi na sledovanie prírodných alebo atmosférických javov, ako je počasie alebo znečistenie, alebo na sledovanie technických aspektov výrobných postupov, sa netýkajú „identifikovanej alebo identifikovateľnej fyzickej osoby“⁷. Jedna z najväčších hodnôt veľkých dát pre podniky a vlády však vyplýva zo sledovania ľudského správania, kolektívne a jednotlivo, a spočíva v jeho potenciáli predpovedať⁸.

Jedným výsledkom je vznik nového modelu výnosov pre internetové spoločnosti opierajúce sa o sledovanie online činnosti na optimalizovanie ekonomickej hodnoty transakcií pre poskytovateľov služieb, nielen v cielej reklame, ale aj v podmienkach a sadzbách poisťných zmlúv, úverov a iných zmluvných vzťahov. Na konkurenčnom trhu pre pozornosť používateľov si väčšina ľudí neuvedomuje široký rozsah tohto sledovania⁹. Tieto veľké dáta treba považovať za osobné aj v prípade uplatnenia postupov anonymizácie. Je čoraz jednoduchšie zasiahnúť do totožnosti osoby spojením údajne anonymných údajov s inými súbormi údajov vrátane verejne dostupných informácií, napríklad na sociálnych médiách¹⁰. Keď sa s týmito údajmi obchoduje osobitne cez hranice a jurisdikcie, zodpovednosť za spracovanie informácií sa stáva nejasnou a je zložité ju zistiť alebo presadiť na základe právnych predpisov o ochrane údajov, osobitne v prípade neexistencie medzinárodných štandardov.

1.2 Internet vecí

Mnohé zariadenia pripojené k internetu sú už spoločným miestom, ako sú smartfóny, tablety a stroje na vydávanie hotovosti a na registrácie na let. Očakáva sa, že do roku 2020 sa pripojenie stane štandardnou funkciou s pripojenými 25 miliardami objektov (v porovnaní so 4,8 miliardy v roku 2015) v rozsahu od telemedicíny po vozidlá, od inteligentných meračov po celú škálu nových stacionárnych a mobilných zariadení na umožnenie inteligentných miest¹¹.

Tieto senzory budú poskytovať okamžité a štruktúrované informácie, ku ktorým v súčasnosti štatistické úrady a prieskumy nemajú prístup, ale ktoré už nevyhnutne nemusia byť presné a môžu byť prípadne zavádzajúce¹². Odhadovaných 1,8 miliardy spojení medzi automobilmi do roku 2022 by mohlo znížiť počet nehôd a znečistenie, zvýšiť produktivitu a samostatnosť starších ľudí a zdravotne postihnutých¹³. Veci nositeľné na tele, ako je oblečenie a hodinky, budú spracúvať osobné informácie ako iné pripojené zariadenia. Budú schopné zistiť krvné zrazeniny a sledovať kondíciu a liečenie rán; pripojené tkaniny by mohli chrániť proti extrémnym prostrediam, napríklad v boji proti požiarom. Tieto zariadenia budú zasielať osobné údaje priamo do ukladania v cloude, budú spojené so sociálnymi sieťami a prípadne verejne šírené s umožnením identifikácie používateľov a zaznamenávaním správania a pohybov jednotlivcov a davov¹⁴.

To, ako sa zaobchádza s týmito informáciami, by mohlo mať vplyv na súkromie nielen používateľov zariadení vrátane prípadu používania na pracovisku, ale aj na práva iných, ktorí sú pozorovaní a zaznamenaní zariadením. Existuje síce málo dôkazov o skutočnej diskriminácii, ale je jasné, že obrovský objem osobných informácií zhromažďovaných internetom vecí je predmetom veľkého záujmu ako prostriedok na maximalizovanie výnosov personalizovanejšou tvorbou cien podľa zaznamenaného správania, najmä v odvetví zdravotného poistenia¹⁵. Spochybnené budú aj osobitné pravidlá v iných oblastiach, napríklad v prípadoch, keď zariadenia zahŕňajúce spracovanie zdravotných údajov nemajú byť technicky zaradené ako zdravotné pomôcky a nebudú patriť do rozsahu pôsobnosti regulácie¹⁶.

1.3 Ambientné počítačové služby

Ambientné alebo neviditeľné počítačové služby sa týkajú kľúčovej technológie, ktorá je podkladom tzv. internetu vecí. Jedným z ich najjasnejších použití sú tzv. inteligentné domovy a inteligentné kancelárie skladajúce sa zo zariadení so vstavanou sofistikovanou schopnosťou spracúvania informácií, ktoré sľubujú väčšiu energetickú účinnosť a informovanejších jednotlivcov schopných ovplyvňovať svoju spotrebu na diaľku (aj keď by to záviselo od nezávislosti rezidenta od prenajímateľa alebo správcu budovy). Bude potrebné objasniť, kto je zodpovedný za účel a prostriedky spracovania osobných údajov obsiahnutých v zariadeniach ambientných počítačových služieb, nielen na účel ochrany základných práv jednotlivcov, ale aj na účel primeraného pridelenia zodpovednosti za zaistenie rešpektovania bezpečnostných požiadaviek na celkový systém.

1.4 Cloud computing

Termín cloud computing je známy ako ústredná podporná technológia pre pokročilé schopnosti analyzovania a získavania údajov, zberu a analyzovania veľkých dát a tok údajov z internetu vecí, ktoré v súčasnosti používa približne pätina jednotlivcov a podnikov v EÚ¹⁷.

Umožňuje koncentráciu údajov z nespočetného množstva zariadení internetu vecí a opiera sa o dostupnosť a pripojenie enormných objemov údajov vo veľkých zariadeniach na uchovávanie a spracovanie po celom svete¹⁸. Odhaduje sa, že všeobecnejšie prijatie cloud computingu¹⁹ súkromným a verejným sektorom môže prispieť celkovo 449 miliardami EUR k HDP EÚ28 (0,71 % celkového HDP EÚ).

O kontrolu nad osobnými informáciami sa často delí spotrebiteľ a poskytovateľ služby cloudu a zodpovednosť za povinnosti týkajúce sa ochrany údajov nie je vždy jasná. Mohlo by to znamenať, že sa v praxi poskytuje nedostatočná ochrana. Tieto povinnosti existujú bez ohľadu na **fyzické umiestnenie ukladania údajov**. Okrem toho, aj keď ide len o technológiu na pozadí, ktorá podporuje podnikové aplikácie, infraštruktúra cloud computingu samotná sa môže stať kritickou infraštruktúrou a zvýšiť nerovnováhy v trhovej sile, pričom 30 % podnikov nedávno oznámilo ťažkosti v odhlásení sa alebo zmene poskytovateľov²⁰.

1.5 Obchodné modely závislé od osobných údajov

Tieto technológie umožnili vznik nových obchodných modelov, ktoré sa opierajú o informácie nielen generované z poskytovania služieb, ale aj z iných zdrojov, ako je prítomnosť na sociálnych médiách, na účel posúdenia rizika a úverovej bonity a maximalizovanie výnosov. Prevládajúci obchodný model dneška je zastúpený platformami, ktoré spájajú predávajúcich a kupujúcich a umožňujú výmenu a redistribúciu výrobkov, služieb, zručností a aktív. Často sa označujú ako zdieľaná ekonomika, spoluspotrebiteľstvo alebo online a mobilné peer-to-peer (rovný s rovným) obchodné platformy,²¹ pričom tieto platformy môžu ponúkať klasické ekonomické výhody, zvýšiť konkurencieschopnosť na trhoch a znížiť objem odpadu. Odhaduje sa, že ich svetová hodnota v nadchádzajúcich rokoch štvornásobne vzrastie z 26 miliárd USD na 110 miliárd USD²². Tieto obchodné modely založené na údajoch už generujú enormné príjmy v oblasti spoločného používania aut a prenájmov obytných nehnuteľností a vo finančnej technológii a sociálnom požíčovaní. Prieskumy naznačujú, že spotrebiteľia oceňujú ich zrejmu väčšiu cenovú dostupnosť a pohodlie²³.

Menou týchto platforiem je zvyčajne povest' používateľa, partnerské hodnotenia a overovanie totožnosti. Možno to potenciálne vnímať ako zvyšovanie transparentnosti a zodpovednosti, nie však nevyhnutne vo vzťahu k samotnému poskytovateľovi platformy. Veľkí hráči na týchto trhoch boli kritizovaní za údajné zadržiavanie údajov o povesti pred veľmi individuálnymi používateľmi, ktorých sa informácie týkajú. Existuje obrovské riziko, že jednotlivci by mohli byť zo služieb vylúčení na základe povesti založenej na nepresných údajoch, ktoré nemôžu spochybníť ani požiadať o ich vymazanie. Opieranie sa o údaje z viacerých zdrojov takisto spochybňuje zásadu práva EÚ týkajúcu sa minimalizácie údajov. Rozsah budúceho vplyvu týchto a budúcich technologických obchodných modelov na jednotlivcov a spoločnosti si zaslúži dôkladné zváženie²⁴.

1.6 Drony a autonómne vozidlá

Drony, alebo poloautonómne lietadlá v súčasnosti slúžia hlavne na vojenské účely, ale čoraz viac sa používajú na účely sledovania, mapovania, dopravy, logistiky a verejnej bezpečnosti, ako je hasenie lesných požiarov²⁵. Fotografie, videá a iné osobné údaje zbierané dronmi sa dajú vymieňať prostredníctvom telekomunikačných sietí. Ich používaním sa riskuje vážny zásah do súkromia a majú odrádzajúci účinok na slobodu prejavu. Vzniká otázka, ako sa dá ich návrh a používanie účinne regulovať tak, aby dotknuté osoby mohli uplatňovať svoje práva na prístup k údajom zachyteným týmito strojmi.

Na zemi autonómne vozidlá alebo autá bez šoféra zmenia spôsob používania a organizácie individuálnej dopravy a môžu prekryť rozdiel medzi súkromnou a verejnou dopravou. Odhaduje sa, že v roku 2035 bude 12 miliónov plne autonómnych a 18 miliónov čiastočne autonómnych vozidiel, pričom Európa bude patriť k ich prvým používateľom²⁶. Algoritmy riadiace autá budú spravovať rozhodnutia, ktoré sa môžu priamo týkať fyzickej integrity a dokonca života alebo smrti jednotlivcov, napríklad vo výbere naprogramovanom v prípade nárazu, ktorému sa nedá zabrániť. Popri zrejmej potrebe mať jasno v tom, kto je zodpovedný za kontrolu údajov a bezpečnosť údajov, nastoľujú tieto aplikácie rad etických otázok.

1.7 Trendy s potenciálne väčším, dlhodobejším vplyvom

3D biotlač organických predmetov, ktorá používa kópie buniek pacientov a kolagénové biologické bandáže (to znamená citlivé údaje podľa práva EÚ) na uloženie následných radov živých buniek, sa podľa odhadov čoskoro stane ľahko dostupnou²⁷. Uľahčí poskytovanie prispôbených ľudských anatomických častí a bude osobitne cenná v chudobnejších oblastiach sveta a v oblastiach po konfliktoch. Biotlač vyvoláva zrejme otázky pre lekársku etiku, ochranu duševného vlastníctva a ochranu spotrebiteľa, zároveň však, keďže sa opiera o spracovanie intímnych a citlivých údajov o zdraví jednotlivcov, pre uplatňovanie pravidiel ochrany údajov.

Umelá inteligencia, ako robotika, sa týka technickej požiadavky na autonómne stroje, a to stojace aj mobilné. Ich pokrok poskytne nesmierny potenciál presahujúci ich súčasné uplatnenie. Hĺbkovo sa učiace počítače sa naučia úlohy spracúvaním veľkých súborov údajov s použitím (okrem iných vecí) neurónových sietí, ktoré sa javia ako napodobňujúce mozog. Cieľom výskumných pracovníkov a spoločností je zlepšiť vzdelávanie bez dohľadu. Algoritmy už dokážu rozumieť jazykom a prekladať ich, spoznávať obrázky, písať novinové články a analyzovať lekárske údaje²⁸. Sociálne médiá poskytujú obrovské množstvá osobných informácií účinne vopred označených samotnými jednotlivcami. Toto môže byť posledný bod v rade kognitívnych zlepšení na zvýšenie schopnosti ľudského mozgu, ako papier alebo počítač, alebo integrované do autonómnych strojov, robotov, ale teraz je okamih, keď je potrebné zvážiť širšie následky pre jednotlivcov a spoločnosť²⁹.

2. Ekosystém ochrany veľkých dát

EÚ má teraz príležitosť prevziať vedúcu úlohu a ukázať, ako môžu vlády, regulačné orgány, prevádzkovatelia, návrhári, vývojári a jednotlivci lepšie spolupracovať s cieľom posilniť práva a riadiť technologickú inováciu, nie ju blokovať. Trendy opísané v druhom oddiele podľa jedného komentátora „prehĺbili rozdiely medzi tým, čo je možné, a tým, čo je zo zákona povolené“³⁰. Na rozdiel od niektorých tvrdení je ochrana súkromia a údajov platformou pre udržateľné a dynamické digitálne prostredie, nie prekážkou. Nezávislé orgány pre ochranu údajov, ako je EDPS, zohrávajú kľúčovú úlohu pri vyvracaní takýchto mýtov a reagujú na skutočné obavy jednotlivcov týkajúce sa straty kontroly nad svojimi osobnými informáciami³¹.

Ďalšia generácia osobných údajov bude zrejme ešte menej dostupná jednotlivcom, ktorých sa týka. Zodpovednosť za formovanie udržateľného jednotného digitálneho trhu je nevyhnutne rozptýlená, ale aj vzájomne závislá, ako ekosystém, pretože vyžaduje účinnú interakciu medzi vývojármi, podnikmi a regulačnými orgánmi v záujme jednotlivca. V tejto časti poukážeme na prínos, ktorý môžu mať tieto štyri základné subjekty.

2.1 Regulovanie zamerané na budúcnosť

Nedávno sme vyzvali EÚ, aby sa chopila svojej historickej príležitosti a zaviedla jednoduchšie pravidlá pre spracovanie osobných údajov, ktoré zostanú relevantné pre celú generáciu³². Rokovania o všeobecnom nariadení o ochrane údajov a smernici o ochrane údajov v sektoroch polície a spravodlivosti sú v poslednej fáze, a čoskoro sa pozornosť zameria na budúcnosť smernice o elektronickom súkromí o elektronických komunikáciách a na nové nariadenie o tom, ako samotné inštitúcie a orgány EÚ spracúvajú osobné údaje. Aj keď sú hospodárske náklady na zhromažďovanie a ukladanie údajov takmer zanedbateľné, orgány na ochranu údajov budú musieť tieto pravidlá dôsledne presadzovať, aby sa predišlo „morálnemu riziku“ nadmerného spracovania údajov³³.

Stratégia jednotného digitálneho trhu uznáva prepojenie medzi kontrolou veľkých objemov dát a silou trhu. Súhlasí s presvedčením vyjadreným v našom predbežnom stanovisku z roku 2014 s názvom Súkromie a konkurencieschopnosť vo veku veľkých dát o potrebe väčšej súdržnosti medzi regulačnými orgánmi. EÚ už disponuje nástrojmi na nápravu nerovnováhy síl na digitálnom trhu: napríklad prebiehajúce antitrustové konania Európskej komisie sú uznaním prevahy mobilných zariadení, pokiaľ ide o prístup na internet. Väčšmi holistické presadzovanie je možné v rámci existujúceho právneho rámca, napríklad prostredníctvom strediska EÚ na výmenu informácií pre orgány dohľadu s cieľom zväziť, či jednotlivé prípady môžu vyvolať otázky týkajúce sa dodržiavania pravidiel hospodárskej súťaže, ochrany spotrebiteľa a údajov. Napríklad:

- požadovanie väčšej transparentnosti cien – v hotovosti alebo inak – za službu môže informovať a uľahčiť analýzu prípadov hospodárskej súťaže³⁴, a
- detekcia nespravodlivej cenovej diskriminácie na základe nedostatočnej kvality údajov a nespravodlivého profilovania a korelácií³⁵.

Užší dialóg medzi regulačnými orgánmi z rôznych odvetví by mohol viesť k reakcii na rastúce výzvy pre globálne partnerstvo, ktoré môže vytvoriť „systém“ otvorených dát, do ktorého môžu prúdiť údaje a myšlienky, ako sú štatistiky a mapy, a kde môžu byť dostupné a vymieňané vo verejnom záujme s menším rizikom dohľadu, s cieľom poskytnúť jednotlivcom väčší vplyv na rozhodnutia, ktoré sa ich týkajú³⁶.

2.2 Zodpovední prevádzkovatelia

Zodpovednosť si vyžaduje zavedenie vnútorných politík a systémov kontroly, ktoré zabezpečia súlad a poskytnú relevantné dôkazy najmä nezávislým orgánom dohľadu.

Argumentovali sme za odstránenie byrokracie v zákone o ochrane údajov tým, že sa minimalizujú požiadavky na zbytočnú dokumentáciu s cieľom maximalizovať priestor pre ďalšie zodpovedné iniciatívy zo strany podnikov, doplnené o usmernenie od orgánov na ochranu údajov. Zásada, že osobné údaje by mali byť spracované iba spôsobom, ktorý je zlučiteľný s konkrétnym účelom (-mi), na ktorý (-é) boli zhromaždené, je nevyhnutná na rešpektovanie legitímnych očakávaní jednotlivcov. Napríklad kódexy správania, audity, osvedčenia, kontroly a nová generácia zmluvných doložiek a záväzné podnikové pravidlá môžu pomôcť pri vytvorení silnej dôvery v digitálny trh. Osoby zodpovedné za spracovanie osobných informácií by mali byť oveľa dynamickejšie a aktívnejšie a mali by upustiť od tzv. tendencie „čiernej skrinky“ tajomstiev a netransparentnosti obchodných praktík a súčasne vyžadovať ešte väčšiu transparentnosť zákazníkov³⁷.

2.3 Inžinierstvo zohľadňujúce súkromie

Ľudská inovácia bola vždy produktom činností konkrétnych sociálnych skupín a osobitných kontextov, ktoré zvyčajne odrážajú spoločenské normy času³⁸. Rozhodnutia o technologickom dizajne by nemali diktovať naše spoločenské interakcie a štruktúru našich komunit, ale mali byť skôr podporovať naše hodnoty a základné práva.

EÚ by mala vyvíjať a podporovať inžinierske postupy a metodiky, ktoré umožňujú uplatňovať technológie na spracovanie údajov s cieľom plne rešpektovať dôstojnosť a práva jednotlivca. Systémoví a softvéroví inžinieri musia chápať a lepšie uplatňovať zásady ochrany súkromia už v štádiu návrhu v nových produktoch a službách vo všetkých fázach dizajnu a technológiách. Zodpovednosť musí byť podporovaná lepším výskumom a vývojom metód a nástrojov na zabezpečenie presných auditov a na stanovenie dodržiavania pravidiel zo strany prevádzkovateľov a spracovateľov, napríklad „označovaním“ každej jednotky osobných údajov „metadátami“, ktoré opisujú požiadavky na ochranu údajov.

Inžinierske riešenia by mali posilniť postavenie jednotlivcov, ktorí si chcú zachovať súkromie a slobodu prostredníctvom anonymity. EÚ by mala podporovať návrh a implementáciu algoritmov, ktoré skrývajú identity a súhrnné údaje s cieľom chrániť jednotlivca pri súčasnom využití prediktívnej sily dát³⁹.

Dnes musíme položiť základy pre riešenie týchto úloh tým, že vývojárov a odborníkov na ochranu údajov z rôznych oblastí prepojíme v rámci rozsiahlych sietí, ako je Sieť pre spravovanie súkromia na internete (IPEN), ktoré prispievajú k plodnej interdisciplinárnej výmene myšlienok a prístupov.

2.4 Oprávnené fyzické osoby

Prostredie výrobcu-spotrebiteľa

Jednotlivci nie sú len pasívnymi objektmi, ktoré vyžadujú ochranu zákona pred využívaním. Vyššie opísané digitálne trendy predstavujú pozitívne príležitosti na posilnenie úlohy jednotlivca. Napríklad ľudia v súčasnosti produkujú a spotrebúvajú obsah a služby, a v čoraz väčšej miere možno usudzovať, že sú spoločne s poskytovateľmi služieb zodpovední za spracovanie osobných údajov, pokiaľ neslúži výlučne na účely „domácnosti“⁴⁰ (pojem „výrobca-spotrebiteľ“ vznikol s cieľom opísať tento vývoj⁴¹). Virtuálne meny medzitým ponúkajú používateľom anonymitu a obchádzanie overovania transakcií treťou stranou, a tým aj nižšie náklady na transakcie pri cezhraničnej platbe za tovary a služby. Na druhej strane, anonymita a medzijurisdikčná (alebo, ako by sa mohlo tvrdiť, *mimojurisdikčná*) povaha týchto virtuálnych mien spôsobuje, že jednotlivci sú zraniteľní voči podvodom a kriminálnym trhom, ktoré sa iba ťažko odhaľujú a prešetrujú. Okrem povinností regulačných orgánov, podnikov a inžinierov majú aj občania zodpovednosť byť upovedomení, ostrážení, kritickí a informovaní pri rozhodovaní online, ako aj offline⁴².

Súhlas

Okrem toho, na rozdiel od tradičného myslenia nemožno každé ľudské správanie vysvetliť ekonomickými zásadami, ktoré predpokladajú, že ľudia sú úplne racionálni a citliví voči ekonomickým stimulom⁴³. Je to relevantné pre budúcu úlohu súhlasu jednotlivca so spracovaním jeho osobných informácií. Podľa právnych predpisov EÚ nie je súhlas jediným legitímnym základom pre väčšinu spracovania. Dokonca aj tam, kde súhlas zohráva dôležitú

úlohu, to prevádzkovateľov nezabavuje zodpovednosti za to, ako nakladajú s údajmi, najmä vtedy, ak získali všeobecný súhlas so spracovaním na širokú škálu účelov.

Kontrola a „vlastníctvo“ údajov

Jednotlivci musia mať možnosť spochybníť chyby a nespravodlivé odchýlky vyplývajúce z logiky používanej algoritmami na určenie predpokladov a predpovedí. Na ilustráciu, v štúdiu uskutočnenej v USA na takmer 3 000 úverových správach patriacich 1 000 spotrebiteľom sa zistilo, že 26 % obsahovalo nedostatky týkajúce sa „vecných“ chýb, ktoré boli dosť závažné na to, aby ovplyvnili úverové skóre spotrebiteľov a tým aj náklady na získanie úveru⁴⁴.

Údaje sú často považované za zdroj, ako je ropa, s ktorým sa obchoduje, v ideálnom prípade s rovnako dobre informovanými účastníkmi transakcie⁴⁵. Zákazníci nedostávajú spravodlivú náhradu za svoje osobné informácie, s ktorými sa obchoduje, pričom niektorí argumentovali v prospech modelu vlastníctva údajov. Absolútnu kontrolu nad osobnými údajmi však možno len ťažko zaručiť – sú tu aj iné obavy, napríklad verejný záujem a práva a slobody ostatných. Kontrola je potrebná, ale nie dostatočná⁴⁶. Ľudská dôstojnosť je vždy nemenná, a podľa právnych predpisov EÚ nemožno analógiu vlastníctva používať ako takú na osobné informácie, ktoré majú skutočné prepojenie na jednotlivé osobnosti. V právnych predpisoch EÚ o ochrane údajov neexistuje žiadne ustanovenie o tom, že jednotlivci sa musia vzdať tohto základného práva.

Jednou alternatívnou metódou, ktorá jednotlivcom poskytne lepšiu kontrolu nad svojimi údajmi, kto k nim môže mať prístup a na aký účel, by mohlo byť používanie úložisk osobných údajov alebo „ dátových trezorov“⁴⁷. Koncepcia takéhoto „osobného úložiska“ vyžaduje bezpečnostné mechanizmy, ktoré zabezpečia, že k údajom môžu mať prístup iba subjekty, ktoré oprávnila dotknutá osoba, a iba k tým častiam, na ktoré majú oprávnenie. Úložiská osobných údajov budú najúčinnnejšie, keď sa budú týkať aktuálnych a priebežne aktualizovaných informácií, ako sú geopriestorové údaje alebo známky života. Okrem technických záruk by používatelia údajov boli povinní dodržiavať pravidlá týkajúce sa výmeny a používania údajov. Hospodárska súťaž a možnosť zmeniť službu, ktorú človek používa, je jedinou najúčinnnejšou možnosťou spotrebiteľov, ako ovplyvňovať trh služieb, ktoré majú k dispozícii. Zabezpečenie prenosnosti prepojení vrátane identifikátorov a kontaktných informácií, sa preukázalo ako účinný nástroj hospodárskej súťaže, ktorý po liberalizácii telekomunikačného trhu viedol k efektívnemu zníženiu cien pre spotrebiteľov. Prenosnosť údajov, t. j. vecná a praktická možnosť prenášať väčšinu vlastných údajov jednotlivca od jedného poskytovateľa služby k inému, je účinným východiskom pre vytvorenie podmienok pre skutočnú možnosť voľby spotrebiteľov.

3. Dôstojnosť ako ústredný prvok novej digitálnej etiky

Etický rámec musí podporiť základné prvky tohto digitálneho ekosystému. Európsky dozorný úradník pre ochranu údajov sa domnieva, že lepšie dodržiavanie a zabezpečenie ľudskej dôstojnosti by mohlo byť protiváhou všadeprítomného sledovania a asymetrie moci, ktorým čelí jednotlivec. Mali by predstavovať ústredný prvok novej digitálnej etiky.

3.1 Dôstojnosť a údaje

V dôsledku priemyselnej revolúcie v 18. a 19. storočí sa hnutie za ľudské práva snažilo zabezpečiť väčšiu spoločenskú prosperitu odstránením prekážok v súvislosti s rešpektovaním jednotlivca. EÚ v súčasnosti na základe Charty základných práv a nadväzujúcej Všeobecnej

deklarácie ľudských práv a Európskeho dohovoru o ľudských právach prijalo za svoje východisko nedotknuteľnosť ľudskej dôstojnosti. Dôstojnosť človeka nie je len základným právom ako takým, ale aj základom pre nadväzujúce slobody a práva vrátane práv na súkromie a ochranu osobných údajov⁴⁸. Porušovanie dôstojnosti môže zahŕňať patriť objektivizáciu, keď sa s osobou zaobchádza ako s nástrojom, ktorý slúži účelom inej osoby⁴⁹. Súkromie je neoddeliteľnou súčasťou ľudskej dôstojnosti a právo na ochranu údajov bolo pôvodne sformulované v 70. a 80. rokoch minulého storočia ako spôsob na kompenzovanie potenciálu narušenia súkromia a dôstojnosti prostredníctvom rozsiahleho spracovania osobných údajov. V Nemecku bolo právo na „informačné sebaurčenie“ založené na práve na osobnú dôstojnosť a práve na slobodný rozvoj osobnosti, stanovené v článkoch 1 a 2 nemeckej ústavy⁵⁰.

Začiatkom 21. storočia však jednotlivci stále častejšie žiadali zverejniť oveľa viac osobných informácií cez internet na účely účasti v sociálnych, administratívnych a obchodných záležitostiach, s čoraz väčším obmedzeným priestorom pre odstúpenie. Keďže všetky aktivity prebiehajú potenciálne vždy online, pojem slobodného a informovaného súhlasu je pod obrovským tlakom. Každú chvíľu sa vkladajú a kombinujú „digitálne odrobinky“ s cieľom zaradiť jednotlivcov v reálnom čase s cieľom vytvorenia viacnásobných a niekedy protichodných profilov. Tieto profily môžu byť rozosielené v mikrosekundách bez vedomia jednotlivcov a používané ako základ pre dôležité rozhodnutia, ktoré sa ich týkajú.

Profily používané na predpovedanie stigmatizácie rizikového správania ľudí, posilnenie existujúcich stereotypov, sociálnej a kultúrnej segregácie a vylúčenia⁵¹ s takouto „kolektívnou inteligenciou“ vyvracajú individuálnu voľbu a rovnaké príležitosti. Takéto „filtrácie bubliny“ alebo „osobné dozvukové komory“ by mohli viesť k utlmeniu samotnej kreativity, inovácie a slobody prejavu a združovania, ktoré umožnili rozkvet digitálnych technológií.

Medzitým pretrvávajúci výnimočný stav z dôvodu „bezpečnosti“ sa používa na ospravedlnenie viacnásobného vrstvenia dotieravých techník na monitorovanie činnosti jednotlivcov⁵². Pochopenie tohto nárastu dohľadu si vyžaduje dlhodobjšiu perspektívu o celkovom vplyve na spoločnosť a správanie.

EÚ musí spolu s tretími krajinami tvrdo dohliadať na to, akým spôsobom zabezpečí tieto hodnoty tak, aby neboli dodržiavané iba na papieri, zatiaľ čo v skutočnosti sú v kybernetickom priestore neutralizované. EÚ je najmä teraz, pred hromadným prijatím týchto technológií, kriticky otvorená zavedeniu hodnôt do digitálnych štruktúr, ktoré budú definovať našu spoločnosť⁵³. V tejto súvislosti je potrebné nové posúdenie, či potenciálne výhody nových technológií skutočne závisia od zhromažďovania a analýzy osobne identifikovateľných informácií miliárd jednotlivcov. Takéto posúdenie by mohlo podnietiť vývojárov, aby navrhli produkty, ktoré v reálnom čase odosobnia obrovské objemy neorganizovaných informácií, čím sťažia alebo znemožnia vyčlenenie jednotlivca.

Už sme uznali, že určité spracovanie údajov, napríklad genetických údajov, musí byť nielen regulované, ale aj predmetom vyhodnotenia širších obáv spoločnosti, napríklad etických výborov. Genetické údaje sa vo svojej podstate netýkajú iba jednej osoby, ale aj jej predkov a potomkov. Genetické údaje slúžia nielen na identifikáciu rodinných vzťahov, ale prvky nájdené v génoch jednej osoby môžu poskytnúť informácie aj o jej rodičoch a deťoch, a môžu viesť k tomu, že prevádzkovatelia prijímú rozhodnutia, ktoré ovplyvnia ich šance na život ešte pred ich narodením. Potenciálna koncentrácia osobných genetických údajov v rukách niekoľkých obrovských hráčov na trhu má dosah na trhové ekonomiky, ako aj na

dotknuté osoby. Z dôvodu rastúcej závislosti od globálneho systému zhromažďovania a analýzy konštantného toku dát by spoločnosť a hospodárstvo mohli byť zraniteľnejšie voči bezprecedentným bezpečnostným nedostatkom a škodlivým útokom.

Existujúci rámec by mohol zlyhať, ak k budúcnosti nebudeme pristupovať s inovatívnym myslením. Prevláda čoraz väčší dopyt a potreba považovať dotknutú osobu za jednotlivca, a nie jednoducho za spotrebiteľa alebo používateľa. Skutočne nezávislé orgány na ochranu údajov zohrávajú kľúčovú úlohu v prevencii budúcnosti, v ktorej sú jednotlivci určovaní algoritmi a ich neustálymi variáciami. Musia byť vybavené tak, aby plnili „povinnosť starostlivosti“ voči jednotlivcom a ich dôstojnosti online. Tradičné pojmy a zásady ochrany súkromia a údajov sú už obsiahnuté v etických nuansách na ochranu dôstojnosti, ako sú zamestnanosť a zdravie. Dnešné trendy však začali písať celkom novú kapitolu, a je potrebné preskúmať, či sú tieto zásady dostatočne silné pre digitálny vek⁵⁴. Je pravdepodobné, že samotný pojem osobných údajov sa radikálne zmení, keďže technológia jednotlivcom čoraz viac umožňuje znovu sa identifikovať z údajne anonymných dát. Okrem toho, strojové učenie a zlúčenie ľudskej a umelej inteligencie ohrozí poňatie práv a zodpovednosti jednotlivca.

3.2 Európsky poradný výbor pre etiku

Účelom nie je vykreslenie alarmujúceho obrazu dystopie. V právnej, politickej, ekonomickej, sociálnej, vedeckej a dokonca v náboženskej sfére už prebiehajú diskusie⁵⁵. Zjednodušujúce postupy, ktoré poskytujú jednostrannú výhodu pre ekonomický zisk alebo sledovanie bezpečnosti, už pravdepodobne nie sú o nič užitočnejšie než nadmerne reštriktívne uplatňovanie existujúcich zákonov, ktoré brzdia inováciu a pokrok. Európsky dozorný úradník pre ochranu údajov preto navrhuje dôkladnú, rozsiahlu a multidisciplinárnu analýzu, ktorá poskytne odporúčania a informuje spoločenskú diskusiu o tom, ako by slobodná, demokratická spoločnosť mala riešiť technologické problémy.

Stratégia EDPS⁵⁶ je venovaná rozvoju etického prístupu k ochrane údajov, v rámci ktorého sa uznalo, že „uskutočiteľné, užitočné a ziskové sa nerovná udržateľné“, a v ktorej bola zdôraznená „zodpovednosť za mechanický súlad s literou zákona“. Naším úmyslom je osloviť komunitu významných osobností mimo úradníkov, právnikov a IT odborníkov EÚ, ktoré sú schopné posúdiť strednodobý až dlhodobý vplyv technologických zmien a regulačných reakcií. V nadchádzajúcich mesiacoch zriadime v našej nezávislej inštitúcii externú poradnú skupinu pre etický rozmer ochrany údajov, aby preskúmala vzťahy medzi ľudskými právami, technológiou, trhmi a obchodnými modelmi v 21. storočí.

Náš poradný výbor pre etiku bude zložený z vybranej skupiny významných osobností z oblasti etiky a filozofie, sociológie, psychológie, technológie a ekonomiky, a v prípade potreby ho podporia ďalší odborníci s odbornými znalosťami a skúsenosťami v oblastiach, ako sú zdravotníctvo, doprava a energetika, sociálna interakcia a médiá, hospodárstvo a financie, správa vecí verejných a demokracia, a bezpečnosť a kontrola. Budú vyzvaní, aby zvážili širšie etické dôsledky spôsobu uchopenia a používania osobných údajov, pričom ich rokovania budú maximálne transparentné.

4. Záver: Prišiel čas na hlbšie úvahy

Ochrana súkromia a údajov je súčasťou riešenia, nie problému. Momentálne technológiu kontrolujú ľudia. Nie je jednoduché jednoznačne určiť, že tento možný vývoj je dobrý alebo zlý, priaznivý alebo nepriaznivý, pokrovový alebo škodlivý, a to o to menej, ak sa má niekoľko možných trendov vnímať v súvislostiach. Politickí činitelia, technologickí vývojoví

pracovníci, obchodní vývojoví pracovníci a my všeci musíme zodpovedne zvážiť, či a ako chceme ovplyvňovať vývoj technológie a jej uplatňovanie. Rovnako dôležité však je, aby EÚ naliehavo zvážila etiku a miesto pre ľudskú dôstojnosť v technológiách budúcnosti.

Zásady ochrany údajov sa preukázali ako schopné chrániť fyzické osoby a ich súkromie pred rizikami nezodpovedného spracovania údajov. Súčasný trendy však môžu vyžadovať úplne nový prístup. Otvárame preto novú debatu o tom, v akom rozsahu stačí uplatňovanie zásad, ako je spravodlivosť a legitímnosť. Spoločenstvo ochrany údajov môže plniť novú úlohu s použitím existujúcich nástrojov, ako sú predbežné kontroly a povolenia – pretože žiadne iné orgány nie sú vybavené na kontrolovanie tohto spracúvania údajov. Pritom ako sa technológia, svetové inovácie a prepojenosť ľudí vyvíjajú závratnou rýchlosťou, máme príležitosť upriamiť pozornosť, vyvolať záujem a dosiahnuť konsenzus.

Dúfame, že týmto stanoviskom zabezpečíme rámec pre širšiu a hlbšiu diskusiu o tom, ako môže EÚ zaistiť integritu svojich hodnôt a zároveň prijať výhody nových technológií.

V Bruseli 11. septembra 2015

(podpísaný)

Giovanni BUTTARELLI
európsky dozorný úradník pre ochranu údajov

Poznámky

¹ Zdroj: Spravodajské informácie GSMA.

² Moorov zákon, že počet tranzistorov, ktoré môžu byť umiestnené na mikročip, sa zdvojnásobí každých 18 mesiacov, sa preukázal ako všeobecne presný, Moore, Gordon E. (1965-04-19). Cramming more components onto integrated circuits, Electronics. 22. augusta 2011

³ Nathan Eagle, Alex (Sandy) Pentland, Reality mining: sensing complex social systems, Journal Personal and Ubiquitous Computing, ročník 10 číslo 4, marec 2006, strany 255 – 268. Shoshana Zuboff v Big Other: surveillance capitalism and the prospects of an information civilization, Journal of Information Technology (2015) 30, strany 75 – 89, píše: „V dôsledku všadeprítomnej počítačovej mediácie je takmer každý aspekt sveta zaradený v novom symbolickom rozmere, ako podujatia, objekty, procesy a ľudia sa stávajú viditeľnými, poznateľnými a zdieľateľnými novým spôsobom.“ Zuboff predvída „vzostup novej univerzálnej architektúry“, ktorú nazýva „Big Other“, „všadeprítomný režim zosieťovaných inštitúcií, ktorý zaznamenáva, upravuje a spoluupravuje každodenné skúsenosti od hriankovačov po telá, komunikáciu po myšlienky, a to všetko s cieľom vytvoriť nové cesty k speňaženiu a zisku“, strany 77, 81.

⁴ BBC Micro Bit computer's final design revealed 7. júla 2015, [http://www.bbc.com/news/technology-33409311\(10.09.2015\)](http://www.bbc.com/news/technology-33409311(10.09.2015)); No assembler required: How to teach computer science in nursery school, The Economist, 1. augusta 2015.

⁵ Žiadna z desiatich najväčších spoločností v odvetví technológií na základe trhovej kapitalizácie nemá sídlo v EÚ (osem je spoločností v USA, jedna v Číne a na Taiwane) podľa aktualizácie rebríčka z 31. marca 2015 spoločnosti PWC Desať najväčších svetových spoločností podľa trhovej kapitalizácie.

⁶ „Veľké dáta sa týkajú exponenciálneho rastu dostupnosti, ako aj automatického používania informácií: týkajú sa obrovských digitálnych súborov údajov, ktoré majú podniky, vlády a iné veľké organizácie, pričom sa potom rozsiahlo analyzujú (odtiaľ meno: analytika) s použitím počítačových algoritmov“; pracovná skupina 29 stanovisko 3/2013 o obmedzení účelu. V správe Bieleho domu z roku 2014 boli veľké dáta opísané ako: „Rastúca technologická schopnosť zachytiť, zhrnúť a spracovať stále väčší objem, rýchlosť a rozmanitosť údajov.“ Pozri Big Data: Seizing Opportunities, Preserving Values, výkonný úrad prezidenta (tzv. správa Podesta), máj 2014.

⁷ Podľa práva EÚ sú „osobné údaje“ vymedzené ako akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby („dotknutej osoby“): identifikovateľná osoba je osoba, ktorú možno identifikovať priamo alebo nepriamo, najmä odkazom na identifikačné číslo alebo jeden alebo viaceré faktory špecifikujúce jej fyzickú, fyziologickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu; článok 2 písm. a) smernice 95/46/ES. Toto vymedzenie je zhruba porovnateľné s vymedzeniami prijatými Radou Európy v Dohovore o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov (známom ako dohovor 108) a v Usmerneniach OECD o ochrane súkromia a cezhraničných tokoch osobných údajov. Na účely hĺbkovej analýzy pozri článok 20 stanoviska pracovnej skupiny 4/2007 o koncepcii osobných údajov, pracovná skupina 136.

⁸ Pozri napríklad prejav predsedníčky Federálnej obchodnej komisie USA v roku 2014: „Šírenie spojených zariadení, prudko klesajúce náklady na zber, uchovávanie a spracovanie informácií a schopnosť sprostredkovateľov údajov a iných spájať údaje offline a online znamená, že spoločnosti môžu zhromažďovať v podstate neobmedzené množstvá údajov o spotrebiteľoch a uchovávať ich na natrvalo. S používaním prediktívnej analýzy sa z toho môžu o každom z nás dozvedieť prekvapujúce množstvo informácií.“ Úvodné poznámky predsedníčky Federálnej obchodnej komisy, Edith Ramirezovej, Big Data: A Tool for Inclusion or Exclusion?, Washington, DC, 15. septembra 2014. Podľa Sandy Pentlandovej: „Sociálna fyzika je kvantitatívno-sociálna veda, ktorá opisuje matematické súvislosti medzi informáciami a tokom myšlienok na jednej strane a ľudským správaním na druhej strane... umožňuje nám predvídať produktivitu malých skupín, oddelení v spoločnostiach a

dokonca celých miest“. To „je to, čo treba na vybudovanie lepších sociálnych systémov“ (strany 4, 7) a aby sa „umožnilo (štátnym úradníkom, priemyselným manažérom a občanom) využívať nástroje stimulov sociálnych sietí na stanovenie nových noriem správania (s. 189) (naša kurzíva); Pentland, *Social Physics: How Good Ideas Spread: The Lessons from a New Science*.

⁹ Osobitný prieskum Eurobarometer 431 o ochrane údajov, jún 2015 and prieskum Pewovej výskumnej skupiny 2014 o verejnom vnímaní súkromia a bezpečnosti v ére po Snowdenovi. Priemerná návšteva na jednu webovú lokalitu znamená podľa jednej štúdie 56 prípadov zberu údajov podľa Julie Angwinovej a jej diela *Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance*, 2012). V správe Bieleho domu o veľkých dátach z roku 2014 sa uvádza, že „nevídaná počítačová sila a sofistikácia... vytvárajú asymetriu moci medzi tými, ktorí majú údaje, a tými, ktorí ich zámerne alebo neúmyselne poskytujú“, „niektoré z najzásadnejších výziev odhalených v tomto preskúmaní sa týkajú toho, ako môže analýza veľkých dát... vytvoriť také neprehľadné prostredie rozhodovania, že sa samostatnosť jednotlivca stratí v nepreniknuteľnom súbore algoritmov“.

¹⁰ S použitím verejných anonymných údajov zo sčítania z roku 1990 by bolo 87 % obyvateľov USA pravdepodobne identifikovaných na základe ich päťmiestneho PSČ v spojení s rodom a dátumom narodenia; pozri 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, apríl 2011. DNA je jedinečné (s výnimkou identických dvojčiat) a stabilné počas celého života. Obsahuje informácie o etnickej príslušnosti, predispozície na choroby a môže identifikovať ostatných rodinných príslušníkov. V januári 2013 boli výskumní pracovníci schopní identifikovať jednotlivcov a rodiny z anonymných údajov o DNA z verejne dostupných genealogických databáz; M., McGuire, A. L., Golan, D., Halperin, E. & Erlich, Y. *Science* 339, 321–324 (2013). Pozri tiež Poorly anonymized logs reveal NYC cab drivers' detailed whereabouts, 23.06.2014 <http://arstechnica.com/tech-policy/2014/06/poorly-anonymized-logs-reveal-nyc-cab-drivers-detailed-whereabouts/> (10.09.2015). Pozri tiež stanovisko pracovnej skupiny 29 č. 04/2007 o koncepcii osobných údajov, stanovisko pracovnej skupiny 29 č. 03/2013 o obmedzení účelu, stanovisko pracovnej skupiny 29 č. 06/2013 o otvorených údajoch a opätovnom používaní informácií verejného sektora a stanovisko pracovnej skupiny 29 č. 05/2014 o anonymizácii.

¹¹ Zdroj: Gartner.

¹² Pozri napríklad moderovanú diskusiu What is the future of official statistics in the Big Data era? Kráľovská štatistická spoločnosť, Londýn, 19. januára 2015; <http://www.odi.org/events/4068-future-official-statistics-big-data-era> (10.09.2015).

¹³ Desať technológií, ktoré by mohli zmeniť naše životy: možné vplyvy a politické dôsledky, Útvar pre vedeckú prognostiku, Výskumná služba Európskeho parlamentu, január 2015.

¹⁴ Pracovný program EÚ Horizont 2020 na roky 2016 – 2017 podporuje tento vývoj vrátane rozsiahlych pilotných projektov, ktoré budú zamerané na problematiku súkromia a etiky.

¹⁵ Poistenie bolo opísané ako „vlastný podnikateľský model pre internet vecí“; From fitness trackers to drones, how the ‘Internet of Things’ is transforming the insurance industry, *Business Insider* 11. júna 2015. Pojem cenovej diskriminácie v práve o hospodárskej súťaži odvodený z článku 102 ZFEÚ, ktorým sa zakazuje podniku s významným postavením na trhu „priame alebo nepriame vynucovanie neprímeraných nákupných alebo predajných cien alebo iných obchodných podmienok“, je veľmi sporné, pozri napríklad Damien Gerardin a Nicolas Petit Price Discrimination Under EC Competition Law: Another Antitrust Theory in Search of Limiting Principles (júl 2005), *Global Competition Law Centre Working Paper* súbor č. 07/05. Vo veci veľkých dát a ich (podľa autorov ešte nerealizovaného) potenciálu posilniť personalizovanú tvorbu cien pozri Výkonný úrad prezidenta Spojených štátov, Big Data and Differential Pricing, február 2015 a nedávnu analýzu, v ktorej sa dospelo k záveru, že personalizovaná tvorba cien všeobecne znamená spracovanie osobných údajov, a preto musí rešpektovať zásadu transparentnosti zo zákona o ochrane údajov, ktorou sa od spoločností vyžaduje, aby informovali ľudí o účele spracovania ich osobných údajov: spoločnosti to musia uviesť, ak

personalizujú ceny. A ak spoločnosť používa súbor cookie na spoznanie niekoho, v smernici o elektronickom súkromí sa vyžaduje, aby spoločnosť informovala osobu o účele súboru cookie“, pracovný návrh Frederika Borgesiusa, Online Price Discrimination and Data Protection Law. Nachádza sa na adrese http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2652665 (10.09.2015).

¹⁶ Zdravotnícke pomôcky sú vymedzené v práve EÚ v smernici Rady 93/42/EHS o zdravotníckych pomôckach zmenenej a doplnenej smernicou Európskeho parlamentu a Rady 2007/47/ES z 5. septembra 2007. O dôsledkoch tzv. mobilného zdravotníctva na ochranu údajov pozri stanovisko EDPS 1/2015.

¹⁷ Podľa Eurostatu používa služby ukladania v cloude 21 % jednotlivcov a 19 % podnikov v EÚ.

¹⁸ „Ak by svetový internet bola krajina, bola by 12. najväčším spotrebiteľom elektriny na svete, niekde medzi Španielskom a Talianskom. Predstavuje to približne 1,1 až 1,5 percenta svetovej spotreby elektriny (v roku 2010) a skleníkové plyny vyprodukované ročne 70 až 90 veľkými (500 megawatt) uhoľnými elektrárnami.“ Natural Resources Defense Council, Data Centre Efficiency Assessment: Scaling Up Energy Efficiency Across the Data Centre Industry: Evaluating Key Drivers and Barriers 2014.

¹⁹ Správa štúdie SMART 2013/0043 - Uptake of Cloud in Europe.

²⁰ Zdroj: Eurostat.

²¹ Pojem zdieľanej ekonomiky bol kritizovaný ako zavádzajúci: 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 Future of Privacy Forum, „User Reputation: Building Trust and Addressing Privacy Issues in the Sharing Economy, jún 2015.

²⁴ Pozri seminár z 9. júna 2015 Federálnej obchodnej komisie USA na tému Hospodárska súťaž, ochrana spotrebiteľa a ekonomické otázky vyvolané zdieľanou ekonomikou, <https://www.ftc.gov/news-events/events-calendar/2015/06/sharing-economy-issues-facing-platforms-participants-regulators/> (10.09.2015).

²⁵ Vo veci dôsledkov dronov alebo systémov diaľkovo pilotovaných lietadiel na ochranu údajov pozri stanovisko EDPS k oznámeniu Komisie Európskemu parlamentu a Rade – Nová éra letectva – Otvorenie trhu leteckej dopravy pre bezpečné a udržateľné používanie systémov diaľkovo pilotovaných lietadiel na civilné účely, november 2014.

²⁶ Zdroj: Boston Consulting Group.

²⁷ Gartner.

²⁸ Algoritmus na spoznanie tváre Facebook DeepFace zaznamenal 97 % úspech, čím prekonal ľudí, DeepFace: Closing the Gap to Human-Level Performance in Face Verification, uverejnené v správe na konferencii IEEE o počítačovom rozpoznávaní vizuálov a vzorov v júni 2014.

²⁹ Robo bol vymedzený ako „stroj umiestnený vo svete, ktorý cíti, myslí a koná“, Bekey, G, Current trends in robotics: technology and ethics, v Robot Ethics - The ethical and social implications of robotics, The MIT Press, 2012, s. 18. Odhaduje sa, že v rokoch 2013 až 2016 sa predá 22 miliónov služobných robotov; správa IRF o svetovej robotike, 2013. Na tému umelá inteligencia pozri Rise of the Machines, Economist, 9. 5. 2015 a Pew Research Centre Internet Project 2014. Spoločnosť na umelú inteligenciu uskutočnila akvizíciu prostredníctvom poprednej technologickej spoločnosti v roku 2014 pod podmienkou vytvorenia etickej a bezpečnostnej rady a zákazu používania umelej inteligencie na vojenské alebo spravodajské účely; Forbes, Inside Google's Mysterious Ethics Board, 3. 2. 2014.

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

³¹ Pozri poznámku pod čiarou 9. Pentland *Social Physics* s.153: „Možné sú veľké pokroky v oblasti zdravotníctva, dopravy, energetiky a bezpečnosti... hlavnými prekážkami v dosiahnutí týchto cieľov sú obavy zo straty súkromia a skutočnosť, že sme doteraz nedosiahli žiadny konsenzus medzi osobnými a sociálnymi hodnotami“. Diskusia o pandémie eboly v západnej Afrike v roku 2014 poukazuje na to, ako vznikla táto falošná dichotómia medzi súkromím jednotlivca a potrebami spoločnosti. Choroby sa zvyknú sledovať a ich životnosť sa meria pomocou prieskumov a sčítaní, ktoré rýchlo zastarávajú a v prípade ktorých sa ťažko odhaduje, kde najbližšie udrú. Existuje niekoľko príkladov používania „veľkých dát“ na sledovanie ohnísk malárie v Namíbii a Keni, a v roku 2009 na sledovanie účinnosti zdravotných varovaní vlády počas krízy mexickej prasacej chrípky. Jedným zdrojom údajov sú záznamy volaní z mobilných telefónov, ktoré zobrazujú základňu, cez ktorú prešiel hovor, a v reálnom čase môžu poskytnúť hrubý odhad lokalizácie ľudí a ich smerovanie. Zhromažďovanie všetkých týchto záznamov nie je cieleňé – nemožno rozlišovať medzi ľuďmi s ebolou a ľuďmi bez eboly. Švédska nezisková organizácia mapovala mobilitu obyvateľstva v západnej Afrike, ale tieto údaje neboli použité, pretože mobilní operátori ich neposkytli externým výskumným pracovníkom, pričom tvrdili, že na to potrebujú pokyny od vlády, ktorá zase vyslovila obavy zo straty súkromia, ktoré by podľa právnych predpisov EÚ nebolo zaručené; <http://www.pri.org/stories/2014-10-24/how-big-data-could-help-stop-spread-ebola>. (10.09.2015)

³² Stanovisko EDPS 3/2015.

³³ Predpoklad veľkých dát, že „N=všetky“, znamená, že na všetky informačné miesta sa nemá nazeráť iba ako na vzorku, Viktor Mayer-Schönberger a Kenneth Cukier, *The Rise of Big Data: How it's changing the way we think about the world*, 2013. Lisabonská rada a Inštitút progresívnej politiky tvrdili, že blahobyt sa zvýši maximalizovaním „digitálnej hustoty“ – „množstva údajov použitých na obyvateľa v rámci hospodárstva“ <http://www.lisboncouncil.net/component/downloads/?id=1178> (10.09.2015). Medzinárodná pracovná skupina pre ochranu údajov v telekomunikáciách (známa ako „Berlínska skupina“) navrhla odchýlky od zásad ochrany údajov pre veľké dáta; http://www.datenschutz-berlin.de/attachments/1052/WP_Big_Data_final_clean_675.48.12.pdf. (10.09.2015). Svetové ekonomické fórum žiadalo zamerať sa na použitie a nie na zhromažďovanie a na upustenie od požiadavky udelenia súhlasu so zberom osobných údajov; *Unlocking the Value of Personal Data: From Collection to Usage*, 2013.

³⁴ Pozri predbežné stanovisko EDPS o súkromí a konkurencieschopnosti vo veku veľkých dát.

³⁵ V článku 21 Charty základných práv je zakázaná „akákoľvek diskriminácia z akéhokoľvek dôvodu ako napr. pohlavie, rasa, farba pleti, etnický alebo sociálny pôvod, genetické charakteristiky, jazyk, náboženstvo alebo viera, politický alebo iný názor, príslušnosť k národnostnej menšine, majetok, narodenie, postihnutie, vek alebo sexuálna orientácia“. Mnohé z týchto kategórií údajov („odhaľujúce rasový alebo etnický pôvod, politické názory, náboženské alebo filozofické presvedčenie alebo členstvo v odboroch a spracovanie údajov týkajúcich sa zdravia alebo sexuálneho života“) majú zvýšenú ochranu podľa článku 8 smernice 95/46/ES.

³⁶ K myšlienke digitálneho systému pozri *Ambition numérique: Pour une politique française et européenne de la transition numérique*, Francúzska digitálna rada, jún 2015, s. 276; Bruce Schrier obhajuje vytvorenie „nevlastných verejných priestorov“ na internete, ako sú verejné parky, *Data and Goliath*, s. 188 – 189; Sandy Pentland žiada o „verejné dátové systémy“, *Social Physics*, s. 179. Vo veci posúdenia bezpečnosti uverejňovania súhrnných súborov dát ako otvorených dáta, pozri stanovisko 06/2013 pracovnej skupiny 29 o otvorených dátach a opätovnom využívaní informácií verejného sektora.

³⁷ „Während die Einzelnen immer transparenter werden, agieren viele Unternehmen hochgradig intransparent“ <http://crackedlabs.org/studie-kommerzielle-ueberwachung/info>. Vo veci kvalifikovanej transparentnosti pozri napr. Frank Pasquale: *The Black Box Society: The Secret Algorithms that Control Money and Information*.

³⁸ Behind the technology that affects social relations lie the very same social relations, David Noble, *Social Choice in Machine Design: The Case of Automatically Controlled Machine Tools*, v *Case*

Studies in the Labor Process, ed. Andrew Zimbalist, 1979. Pozri tiež Judy Wacjman, *Pressed for Time: The Acceleration of Life in Digital Capitalism*, 2014, s. 89 – 90; a Zuboff, Big Other (citované v poznámke pod čiarou 3).

³⁹ Stanovisko 05/2014 o technikách anonymizácie, prijaté 10. apríla 2014 (pracovná skupina 216.)

⁴⁰ Vo veci reštriktívnej výnimky z pravidiel o ochrane údajov na čisto osobné účely alebo účely domácností, pozri rozsudok Súdneho dvora EÚ vo veci C-212/13 *František Ryneš/Úrad pro ochranu osobních údajů*.

⁴¹ Pojem výrobca-spotrebiteľ vytvoril Alvin Toffler v *The Third Wave*, 1980. Vo veci diskusie o „prostredí výrobca-spotrebiteľ“ a spôsobe jej regulovania, pozri Ian Brown a Chris Marsden, *Regulating Code*, 2013.

⁴² Stanovisko Európskej skupiny pre etiku vo vede a nových technológiách pre Európsku komisiu: Ethics of Security and Surveillance Technologies, stanovisko č. 28, 20.05.2015, s. 74.

⁴³ Pozri napríklad Homer Economicus: The Simpsons and Economics, ed. Joshua Hall, 2014.

⁴⁴ Pri najkonzervatívnejšej definícii chyby to znamená, že spotrebiteľské správy 23 miliónov Američanov obsahujú vecné chyby. V prípade 5 % účastníkov štúdie boli tieto chyby raz opravené a ich úverové skóre sa zlepšilo natoľko, že mohli získať úver za nižšiu cenu; Federálna obchodná komisia, správa kongresu podľa oddielu 319 zákona o spravodlivých a presných úverových transakciách z roku 2003, december 2012; Chris Jay Hoofnagle, How the Fair Credit Reporting Act Regulates Big Data (10. septembra 2013). Future of Privacy Forum Workshop on Big Data and Privacy: Making Ends Meet, 2013. K dispozícii na SSRN: <http://ssrn.com/abstract=2432955>.

⁴⁵ WEF považuje údaje za cenný majetok jednotlivca, ktorého práva na vlastníctvo, používanie a likvidáciu môžu byť poskytnuté spoločnostiam a vládam výmenou za služby. Pozri nedávne prejavy, aj prejav podpredsedu Komisie Ansipa, napríklad zo dňa 7.9.2015 na výročnej schôdzi v Bruegel s názvom Produktivita, inovácia a digitalizácia – ktoré sú globálne politické výzvy?: Vlastníctvo a riadenie dátových tokov, používanie a opätovné využívanie údajov. Správa a ukladanie údajov. Podporujú významné rozvíjajúce sa odvetvia, ako sú cloud computing, internet vecí a veľké dáta.

⁴⁶ Tak kto má právo používať informácie a údaje, ktoré skutočne nepatria sebe samému? Je to problém, ktorý prekračuje hranice obchodu, etiky a morálky, čo vedie k otázkam týkajúcim sa súkromia a ochrany súkromia; Al-Khouri, november 2012, http://www.academia.edu/6726887/Data_Owner

[ship Who Owns My Data 036](http://www.academia.edu/6726887/Data_Owner). Pozri tiež Margaret Jane Radin, Incomplete Commodification in the Computerized World, v *The Commodification of Information* 3, 17, Niva Elkin-Koren & Neil Weinstock Netanel eds. 2002: „Je veľký rozdiel, či sa súkromie vníma ako ľudské právo, ktoré majú všetky osoby na základe svojej osobnosti, alebo ako vlastnícke právo, niečo, čo môžu osoby vlastniť a kontrolovať. Ľudské práva sú pravdepodobne trhovu nescudziteľné, zatiaľ čo vlastnícke práva sú pravdepodobne trhovu scudziteľné“.

⁴⁷ Cieľom projektu MIT Computer Science and Artificial Intelligence Lab's Crosscloud, ktorý podporilo niekoľko spoločností so sídlom v EÚ, je „1) zjednodušiť rozvoj („sociálneho“) softvéru pre viacerých používateľov, ktorý využíva iba vývoj klientskej časti webového rozhrania a rešpektuje práva a súkromie používateľov, a 2) poskytnúť používateľom slobodu jednoduchého pohybu medzi aplikáciami, hardvérovými platformami a sociálnymi sieťami pri uchovaní ich údajov a sociálnych väzieb“; <http://openpds.media.mit.edu/#architecture> (10.09.2015).

⁴⁸ Pozri vysvetlenie k článku 1 Charty základných práv.

⁴⁹ Martha Nussbaum, Objectification, in *Philosophy and Public Affairs* 24, 4, 1995.

⁵⁰ Rozsudok z 15. decembra 1983, BVerfGE 65, 1-71, Volkszählung.

⁵¹ Pozri Európsku skupinu pre etiku vo vede a nových technológiách, stanovisko o etike a dohľade, s. 75. Zo štúdie vyplynulo, že algoritmus zameriavania na reklamy bol diskriminačný, pričom muži v

priemere vyhľadávali opakujúce sa reklamy na lepšie platené pracovné miesta a ženy navštevovali stránky ponúkajúce pracovné miesta; Carnegie Mellon University a International Computer Science Institute. Vo veci tendencie uprednostňovania v predvolenom nastavení digitálnych asistentov ženský hlas, pozri napríklad Judy Wajcman, *Feminist theories of technology*. *Cambridge Journal of Economics*, 34 (1). s. 143 – 152, 2010.

⁵² Giorgio Agamben, *State of Exemption*, 2005.

⁵³ Neil Richards, Neil a Jonathan King, *Big Data Ethics* (19. mája 2014), *Wake Forest Law Review*, 2014.

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

⁵⁵ Pozri list od organizácie Future of Life Institute. Pápežská encyklika *Laudato Si'*: „K tomu pristupuje dynamika médií a digitálneho sveta, ktorý, ako je všadeprítomný, nepodporuje rozvoj schopnosti múdro žiť, hlbavo premýšľať a veľkodušne milovať. Veľkým mudrcom minulosti by v tomto kontexte hrozilo, že zbadajú svoju múdrosť, ako sa dusí uprostred rozvratného hluku informácií. Vyžaduje si to od nás snahu, aby tieto prostriedky prispievali k novému kultúrnemu vývoju ľudstva, a nie k úbytku jeho najhlbšieho bohatstva. Pravú múdrosť, plod reflexie, dialógu a veľkodušného stretnutia medzi ľuďmi nemožno dosiahnuť iba akumuláciou údajov, ktoré zahlcujú a mätú na spôsob mentálneho znečistenia. Reálne vzťahy s druhými a všetko, čo so sebou prinášajú, zároveň majú tendenciu k tomu, aby sa nahradili typom komunikácie sprostredkovanej internetom. To umožňuje selekciu či elimináciu vzťahov podľa našej ľubovôle, čím nezriedka vzniká nový typ umelých emócií, ktoré sa viažu skôr k prístrojom a obrazovkám než k ľuďom a k prírode. Súčasné prostriedky umožňujú, aby sme vzájomne komunikovali, vymieňali si poznatky a pocity. Niekedy nám však tiež bránia nadviazať priamy kontakt s úzkosťou, chvením a radosťou druhého a so zložitou jeho osobnou skúsenosťou. Preto by nemala udivovať skutočnosť, že dotieravú ponuku týchto produktov sprevádza hlboké a melancholické neuspokojenie v medziľudských vzťahoch či škodlivá osamelosť“.

⁵⁶ Pozri Akciu 4 stratégie EDPS 2015 – 2020, rozvoj etického rozmeru ochrany údajov.