

EUROPEAN DATA PROTECTION SUPERVISOR

## Mišljenje 4/2015

# Prema novoj digitalnoj etici

*Podaci, dostojanstvo i tehnologija*



11. rujna 2015.

*Europski nadzornik za zaštitu podataka (EDPS) neovisna je institucija EU-a, nadležna na temelju članka 41. stavka 2. Uredbe 45/2001 „za poslove obrade osobnih podataka... osiguranje da institucije i tijela Zajednice poštuju temeljna prava i slobode fizičkih osoba, a posebno njihovo pravo na privatnost” i „...za savjetovanje institucija i tijela Zajednice te subjekata podataka o svim pitanjima koja se tiču obrade osobnih podataka”. Imenovan je u prosincu 2014. zajedno s pomoćnikom nadzornika, s naglaskom na konstruktivnijem i proaktivnijem radu. EDPS je u ožujku 2015. godine objavio petogodišnju strategiju u kojoj se navodi namjera provedbe tog zadatka kao i odgovornost za njegovo izvršenje.*

*Ovo mišljenje nastavak je prethodnog mišljenja EDPS-a o Općoj uredbi o zaštiti podataka kojemu je cilj bio pomoći glavnim institucijama EU-a u postizanju pravog konsenzusa o realnom skupu pravila, orijentiranom prema budućnosti, koji potiče prava i slobode pojedinca. Kao i mišljenje o mobilnom zdravstvu početkom 2015. godine, ovo se mišljenje odnosi na izazov da zaštita podataka „prijeđe na digitalni oblik”, što je treći cilj EDPS-ove strategije „prilagođavanje postojećih načela zaštite podataka, kako bi se uklopili u globalno digitalno tržište”, također i u sklopu planova EU-a za jedinstveno digitalno tržište. Mišljenje je u skladu s pristupom radne skupine iz članka 29. o aspektima zaštite podataka u vezi s uporabom novih tehnologija, poput „interneta stvari” kojemu je EDPS pridonio kao punopravni član grupe.*



Dignity	Dostojanstvo
Future-oriented rules and enforcement	Pravila i provođenje orijentirani prema budućnosti
Accountable controllers	Odgovorni nadzornici
Empowered individuals	Ovlašteni pojedinci
Innovative privacy engineering	Inovativno projektiranje privatnosti
Ethics	Etika

**„Ljudsko je dostojanstvo nepovredivo. Ono se mora poštovati i štiti.“**

### **Članak 1. Povelje EU-a o temeljnim pravima**

**Temeljna prava na privatnost i zaštitu osobnih podataka postala su važnija za zaštitu ljudskog dostojanstva nego ikada prije.** Ona su sadržana u ugovorima EU-a te u Povelji EU-a o temeljnim pravima. Ta prava pojedincima omogućavaju razvoj svoje vlastite osobnosti, samostalan život, te stvaranje i ostvarivanje drugih prava i slobode. Načela zaštite podataka definirana u Povelji EU-a – nužnost, razmjernost, pravednost, minimizacija podataka, ograničenje namjene, pristanak i transparentnost – u cijelosti se primjenjuju na obradu, prikupljanja i uporabu podataka.

**Tehnologija ne bi trebala diktirati vrijednosti i prava, ali se ni njihov odnos ne bi trebao svesti na lažnu dihotomiju.** Digitalna revolucija obećava pogodnosti za zdravlje, okoliš, međunarodni razvoj i gospodarsku učinkovitost. Prema planovima EU-a za jedinstveno digitalno tržište, računalstvo u oblaku, „internet stvari“, veliki podaci i ostale tehnologije smatraju se ključem konkurentnosti i rasta. Poslovni modeli iskorištavaju nove mogućnosti za masivno prikupljanje, trenutačni prijenos, kombiniranje i ponovnu uporabu osobnih podataka u nepredviđene svrhe, te ih opravdavaju duga i nedostupna pravila o privatnosti. To je ponovno opteretilo načela zaštite podataka, zbog čega je potrebno ponovo razmisliti o njihovoj primjeni.

**U današnjem digitalnom okruženju poštovanje zakona nije dovoljno; moramo uzeti u obzir etičku dimenziju obrade podataka.** Regulatorni okvir EU-a već omogućuje prostor za fleksibilne, pojedinačne odluke i zaštitne mjere pri obradi osobnih podataka. Reforma regulatornog okvira bit će dobar korak naprijed. Međutim, postoje dublja pitanja koja se tiču utjecaja trendova u društvu koje se temelji na podacima, koja se odnose na dostojanstvo, slobodu pojedinca i funkcioniranje demokracije.

**Ta pitanja imaju inženjerske, filozofske, pravne i moralne implikacije.** U ovom se mišljenju naglašava neke velike tehnološke trendove koji mogu uključivati neprihvatljivu obradu osobnih podataka ili mogu ometati pravo na privatnost. Mišljenje prikazuje četverostupanjski „ekosustav zaštite velikih podataka“ kao odgovor na digitalni izazov: kolektivni napor, koji se temelji na etičkim razmatranjima.

- (1) Reguliranje obrade podataka orijentirano prema budućnosti i poštivanje prava na privatnost i zaštitu podataka.
- (2) Odgovorni voditelji obrade koji određuju obradu osobnih podataka.
- (3) Inženjering koji poštuje privatnosti te dizajniranje proizvoda i usluga za obradu podataka.
- (4) Ovlašteni pojedinci.

**Europski nadzornik za zaštitu podataka želi potaknuti otvorenu i informiranu raspravu unutar i izvan EU-a,** koja uključuje civilno društvo, kreatore, tvrtke, akademike, javna tijela i regulatorna tijela. Novi odbor EU-a za etiku zaštite podataka koji ćemo osnovati u EDPS-u pomoći će definirati novu digitalnu etiku, čime će se moći bolje ostvariti pogodnosti tehnologije za društvo i gospodarstvo na načine koji jačaju prava i slobode pojedinaca.

## SADRŽAJ

<b>1. Podaci su svugdje: trendovi, prilike i izazovi .....</b>	<b>6</b>
1.1 VELIKI PODACI ( <i>BIG DATA</i> ).....	6
1.2 „INTERNET STVARI” .....	7
1.3 AMBIJENTALNO RAČUNALSTVO .....	7
1.4 RAČUNALSTVO U OBLAKU.....	7
1.5 POSLOVNI MODELI OVISNI O OSOBNIM PODACIMA .....	8
1.6 BESPILOTNE LETJELICE I AUTONOMNA VOZILA.....	8
1.7 TRENDOVI S POTENCIJALNO VEĆIM, DUGOROČNIJIM UČINKOM .....	9
<b>2. Ekosustav zaštite velikih podataka.....</b>	<b>9</b>
2.1 PROPISI USMJERENI NA BUDUĆNOST .....	9
2.2 ODGOVORNI NADZORNICI .....	10
2.3 INŽENJERING USMJEREN NA PRIVATNOST .....	10
2.4 OVLAŠTENI POJEDINCI .....	11
<i>Protrošačko (prosumer) okruženje .....</i>	<i>11</i>
<i>Pristanak.....</i>	<i>11</i>
<i>Kontrola i „vlasništvo” nad podacima .....</i>	<i>11</i>
<b>3. Dostojanstvo u samoj srži nove digitalne etike .....</b>	<b>12</b>
3.1 DOSTOJANSTVO I PODACI.....	12
3.2 EUROPSKI ETIČKI SAVJETODAVNI ODBOR .....	14
<b>4. Zaključak: Vrijeme je za produbljivanje rasprave .....</b>	<b>14</b>
<b>Napomene.....</b>	<b>16</b>

## 1. Podaci su svugdje: trendovi, prilike i izazovi

Prikupljaju se sve veće količine osobnih podataka i obrađuju na sve netransparentnije i složenije načine. Osim sve veće primjene računala u tvrtkama i javnim upravama u 80-ima, bilo je rašireno i shvaćanje da su prakse moćnih vlada i korporacija u obradi osobnih podataka dovodile pojedince do statusa pukih subjekata podataka, ugrožavajući tako temeljna prava i slobode. Ono što razlikuje trenutačni val integrirane informacijske i komunikacijske tehnologije njegova je sveprisutnost i moć.

Prošle je godine objavljeno da je na planetu bilo više povezanih uređaja nego ljudi<sup>1</sup>. Povećanje kapaciteta procesora<sup>2</sup>, skladištenje i širina prijenosnog kanala znače da ima sve manje tehničkih ograničenja za obradu osobnih podataka. Očekuje se da „Internet stvari” (*Internet of Things*) i analize velikih podataka konvergiraju s umjetnom inteligencijom, obradom prirodnog jezika i biometrijskim sustavima zbog čega aplikacije dobivaju mogućnost strojnog učenja radi razvoja napredne inteligencije. Vlade i poduzeća u mogućnosti su prijeći iz „rudarenja podataka” (*data mining*) u „rudarenje stvarnosti” (*reality mining*) koje prodiere u svakodnevno iskustvo, komunikaciju pa čak i misli<sup>3</sup>. Kako se društvo prilagođava zahtjevima digitalnog tržišta, sada postoje novi naponi da se djeca uče programiranju<sup>4</sup>. Iskorištavanje ovih trendova u sektoru u kojem je EU vodeći potrošač, ali kaska u pružanju usluga, tema je koja se ponavlja u Strategiji jedinstvenog digitalnog tržišta Europske komisije<sup>5</sup>.

Ovi trendovi i mnogi od pojmova koji se upotrebljavaju i danas, unatoč svojoj učestalosti, nejasni su, a značenja im se preklapaju. Da bismo potaknuli raspravu, želimo istaknuti određene trendove koji, iako očito nisu iscrpni, prema našem mišljenju postavljaju najvažnija etička i praktična pitanja za primjenu načela zaštite podataka.

### 1.1 Veliki podaci (*Big data*)

Veliki podaci<sup>6</sup> odnose se na praksu kombiniranja i analiziranja ogromnih količina informacija iz različitih izvora, često koristeći algoritme koji se samostalno uče za donošenje informiranih odluka. Ovi podaci nisu uvijek osobni: podaci dobiveni sensorima za praćenje prirodnih ili atmosferskih pojava poput vremenskih prilika ili onečišćenja, odnosno za nadzor tehničkih aspekata proizvodnog procesa ne odnose se na „identificiranu fizičku osobu ili onu čiji se identitet može utvrditi”<sup>7</sup>. No, jedna od najvećih vrijednosti velikih podataka za poduzeća i vlade proizlazi iz praćenja *ljudskog* ponašanja, kolektivno i pojedinačno, a nalazi se u njihovom potencijalu za predviđanje<sup>8</sup>.

Jedan od rezultata pojava je modela prihoda za internetska poduzeća koja se oslanjaju na praćenje online aktivnosti radi optimizacije ekonomske vrijednosti transakcija pružateljima usluga, ne samo u ciljanom oglašavanju, već i u uvjetima i cijenama polica osiguranja, kreditima i drugim ugovornim odnosima. Na konkurentnom tržištu za pažnju korisnika većina ljudi nije svjesna koliko je rašireno ovo praćenje<sup>9</sup>. Takvi „veliki podaci” trebaju se smatrati osobnima čak i tamo gdje su primijenjene tehnike anonimizacije: postaje sve lakše saznati identitet osobe kombiniranjem navodno „anonimnih” podataka s pomoću drugih baza podataka, uključujući javno dostupne informacije, primjerice na društvenim medijima<sup>10</sup>. Kada se trguje podacima osobito preko granice i nadležnosti, odgovornosti za obradu podataka postaju nejasne i teško ih je utvrditi ili provesti prema zakonu o zaštiti podataka, osobito u nedostatku bilo kakvih međunarodnih standarda.

## 1.2 „Internet stvari”

Mnogi uređaji povezani preko interneta postali su već uobičajena pojava, poput pametnih telefona, tableta i strojeva za izdavanje gotovine i prijavu za let. Predviđa se da će do 2020. povezivanje postati standardna značajka, s 25 milijardi povezanih objekata (u usporedbi s 4,8 milijardi u 2015. godini), obuhvaćajući sve od telemedicine do vozila, od pametnih brojila do cijelog niza novih stacionarnih i mobilnih uređaja koji će stvoriti pametne gradove<sup>11</sup>.

Ovi će senzori pružiti trenutne i detaljne informacije do kojih statistički uredi i istraživanja ne mogu doći danas, ali koje nisu nužno točnije, a potencijalno mogu čak i navoditi na pogrešan zaključak<sup>12</sup>. Procijenjenih 1,8 milijardi automobilskih veza stroja-sa-strojem (*machine-to-machine*) mogao bi do 2022. smanjiti broj nesreća i onečišćenja, povećati produktivnost i samostalnost starijih osoba te osoba s invaliditetom<sup>13</sup>. „Nosive stvari” (*wearables*), poput odjeće i satova obrađivat će osobne podatke poput drugih spojenih uređaja. Moći će otkrivati krvne ugruške i pratiti tjelesnu kondiciju te zacjeljivanje rana; povezane tkanine mogle bi štiti od ekstremnih uvjeta, primjerice prilikom suzbijanja požara. Ti će uređaji učitavati osobne podatke izravno u oblak za pohranu povezan s društvenim mrežama i potencijalno ih javno emitirati čime će se omogućiti identifikacija korisnika i praćenje ponašanja te kretanja pojedinaca i gomila<sup>14</sup>.

Način na koji se postupa s ovim informacijama mogao bi utjecati ne samo na privatnost korisnika uređaja, uključujući kada se upotrebljavaju na radnom mjestu, već i na prava drugih koje uređaj uoči i snimi. Iako postoji malo dokaza o stvarnoj diskriminaciji, jasno je da je ogromna količina osobnih podataka koju prikupi „Internet stvari” od velikog interesa kao sredstvo za maksimiziranje prihoda putem personaliziranog određivanja cijena prema praćenom ponašanju, osobito u sektoru zdravstvenog osiguranja<sup>15</sup>. Ovo predstavlja izazov i ostalim specifičnim pravilima domena, primjerice, ako se uređaji koji uključuju obradu zdravstvenih podataka ne mogu tehnički kategorizirati kao medicinski uređaji te su izvan područja primjene uredbe<sup>16</sup>.

## 1.3 Ambijentalno računalstvo

**Ambijentalno ili nevidljivo računalstvo** odnosi se na ključnu tehnologiju na kojoj se temelji „internet stvari”. Neke su od najočitijih primjena „pametne kuće” i „pametni uredi” koji se sastoje od uređaja s ugrađenim sofisticiranim kapacitetom za obradu informacija, a koji jamče veću energetska učinkovitost i osobe s više informacija koje mogu utjecati na svoju potrošnju iz daljine (iako će ovisiti o tome koliko stanar (ne) ovisi o stanodavcu ili upravitelju zgrade). Morat će biti jasno tko je odgovoran za svrhu i način obrade osobnih podataka uključenih u primjenu ambijentalnog računalstva, ne samo radi zaštite temeljnih prava pojedinaca, već i zbog odgovarajuće raspodjele odgovornosti radi osiguravanja pridržavanja uvjeta za ukupnu sigurnost sustava.

## 1.4 Računalstvo u oblaku

Računalstvo u oblaku poznato je kao središnja tehnologija koja omogućuje naprednu analitiku i sposobnosti rudarenja, prikupljanje velikih podataka i analitiku te za poplavu podataka iz „interneta stvari” koje trenutačno upotrebljava oko petina pojedinaca i poduzeća u Europskoj uniji<sup>17</sup>. To omogućuje koncentraciju podataka iz bezbroj uređaja „interneta stvari”, a oslanja se na dostupnosti i povezanosti ogromne količine podataka u velikim objektima za pohranu i obradu širom svijeta<sup>18</sup>. Procjenjuje se da šire prihvaćanje računalstva u oblaku<sup>19</sup> u privatnim i javnim sektorima potencijalno dodaje ukupno 449 mil. eura BDP-u EU28 (0,71 % ukupnog BDP-a Europske unije).

Kontrolu nad osobnim podacima često dijele korisnici i davatelji usluga u oblaku, a odgovornost za obveze zaštite podataka nije uvijek transparentna. To bi moglo značiti da se u praksi pruža nedovoljna zaštita. Ove obveze ne ovise o **fizičkoj lokaciji pohrane podataka**. Štoviše, iako samo tehnologija u pozadini koja podržava poslovne primjene, sama infrastruktura računalstva u oblaku može postati rizična infrastruktura i povećati neravnotežu u tržišnoj moći, s 30 % poduzeća koja u zadnje vrijeme navode poteškoće prilikom poništavanja pretplate ili promjene dobavljača<sup>20</sup>.

### 1.5 Poslovni modeli ovisni o osobnim podacima

Ove su tehnologije omogućile nove poslovne modele koji se oslanjaju na informacije koje se stvaraju ne samo pružanjem usluga, već i iz drugih izvora kao što su prisutnost u društvenim medijima radi procjene rizika i kreditne sposobnosti te maksimiziranja prihoda. Značajni poslovni model danas predstavljaju platforme koje povezuju prodavatelje i kupce, omogućujući dijeljenje i preraspodjelu proizvoda, usluga, vještina i sredstava. Često se nazivaju i „ekonomija dijeljenja” (*sharing economy*), „zajednička potrošnja” (*collaborative consumption*) ili umrežene i mobilne poslovne platforme za pojedince na istoj razini (*peer-to-peer*),<sup>21</sup> a mogu ponuditi klasičnu ekonomsku učinkovitost, uvesti konkurentnost na tržišta i smanjiti otpad. Procjenjuje se da će se u nadolazećim godinama njihova globalna vrijednost učeterostručiti u vrijednosti od 26 do 110 milijardi dolara<sup>22</sup>. Takvi poslovni modeli temeljeni na podacima već stvaraju ogromne prihode u dijeljenju automobila i iznajmljivanju kuća te u financijskoj tehnologiji i društvenom pozajmljivanju. Istraživanja pokazuju da potrošači cijene njihovu očito veću dostupnost i prikladnost<sup>23</sup>.

Valuta takvih platformi obično su ugled korisnika, stručna recenzija (*peer review*) i provjera identiteta. To se potencijalno može smatrati povećanjem transparentnosti i odgovornosti, ali ne nužno u odnosu na samog pružatelja platformi. Veliki igrači na ovim tržištima kritizirani su zbog navodnog uskraćivanja podataka o ugledu upravo od samih pojedinaca na koje se informacije odnose. Postoji velik rizik da bi pojedinci mogli biti isključeni iz usluga zbog ugleda na temelju netočnih podataka koje ne mogu osporiti ili tražiti da se izbrišu. Oslanjanje na podatke iz više izvora također dovodi u pitanje načelo u zakonu EU-a o minimizaciji podataka. Opseg budućeg utjecaja na pojedince i društvo ovih i budućih tehnološki omogućenih poslovnih modela zaslužuje pažljivo razmatranje<sup>24</sup>.

### 1.6 Беспilotne letjelice i autonomna vozila

Bespilotne letjelice, ili polu-autonomne letjelice, trenutačno služe uglavnom u vojne svrhe, ali se sve više upotrebljavaju za potrebe nadzora, mapiranja, prijevoza, logistike i javne sigurnosti, kao što je kontrola požara<sup>25</sup>. Fotografije, videozapisi i ostale osobne podatke koje letjelice prikupe moguće je razmijeniti preko telekomunikacijskih mreža. Njihova upotreba predstavlja ozbiljan rizik od zadiranja u privatnost i ograničavanja slobode izražavanja. Postavlja se pitanje kako se njihov dizajn i upotreba mogu učinkovito regulirati kako bi subjekti podataka mogli ostvariti svoja prava na pristup podacima koje zabilježe ovi strojevi.

Na tlu autonomna vozila ili automobili bez vozača promijenit će način na koji se upotrebljava i organizira pojedinačno putovanje, a mogu zamagliti granicu između privatnog i javnog prijevoza. Procjenjuje se da će do 2035. biti 12 milijuna potpuno autonomnih i 18 milijuna djelomično autonomnih vozila, a Europa će biti među prvim usvojiteljima<sup>26</sup>. Algoritmi koji će upravljati automobilima donosit će odluke koje mogu izravno utjecati na fizički integritet pa čak i život ili smrt osobe, na primjer u izboru programiranom u slučaju neizbježnog udara.



Kao i očita potreba za jasnoćom o tome tko je odgovoran za kontrolu i sigurnost podataka, ove primjene otvaraju niz etičkih pitanja.

## 1.7 Trendovi s potencijalno većim, dugoročnijim učinkom

Predviđa se da će **3D bioprintanje** organskih predmeta koje se koristi kopijama stanica bolesnika i kolagenskim „biološkim zavojima” (odnosno, osjetljivim podacima prema zakonu EU-a) za slaganje uzastopnih redova živih stanica uskoro biti lako dostupno<sup>27</sup>. Olakšalo bi opskrbu prilagođenim dijelovima ljudskoga tijela i bilo bi osobito korisno u siromašnijim i postkonfliktnim područjima svijeta. Bioprintanje postavlja očita pitanja za medicinsku etiku uz očuvanje intelektualnog vlasništva i zaštitu potrošača, ali i za primjenu pravila zaštite podataka s obzirom na to da se oslanja na obradu privatnih i osjetljivih podataka o zdravlju pojedinca.

**Umjetna inteligencija**, poput robotike, odnosi se na tehnološku potrebu i za stacionarnim i za mobilnim autonomnim strojevima. Njihovo će unapređenje ponuditi ogroman potencijal izvan njihove trenutačne primjene. Računala za duboko učenje podučit će se zadacima na način da zbiju velike skupove podataka s pomoću (između ostalog) neuronskih mreža koje simuliraju mozak. Cilj je znanstvenika i poduzeća poboljšati učenje bez nadzora. Algoritmi već sada mogu razumjeti i prevoditi jezike, prepoznavati slike, pisati novinske članke i analizirati medicinske podatke<sup>28</sup>. Društveni mediji daju ogromne količine osobnih podataka koje su sami pojedinci učinkovito prethodno označili. To je možda najnovije u nizu kognitivnih poboljšanja kojim se povećava sposobnost ljudskog mozga, poput papira ili abaka integriranih u autonomne strojeve, robote, no sada je trenutak da razmotrimo šire posljedice za pojedince i društvo<sup>29</sup>.

## 2. Ekosustav zaštite velikih podataka

Europska unija sada ima priliku da pokaže kako vlade, regulatorna tijela, nadzornici, dizajneri, programeri i pojedinci mogu bolje zajedno djelovati ne bi li ojačali prava i upravljali, a ne blokirali, tehnološke inovacije. Prema jednom komentatoru, trendovi opisani u drugom odjeljku „povećali su jaz između onoga što je moguće i onoga što je zakonski dopušteno”<sup>30</sup>. Suprotno nekim tvrdnjama, privatnost i zaštita podataka predstavljaju platformu za održivo i dinamično digitalno okruženje, a ne prepreku. Neovisna tijela za zaštitu podataka kao što je EDPS imaju ključnu ulogu u razbijanju takvih mitova i reagiranju na stvarnu zabrinutost pojedinaca zbog gubitka kontrole nad svojim osobnim podacima<sup>31</sup>.

Sljedeća generacija osobnih podataka vjerojatno će biti još manje dostupna pojedincima na koje se odnosi. Odgovornost za oblikovanje održivog digitalnog jedinstvenog tržišta nužno je raspršena, ali je i međuovisna, poput ekosustava, i zahtijeva učinkovitu interakciju između programera, poduzeća i regulatornih tijela u interesu pojedinca. U ovom odjeljku navodimo doprinos koje će ova četiri važna igrača imati.

### 2.1 Propisi usmjereni na budućnost

Nedavno smo pozvali Europsku uniju da iskoristi svoju povijesnu priliku da pripremi jednostavnija pravila za rukovanje osobnim podacima koja će biti relevantna tijekom jedne generacije<sup>32</sup>. Pregovori o Općoj uredbi o zaštiti podataka i direktivi za zaštitu podataka u policijskom i pravosudnom sektoru u završnoj su fazi, a pozornost će se uskoro usmjeriti ka budućnosti Direktive o privatnosti i elektroničkim komunikacijama te novoj Uredbi koja uređuje kako same institucije EU-a i tijela obrađuju osobne podatke. S ekonomskim troškovima prikupljanja i pohranjivanja podataka koji su gotovo zanemarivi, tijela za zaštitu

podataka bit će zadužena za dosljednu provedbu ovih pravila kako bi se izbjegla „moralna opasnost” pretjerane obrade podataka<sup>33</sup>.

Strategija jedinstvenog digitalnog tržišta prepoznaje povezanost između kontrole velikih količina podataka i tržišne moći. Ona dijeli uvjerenje, izraženo u Preliminarnom mišljenju EDPS-a o privatnosti i konkurentnosti u razdoblju velike količine podataka iz 2014., o potrebi za većom koherentnosti među regulatornim tijelima. Europska unija već ima alate za ispravljanje neravnoteže moći na digitalnom tržištu: primjerice trenutni postupak Europske komisije za zaštitu tržišnog natjecanja predstavlja potvrdu da se mobilni uređaji najviše upotrebljavaju za pristup internetu. Moguća je i više holistička provedba unutar postojećeg pravnog okvira, kao što je putem klirinške kuće EU-a za nadzorna tijela kako bi se razmotrilo mogu li pojedini slučajevi postaviti pitanja o usklađenosti s konkurencijom, pravilima za zaštitu potrošača i podataka. Primjerice:

- Zahtijevanje veće transparentnosti cijene, u gotovini ili na neki drugi način, za neku uslugu, može informirati i olakšati analizu slučajeva natjecanja<sup>34</sup>, i
- Otkrivanje nepravedne diskriminacije cijena na temelju loše kvalitete podataka i nepoštenog profiliranja i korelacija<sup>35</sup>.

Intenzivniji dijalog između regulatornih tijela iz različitih sektora mogao bi dovesti do reakcije na rastuću potrebu za globalnim partnerstvima koja mogu stvoriti „javno dobro” (*a commons*) otvorenih podataka kojim podaci i ideje, kao što su statistika i karte, mogu kolati i biti na raspolaganju te se mogu razmjenjivati u javnom interesu, uz manji rizik od nadzora, kako bi pojedinci imali više utjecaja na odluke koje se odnose na njih<sup>36</sup>.

## 2.2 Odgovorni nadzornici

Odgovornost zahtijeva primjenu unutarnje politike i sustava kontrole koji osiguravaju usklađenost i pružaju relevantne dokaze prijave svega neovisnim nadzornim tijelima.

Zalažemo se za ukidanje birokracije u zakonu o zaštiti podataka na način da se potreba za nepotrebnom dokumentacijom svede na minimum kako bi se maksimalno iskoristio prostor za odgovorniju inicijativu poduzeća, uz vodstvo tijela za zaštitu podataka. Načelo da se osobni podaci moraju obrađivati samo na načine kompatibilne s određenom svrhom/ama za koje su prikupljeni važno je za poštivanje legitimnih očekivanja pojedinaca. Primjerice, kodeksi ponašanja, certificiranje, revizije i nove generacije ugovornih klauzula i obvezujuća korporativna pravila mogu pomoći u izgradnji čvrstog povjerenja u digitalno tržište. Oni koji su odgovorni za rukovanje osobnim podacima trebaju biti puno dinamičniji i proaktivniji te se trebaju maknuti od tzv. tajnovitosti „crne kutije” i netransparentnosti poslovne prakse dok zahtijevaju sve veću transparentnost od korisnika<sup>37</sup>.

## 2.3 Inženjering usmjeren na privatnost

Ljudska inovacija uvijek je bila proizvod aktivnosti specifičnih društvenih skupina i određenih konteksta te obično odražava društvene norme dotičnog vremena<sup>38</sup>. Međutim, odluke o tehnološkom dizajnu ne bi trebale diktirati naše društvene interakcije i strukturu zajednica, već trebaju podržati naše vrijednosti i temeljna prava.

Europska unija treba razvijati i promovirati tehnike i metodologije inženjeringa koje dopuštaju primjenu tehnologije obrade podataka kako bi se u potpunosti poštivali dostojanstvo i prava pojedinca. Inženjeri sustava i softvera moraju razumjeti i bolje

primjenjivati načela privatnosti po dizajnu u novim proizvodima i uslugama u fazama dizajniranja i u tehnologijama. Odgovornost treba podržati većim istraživanjem i razvojem metoda i alata kako bi se osigurale točne revizije i utvrdila sukladnost nadzornika i obrađivača s pravilima, kao što je „označavanje” svake jedinice osobnih podataka „metapodacima” koji opisuju zahtjeve za zaštitu podataka.

Inženjerska rješenja trebaju pomoći onim pojedincima koji žele sačuvati svoju privatnost i slobodu putem anonimnosti. Europska unija treba promicati razvoj i primjenu algoritama koji skrivaju identitete i prikupljaju podatke kako bi se zaštitilo pojedinca dok se istovremeno iskorištava moć predviđanja koju imaju podaci<sup>39</sup>.

Danas moramo položiti temelje za rješavanje ovih zadataka okupljanjem programera i stručnjaka za zaštitu podataka iz različitih područja u širim mrežama, kao što su Internet Privacy Engineering Network („IPEN”) koji pridonose plodnoj interdisciplinarnoj razmjeni ideja i pristupa.

## 2.4 Ovlašteni pojedinci

### Protrošačko (*prosumer*) okruženje

Pojedinci nisu samo pasivni objekti kojima je potrebna zaštita zakona protiv izrabljivanja. Digitalni trendovi prethodno opisani predstavljaju pozitivne prilike za jačanje uloge pojedinca. Primjerice, ljudi sada proizvode i konzumiraju sadržaj i usluge te se sve češće može smatrati da su jednako odgovorni kao i pružatelji usluga za obradu osobnih podataka, osim ako je to u čisto „kućanske” svrhe<sup>40</sup> (pojam „protrošači” opisuje ovakav razvoj<sup>41</sup>). U međuvremenu, virtualne valute korisnicima nude anonimnost i zaobilaznje provjere transakcija trećih strana, a time i niže transakcijske troškove za plaćanje roba i usluga preko granica. S druge strane, zahvaljujući anonimnosti i međupravnoj (ili, kao što se može tvrditi, pravnoj) nadležnosti ovih virtualnih valuta pojedinci postaju potencijalne žrtve prijevara i kriminalnih tržišta koja je teško otkriti i istražiti. Osim dužnosti regulatornih tijela, poduzeća i inženjera, građani također imaju odgovornost da budu svjesni, oprezni, kritički i obaviješteni prilikom donošenja odluka na i izvan mreže<sup>42</sup>.

### Pristanak

Štoviše, suprotno tradicionalnom mišljenju, ne može se svo ljudsko ponašanje objasniti ekonomskim načelima koja pretpostavljaju da su ljudska bića u potpunosti racionalna i osjetljiva na ekonomske poticaje<sup>43</sup>. Ovo se odnosi na buduću ulogu pristanka pojedinca na obradu njegovih osobnih podataka. Prema zakonu Europske unije, pristanak nije jedina legitimna osnova za velik dio obrade. Čak i kada pristanak igra važnu ulogu, on ne oslobađa nadzornike od njihove odgovornosti za ono što čine s podacima, osobito kada se dobije opći pristanak na obradu za širok raspon svrha.

### Kontrola i „vlasništvo” nad podacima

Pojedinci moraju moći osporiti pogreške i nepravedne predrasude koje proizlaze iz logike kojom se koriste algoritmi za određivanje pretpostavki i predviđanja. Primjera radi, u SAD-u je istraživanje gotovo 3000 kreditnih izvješća koja pripadaju 1000 potrošača otkrila da je 26 posto imalo „stvarne” pogreške koje su dovoljno ozbiljne da utječu na kreditne ocjene potrošača, a time i na trošak dobivanja kredita<sup>44</sup>.

Podaci se često smatraju resursom, poput ulja, kojim trguju u idealnom slučaju jednako obaviještene strane u transakciji<sup>45</sup>. Potrošači ne dobivaju pravedne naknade za svoje osobne informacije kojima se trguje, a neki se i zalažu za model vlasništva nad podacima. Apsolutnu kontrolu nad osobnim podacima ipak je teško zajamčiti - pojavit će se drugi problemi kao što su javni interes te prava i slobode drugih. Kontrola je nužna, ali ne dovoljna<sup>46</sup>. Međutim, ljudsko je dostojanstvo uvijek konstantno, a po zakonu EU-a analogija vlasništva ne može se primijeniti kao takva na osobne podatke koji su intrinzično povezani s pojedinačnim osobnostima. Ne postoji odredba u zakonu Europske unije o zaštiti podataka koja dopušta pojedincu da se odrekne ovog temeljnog prava.

Jedan alternativni postupak za davanje pojedincima bolje kontrole nad njihovim podacima kojima mogu pristupiti i za koju svrhu mogla bi biti upotreba spremišta osobnih podataka ili „podatkovnih trezora”<sup>47</sup>. Koncept takvog „osobnog spremišta” zahtijeva sigurnosne mehanizme kojima se osigurava da samo oni subjekti koje su subjekti podataka ovlastili mogu pristupiti podacima i samo onim dijelovima za koja su ovlašteni. Spremišta osobnih podataka bila bi najučinkovitija ako se odnose na trenutne i stalno aktualizirane informacije kao što su geoprostorni podaci ili znakovi života. Osim tehničkih mjera zaštite, korisnici podataka bili bi obvezni poštovati pravila za razmjenu podataka i uporabu. Konkurencija i mogućnost promjene usluge kojom se netko koristi najučinkovitija je moć potrošača da utječe na tržište usluga koje su im dostupne. Pokazalo se da je osiguravanje prenosivosti veza, uključujući i označivače i podatke za kontakt izrazito plodonosno za konkurentnost te je učinkovito smanjilo potrošačke cijene kada je liberalizirano telekomunikacijsko tržište. Prenosivost podataka, odnosno činjenična i praktična mogućnost za prijenos većine vlastitih podataka s jednog davatelja usluga na drugi učinkovito je polazište za stvaranje uvjeta za pravi izbor potrošača.

### **3. Dostojanstvo u samoj srži nove digitalne etike**

Etički okvir treba poduprijeti temelje ovog digitalnog ekosustava. Europski nadzornik za zaštitu podataka smatra da bi veće poštivanje i očuvanje ljudskog dostojanstva mogli biti protuteža sveprisutnom nadzoru i asimetriji moći s kojima se sada suočava pojedinac. To bi trebalo biti u samoj srži nove digitalne etike.

#### **3.1 Dostojanstvo i podaci**

Nakon Industrijske revolucije u 18. i 19. stoljeću, pokret za ljudska prava pokušalo je zaštititi šire društveno dobro smanjenjem broja prepreka poštivanju pojedinca. Europska je unija sada, Poveljom o temeljnim ljudskim pravima, nakon Opće deklaracije o ljudskim pravima i Europske konvencije o ljudskim pravima, kao polazište uzela nepovredivost ljudskog dostojanstva. Dostojanstvo ljudske osobe nije samo temeljno pravo, već je i temelj za kasnije slobode i prava, uključujući prava na privatnost i zaštitu osobnih podataka<sup>48</sup>. Povrede dostojanstva mogu uključivati objektivizaciju gdje se s osobom postupa kao s alatom koji služi u tuđe svrhe<sup>49</sup>. Privatnost je sastavni dio ljudskog dostojanstva, a pravo na zaštitu podataka izvorno je zamišljeno 70-ih i 80-ih kao način nadoknade potencijala za eroziju privatnosti i dostojanstva obradom velikog opsega osobnih podataka. U Njemačkoj se pravo na „informacijsko samoodređenje” temelji na pravima na osobno dostojanstvo i slobodan razvoj osobnosti utvrđenima u člancima 1. i 2. njemačkog Ustava<sup>50</sup>.

Međutim, u ranom 21. stoljeću, pojedinci sve češće moraju otkriti puno više osobnih informacija preko interneta kako bi sudjelovali u društvenim, administrativnim i komercijalnim pitanjima, uz sve više ograničeni prostor za povlačenje pristanka. Budući da je

sva aktivnost potencijalno uvijek prikazana online, pojam slobodnog i informiranog pristanka nalazi se pod ogromnim pritiskom. „Digitalne krušne mrvice” ispuštaju se svake minute, a kombiniraju se kako bi klasificirali pojedince u stvarnom vremenu radi stvaranja višestrukih i povremeno kontradiktornih profila. Ovi profili u mikrosekundi mogu cirkulirati bez znanja pojedinca, a upotrebljavaju se kao temelj za važne odluke koje utječu na njih.

Profili koji se upotrebljavaju za predviđanje ponašanja ljudi predstavljaju rizik od stigmatizacije, a učvršćuju postojeće stereotipe, društvenu i kulturnu segregaciju i isključenost<sup>51</sup>, s time da takva „kolektivna inteligencija” potkopava individualni izbor i jednake mogućnosti. Ovi „filter mjehurići” (*filter bubbles*) ili „osobne sobe jeke” (*personal echo-chambers*) na kraju bi mogli ugušiti samu kreativnost, inovativnost i slobode izražavanja te udruživanja koji su omogućili procvat digitalne tehnologije.

U međuvremenu se stalno stanje izuzetka na temelju „sigurnosti” upotrebljava kao opravdanje za višestruko raslojavanje nametljivih tehnika za praćenje aktivnosti pojedinaca<sup>52</sup>. Razumijevanje ove „nadzorne prepreke” zahtijeva dugoročniji pogled na cjelokupne učinke na društvo i ponašanje.

Zajedno s trećim zemljama, EU se treba intenzivno pozabaviti time kako osigurati da se ove vrijednosti ne poštuju samo na papiru, a zapravo se neutraliziraju u *cyberspaceu*. Osobito se Europska unija sada nalazi u „rizičnom razdoblju” prije masovnog usvajanja ovih tehnologija za usađivanje vrijednosti u digitalne strukture koje će definirati naše društvo<sup>53</sup>. A za to treba ponovno procijeniti ovise li potencijalne prednosti novih tehnologija stvarno o prikupljanju i analizi osobnih podataka milijardi pojedinaca. Takva bi procjena mogla predstavljati izazov programerima da smisle proizvode koji u stvarnom vremenu depersonaliziraju ogromne količine neorganiziranih informacija čime se otežava ili onemogućuje izdvajanje pojedinca.

Već smo sada svjesni da obradu određenih podataka, primjerice genetskih podataka, treba ne samo regulirati već ih primjerice etička povjerenstva trebaju procijeniti u okviru širih društvenih problema. Zahvaljujući samoj svojoj prirodi, genetski podaci odnose se ne samo na jednog pojedinca, već i na njegovo porijeklo i potomstvo. Genetski podaci ne služe samo za identifikaciju obiteljskih odnosa, već elementi koji se nalaze u genima jednog pojedinca mogu također pružiti informacije o svojim roditeljima i djeci, te dovesti do odluka koje donose nadzornici koji utječu na njihove prilike u životu, čak i prije njihovog rođenja. Moguća koncentracija genetskih osobnih podataka u rukama nekoliko divovskih igrača na tržištu utjecat će na tržišne ekonomije i na subjekte podataka. Rastuća ovisnost o globalnom sustavu prikupljanja i analize stalnog protoka podataka mogla bi od društva i gospodarstva učiniti žrtve neviđenih sigurnosnih propusta i zlonamjernih napada.

Postojeći okvir mogao bi doživjeti neuspjeh ako budućnosti ne pristupimo inovativno. Sve je veća potražnja i potreba za promatranjem subjekta podataka kao pojedinca, a ne samo kao potrošača ili korisnika. Tijela za zaštitu podataka koja su zaista neovisna imaju ključnu ulogu u sprečavanju budućnosti u kojoj su ljudi određeni algoritmima i njihovim kontinuiranim varijacijama. Moraju biti opremljeni da izvrše „obvezu postupanja s dužnom pozornošću” prema pojedincima i njihovim dostojanstvom online. Tradicionalni pojmovi i načela privatnosti te zaštite podataka već sadrže etičke nijanse za zaštitu dostojanstva, kao što su zapošljavanje i zdravlje. No današnji su trendovi otvorili posve novo poglavlje i treba istražiti jesu li načela dovoljno čvrsta za digitalno doba<sup>54</sup>. Sam će se pojam osobnih podataka vjerojatno radikalno promijeniti jer tehnologija sve češće omogućuje da se pojedinci ponovno identificiraju iz navodno anonimnih podataka. Osim toga, strojno učenje i spajanje ljudske i umjetne inteligencije potkopat će ideje prava i odgovornosti pojedinca.

### 3.2 Europski Etički savjetodavni odbor

Nije nam namjera dočarati alarmantnu sliku distopije. U pravnim, političkim, ekonomskim, društvenim, znanstvenim pa čak i religijskim sferama rasprave su već u tijeku<sup>55</sup>. Jednostavni pristupi koji daju jednostranu prednost ekonomskoj dobiti ili nadzoru radi sigurnosti vjerojatno nisu ništa korisniji od pretjerano restriktivne primjene postojećih zakona koji kočé inovativnost i napredak. Stoga EDPS predlaže detaljnu, široku i multidisciplinarnu analizu koja bi ponudila preporuke i podučila društvenu raspravu o tome kako slobodno, demokratsko društvo treba odgovoriti na tehnološki izazov.

Strategija EDPS-a<sup>56</sup> bavi se razvojem etičkog pristupa zaštiti podataka koji priznaje da „ostvarivo, korisno ili isplativo ne znače isto što i održivo” i koji naglašava važnost „odgovornosti nad mehaničkom sukladnošću u skladu sa slovom zakona”. Namjera nam je da nas čuju i izvan zajednice dužnosnika EU-a, odvjetnika i IT stručnjaka i doći do uglednih osoba koje su opremljene i sposobne procijeniti srednje do dugoročne posljedice tehnoloških promjena i regulatornih odgovora. U narednim mjesecima u našoj neovisnoj instituciji osnovat ćemo vanjsku savjetodavnu skupinu za etičku dimenziju zaštite podataka kako bismo istražili odnose između ljudskih prava, tehnologije, tržišta i poslovnih modela u 21. stoljeću.

Naš Etički savjetodavni odbor činit će odabrana skupina istaknutih osoba iz područja etike i filozofije, sociologije, psihologije, tehnologije i ekonomije, a po potrebi podržavat će ih dodatni stručnjaci sa znanjem i iskustvom u područjima kao što su zdravlje, promet i energetika, socijalna interakcija i mediji, ekonomija i financije, upravljanje i demokracija te sigurnost i policija. Pozvat će se da razmotre šire etičke implikacije toga kako se shvaćaju i upotrebljavaju osobni podaci, uz maksimalnu transparentnost njihovih rasprava.

## 4. Zaključak: Vrijeme je za produblјivanje rasprave

Privatnost i zaštita podataka dio su rješenja, a ne problem. Za sada tehnologiju kontroliraju ljudi. Nije lako takav potencijalni razvoj uredno razvrstati u dobar ili loš, poželjan ili štetan, napredan ili nazadan, a još manje kada se niz mogućnih trendova mora gledati u kontekstu. Kreatori politike, osobe koje razvijaju tehnologije i poslovanje kao i svi mi moramo ozbiljno razmotriti želimo li i na koji način utjecati na razvoj tehnologije i njezinu primjenu. Međutim, jednako je važno da EU žurno razmotri etiku i položaj ljudskog dostojanstva u budućim tehnologijama.

Načela zaštite podataka pokazala su se sposobnim čuvati pojedince i njihovu privatnost od rizika neodgovorne obrade podataka. Međutim, današnji trendovi mogu zahtijevati potpuno novi pristup. Stoga otvaramo novu raspravu o tome u kojoj je mjeri primjena načela poput pravednosti i legitimiteta dostatna. Zajednica za zaštitu podataka može igrati novu ulogu koristeći se postojećim alatima poput prethodnih provjera i odobrenja – jer nijedno drugo tijelo nije opremljeno ispitivati takvu obradu podataka. Uz tehnologiju, globalne inovacije i ljudska povezanost razvijaju se vratolomnom brzinom, te stoga imamo priliku privući pažnju, izazvati interes i postići konsenzus.

Nadamo se da ćemo ovim mišljenjem pružiti okvir za šire i dublje rasprave o tome kako EU može osigurati integritet svojih vrijednosti istodobno s prihvaćanjem pogodnosti novih tehnologija.

Sastavljeno u Bruxellesu 11. rujna 2015.

**(potpis)**

Giovanni BUTTARELLI

Europski nadzornik za zaštitu podataka

## Napomene

---

<sup>1</sup> Izvor: GSMA Intelligence.

<sup>2</sup> „Mooreov zakon” koji kaže da se broj tranzistora koji se mogu staviti na mikročip udvostručuje otprilike svakih 18 mjeseci općenito se pokazala točnom; Moore, Gordon E. (19. 4. 1965.). „Cramming more components onto integrated circuits”, *Electronics*. 22. 8. 2011.

<sup>3</sup> Nathan Eagle, Alex (Sandy) Pentland, „Reality mining: sensing complex social systems”, *Journal Personal and Ubiquitous Computing* svezak 10 izdanje 4. ožujka 2006., str. 255. – 268. Shoshana Zuboff u „Big Other: surveillance capitalism and the prospects of an information civilization”, *Journal of Information Technology* (2015.) 30, str. 75. – 89., navodi „Kao rezultat sveprisutnog računalnog posredovanja, gotovo svaki aspekt svijeta prikazan je u novoj simboličkoj dimenziji dok događaji, objekti, procesi i ljudi postaju vidljivi, razumljivi i djeljivi na novi način”. Zuboff ima viziju o „usponu nove arhitekture svemira” koju naziva „Veliki drugi” (*Big Other*), „sveprisutni režim umreženih institucija koji bilježi, mijenja i pretvara svakodnevno iskustvo u robu, od tostera do tijela, od komunikacije do misli, a sve s ciljem uspostavljanja novih putova do zarade i profita”; str. 77, 81.

<sup>4</sup> „BBC otkrio konačni izgled računala Micro Bit” 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.

<sup>5</sup> Niti jedno od deset najboljih poduzeća u sektoru tehnologije prema tržišnoj kapitalizaciji nema sjedište u Europskoj uniji (osam je američkih tvrtki, po jedna u Kini i Tajvanu) prema istraživanju PWC-a deset najboljih poduzeća na svijetu prema tržišnoj kapitalizaciji, ažurirano 31. ožujka 2015.

<sup>6</sup> „Veliki podaci odnose se na eksponencijalni rast kako u dostupnosti tako i u automatskoj uporabi informacija: odnosi se na gigantske digitalne skupove podataka u posjedu korporacija, vlada i drugih velikih organizacija koji se zatim intenzivno analiziraju (otuda i ime: analitika) s pomoću računalnih algoritama”; Mišljenje 03/2013 o ograničenju namjene Radne skupine iz čl. 29. U izvješću Bijeke kuće u 2014. Veliki podaci opisani su kao „rastuća tehnološka sposobnost bilježenja, skupljanja i obrade sve veće količine, brzine obrade i raznolikosti podataka”, vidjeti *Big Data: Seizing Opportunities, Preserving Values*, Executive Office of the President („Podestovo izvješće”), svibanj 2014.

<sup>7</sup> Prema zakonu Europske unije, „osobni podaci” definirani su kao „bilo koji podaci vezani za fizičku osobu (dalje u tekstu: „subjekt obrade podataka”) kojoj je utvrđen identitet ili onu kojoj se može izravno ili neizravno utvrditi identitet, a posebno pozivanjem na identifikacijski broj ili na jedan ili više čimbenika karakterističnih za fizički, fiziološki, mentalni, ekonomski, kulturni ili socijalni identitet te osobe”; čl. 2. (a) Direktive 95/46/EZ. Ova je definicija uglavnom usporediva s onima koje je usvojilo Vijeće Europe u Konvenciji za zaštitu osoba glede automatizirane obrade osobnih podataka (poznata i kao Konvencija 108) i u OECD-ovim Smjernicama o zaštiti privatnosti i međunarodnom prijenosu osobnih podataka. Za dubinsku analizu vidjeti Mišljenje 4/2007 Radne skupine iz članka 29., WP136.

<sup>8</sup> Vidjeti na primjer govor predsjednice američke Federalne trgovinske komisije iz 2014.: „Drastičan rast povezanih uređaja, nagli pad troška prikupljanja, pohrane i obrade podataka te sposobnost informacijskog posrednika i drugih da kombinira izvanmrežne i mrežne podatke znači da poduzeća mogu prikupljati gotovo neograničene količine podataka potrošača i pohranjivati ih na neodređeno vrijeme. S pomoću prediktivne analize mogu saznati iznenađujuće puno o svakome od nas iz ovoga”; uvodni govor predsjednice Federalne trgovinske komisije Edith Ramirez, „Big Data: A Tool for Inclusion or Exclusion?”, Washington, DC 15. rujna 2014. Prema Sandy Pentland, „Socijalna fizika kvantitativna je društvena znanost koja opisuje pouzdane, matematičke veze između protoka informacija i ideja s jedne strane te ponašanje ljudi s druge strane... to nam omogućuje da predvidimo produktivnost malih skupina, odjela unutar poduzeća pa čak i čitavih gradova”. To je „ono što je potrebno za izgradnju boljih društvenih sustava” (str. 4, 7) i „za omogućavanje (državnim



---

službenicima, industrijskim menadžerima i građanima) da se koriste alatima poticaja društvenih mreža kako bi se *uspostavile nove norme ponašanja*” (str. 189) ( naš kurziv); Pentland, *Social Physics: How Good Ideas Spread: The Lessons from a New Science*.

<sup>9</sup> Posebno ispitivanje Eurobarometra 431 o zaštiti podataka, lipanj 2015. i panel istraživanje Pew Research iz siječnja 2014. o javnoj predodžbi privatnosti i sigurnosti u eri nakon Snowdena. Prema istraživanju, prosječni posjet nekoj internetskoj stranici rezultira s 56 slučajeva prikupljanja podataka, prema Juliji Angwin *Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance*, 2012.). U izvješću Bijele kuće iz 2014. o obradi velikih podataka tvrdi se da „besprimjerna računalna moć i sofisticiranost... stvaraju asimetriju moći između onih koji imaju podatke i onih koji ih namjerno ili nenamjerno daju”; „neki od najvećih izazova otkrivenih tijekom ovog pregleda odnose se na to kako analiza velikih podataka može (...) stvoriti tako neprozirno okruženje za donošenje odluka da se nezavisnost pojedinca gubi u neprobojnom skupu algoritama”.

<sup>10</sup> S pomoću javnih anonimnih podataka iz popisa stanovništva iz 1990., 87 % stanovništva SAD-a najvjerojatnije je bilo moguće identificirati prema peteroznamenastom poštanskom broju u kombinaciji sa spolom i datumom rođenja; vidjeti Paul Ohm „Broken promises of privacy: responding to the surprising failure of anonymisation”, *UCLA Law Review* 2010 i „Record linkage and privacy: issues in creating new federal research and statistical info”, travanj 2011. DNK je jedinstven (osim u slučaju jednodječanih blizanaca) i ne mijenja se tijekom života. Sadrži podatke o etničkoj pripadnosti, predispozicijama za bolesti i služi da identifikaciju ostalih članova obitelji. U siječnju 2013. znanstvenici su uspjeli identificirati pojedince i obitelji iz anonimnih DNK podataka iz javno dostupnih rodoslovnih baza podataka; Gymrek, M., McGuire, A. L., Golan, D., Halperin, E. & Erlich, Y. *Science* 339, 321 – 324 (2013.). Vidjeti također „Poorly anonymized logs reveal NYC cab drivers’ detailed whereabouts” (Zapisi sa slabo anonimiziranim podacima otkrivaju detaljan položaj njujorških taksista), 23. 6. 2014. <http://arstechnica.com/tech-policy/2014/06/poorly-anonymized-logs-reveal-nyc-cab-drivers-detailed-whereabouts/> (pristupljeno 10. 9. 2015.). Vidjeti također Mišljenje 04/2007 o pojmu osobnih podataka Radne skupine iz čl. 29; Mišljenje 03/2013 o ograničenju namjene Radne skupine iz čl. 29; Mišljenje 06/2013 o otvorenim podacima i ponovnoj upotrebi informacija javnog sektora Radne skupine iz čl. 29; i WP29 Mišljenje 05/2014 o anonimizaciji Radne skupine iz čl. 29.

<sup>11</sup> Izvor: Gartner.

<sup>12</sup> Vidi npr. panel raspravu „What is the future of official statistics in the Big Data era?” (Kakva je budućnost službene statistike u doba obrade velike količine podataka) Kraljevskog statističkog društva, London 19. siječnja 2015.; <http://www.odi.org/events/4068-future-official-statistics-big-data-era> (pristupljeno 10. 9. 2015.).

<sup>13</sup> Deset tehnologija koje bi mogle promijeniti naše živote: potencijalni utjecaji i političke implikacije, Odjel za znanstvena predviđanja, Glavna uprava za usluge parlamentarnih istraživanja, siječanj 2015.

<sup>14</sup> Radni program 2016/2017 Obzora Europske unije 2020 podržava takav razvoj, uključujući pilot projekte velikih razmjera koji će se baviti privatnošću i etičkim pitanjima.

<sup>15</sup> Osiguranje je opisano kao „prirodni poslovni model za internet stvari”; „From fitness trackers to drones, how the ‘Internet of Things’ is transforming the insurance industry” (Od praćenja tjelesne kondicije do bespilotnih letjelica, kako „internet stvari” mijenja industriju osiguranja), *Business Insider* 11. 6. 2015. Pojam diskriminacije cijena u pravu tržišnog natjecanja, iz članka 102. UFEU-a koji zabranjuje dominantnom poduzeću na tržištu da „izravno ili neizravno nameće nepravedne kupovne ili prodajne cijene ili druge nepravedne uvjete trgovanja”, vrlo je sporan, vidjeti na primjer Damien Girardin i Nicolas Petit, *Price Discrimination Under EC Competition Law: Another Antitrust Theory in Search of Limiting Principles* (srpanj 2005.), serija radnih dokumenata Global Competition Law Centre br. 07/05. Za velike podatke i njihovo potencijal (koji, prema autorima, još uvijek nije ostvaren) da se ubrza određivanje personaliziranih cijena vidjeti izvješće Izvršnog ureda predsjednika SAD-a, *Big Data and Differential Pricing*, veljača 2015., a nedavna analiza u kojoj se zaključuje da personalizirane cijene općenito podrazumijevaju obradu osobnih podataka pa stoga moraju poštivati načelo transparentnosti zakona o zaštiti podataka koji zahtijeva od poduzeća da obavještavaju ljude o

---

svrsi obrade njihovih osobnih podataka: poduzeća to moraju izjaviti ako će personalizirati cijene. A ako se poduzeće koristi kolačićem za prepoznavanje pojedinaca, Direktiva o privatnosti i elektroničkim komunikacijama zahtijeva od poduzeća da ga obavijesti o svrsi kolačića”; radni nacrt Frederika Borgesiusa „Online Price Discrimination and Data Protection Law”. Dostupno na adresi [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2652665](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2652665) (pristupljeno 10. 9. 2015.).

<sup>16</sup> Medicinski uređaji definirani su u pravu EU-a u Direktivi Vijeća 93/42/EEZ o medicinskim uređajima izmijenjenoj Direktivom 2007/47/EZ Europskoga parlamenta i Vijeća od 5. rujna 2007. Za implikacije „mobilnog zdravstva” na zaštitu podataka vidi Mišljenje Europskog nadzornika za zaštitu podataka 1/2015.

<sup>17</sup> Prema Eurostatu, 21 % pojedinaca i 19 % poduzeća u Europskoj uniji koristi se uslugama oblaka za pohranu.

<sup>18</sup> „Da je internet diljem svijeta država, bio bi 12. najveći potrošač električne energije u svijetu, negdje između Španjolske i Italije. To predstavlja približno 1,1 do 1,5 posto globalne uporabe električne energije (od 2010.) i stakleničkih plinova koje godišnje proizvodi 70 do 90 velikih (500 megavata) termoelektrana na ugljen”. Vijeće za obranu prirodnih resursa, Procjena učinkovitosti podatkovnog centra: Scaling Up Energy Efficiency Across the Data Centre Industry: Evaluating Key Drivers and Barriers 2014.

<sup>19</sup> Izvješće o istraživanju „SMART 2013/0043 - Uptake of Cloud in Europe”.

<sup>20</sup> Izvor: Eurostat.

<sup>21</sup> Pojam „ekonomija dijeljenja” naišao je na kritike jer može navoditi na pogrešan zaključak. „The Sharing Economy Isn’t About Sharing at All”, Giana M. Eckhardt i Fleura Bardhi, Harvard Business Review, 28. 1. 2015.

<sup>22</sup> Rachel Botsman i Roo Rogers, *What’s Mine Is Yours: How Collaborative Consumption is Changing the Way We Live*, 2011.

<sup>23</sup> Future of Privacy Forum, „User Reputation: Building Trust and Addressing Privacy Issues in the Sharing Economy”, lipanj 2015.

<sup>24</sup> Vidjeti radionicu od 9. lipnja 2015. američke Federalne trgovinske komisije o „Natjecanju, zaštiti potrošača i ekonomskim pitanjima koja postavlja ekonomija dijeljenja”, <https://www.ftc.gov/news-events/events-calendar/2015/06/sharing-economy-issues-facing-platforms-participants-regulators/> (pristupljeno 10. 9. 2015.).

<sup>25</sup> Za implikacije zaštite podataka bespilotnih letjelica ili daljinski upravljanih zrakoplovnih sustava vidi Mišljenje Europskog nadzornika za zaštitu podataka o Komunikaciji Komisije Europskom parlamentu i Vijeću o „Novoj eri za zrakoplovstvo – Otvaranje zrakoplovnog tržišta za sigurnu i održivu civilnu uporabu daljinski upravljanih zrakoplovnih sustava”, studeni 2014.

<sup>26</sup> Izvor: Boston Consulting Group.

<sup>27</sup> Gartner.

<sup>28</sup> Facebookov algoritam za prepoznavanje lica DeepFace ostvario je uspjeh od 97 % čime je nadmašio ljude; DeepFace: Closing the Gap to Human-Level Performance in Face Verification, objavljeno u izvješću o IEEE konferenciji o računalnom vidu i raspoznavanju uzoraka od lipnja 2014.

<sup>29</sup> Robo je definiran kao „stroj koji se nalazi u svijetu koji osjeća, misli i djeluje”; Becky, G, „Current trends in robotics: technology and ethics”, u „Robot Ethics - The ethical and social implications of robotics”, MIT Press2, 2012., str. 18. Procjenjuje se da će se 22 milijuna uslužnih robota prodati između 2013. i 2016. godine; IFR World Robotics Report (Svjetsko izvješće o robotici), 2013. Za umjetnu inteligenciju vidjeti Rise of the Machines, Economist, 9. 5. 2015. i internetski projekt Pew Research Centra iz 2014. Poduzeće za umjetnu inteligenciju uvjetovalo je svoju akviziciju od strane vodećeg tehnološkog poduzeća 2014. godine uspostavom etičkog odbora i odbora za sigurnost te

---

zabranom upotrebe umjetne inteligencije u vojne ili obavještajne svrhe; Forbes, Inside Google's Mysterious Ethics Board, 3. 2. 2014.

<sup>30</sup> Pentland, *Social physics*, str. 147.

<sup>31</sup> Vidi prethodnu bilješku 9. Pentland *Social Physics* str. 153: „Mogući su veliki skokovi u zdravstvu, transportu, energetici i sigurnosti... glavne prepreke za postizanje ovih ciljeva jesu pitanje privatnosti i činjenica da još uvijek nemamo nikakav konsenzus oko kompromisa između osobnih i društvenih vrijednosti”. Rasprava oko epidemije ebole u zapadnoj Africi iz 2014. objašnjava kako je nastala ova lažna dihotomija između privatnosti pojedinca i društvenih potreba. Bolesti su se pratile i njihov se vijek trajanja mjerio putem istraživanja i popisa stanovništva koji vrlo lako postanu zastarjeli i koje je teško ekstrapolirati kako bi se predvidjelo gdje će sljedeće izbiti. Postoje neki primjeri upotrebe „velikih podataka” radi praćenja izbijanja malarije u Namibiji i Keniji, a 2009. za praćenje učinkovitosti zdravstvenih upozorenja vlade tijekom meksičke krize zbog svinjske gripe. Zapis mobilnih poziva jedan je izvor podataka, a on pokazuje baznu stanicu koja je primila poziv i može dati grubu procjenu položaja ljudi i smjera kamo idu u stvarnom vremenu. Cilj nije skupljanje tih zapisa. Na taj se način ne mogu razlikovati oni koji imaju ebolu od onih koji nemaju. Švedska neprofitna organizacija mapirala je mobilnost stanovništva u zapadnoj Africi, ali podaci nisu bili upotrijebljeni jer ih mobilni operateri nisu htjeli objaviti odobrenim vanjskim znanstvenicima tvrdeći da trebaju upute od vlade koja je pak navela problem privatnosti koja se nije mogla zajamčiti prema zakonu EU-a; <http://www.pri.org/stories/2014-10-24/how-big-data-could-help-stop-spread-ebola>. (pristupljeno 10. 9. 2015.)

<sup>32</sup> Mišljenje EDPS-a 3/2015.

<sup>33</sup> Pretpostavka velikih podataka da je „N = sve” odnosi se na promatranje svih podataka, a ne samo uzorka, Viktor Mayer-Schönberger i Kenneth Cukier, *The Rise of Big Data: How it's changing the way we think about the world*, 2013. Lisabonsko vijeće i Institut za progresivnu politiku tvrde da će se blagostanje povećati maksimalnim povećavanjem „digitalne gustoće”- „količinom podataka kojom se koristi po glavi stanovnika u gospodarstvu” <http://www.lisboncouncil.net/component/downloads/?id=1178> (pristupljeno 10. 9. 2015.). Međunarodna Radna skupina za zaštitu podataka u telekomunikacijama (poznata kao „Berlinska skupina”) predložila je odstupanja od načela zaštite podataka radi obrade velikih podataka; [http://www.datenschutz-berlin.de/attachments/1052/WP\\_Big\\_Data\\_final\\_clean\\_675.48.12.pdf](http://www.datenschutz-berlin.de/attachments/1052/WP_Big_Data_final_clean_675.48.12.pdf). (pristupljeno 10. 9. 2015.) Svjetski gospodarski forum pozvao je na fokusiranje na upotrebu, a ne skupljanje i odustajanje od zahtjeva za pristankom na prikupljanje osobnih podataka; *Unlocking the Value of Personal Data: From Collection to Usage*, 2013.

<sup>34</sup> Vidjeti Preliminarno mišljenje EDPS-a o privatnosti i konkurentnosti u razdoblju velike količine podataka.

<sup>35</sup> Članak 21. Povelje o temeljnim pravima zabranjuje „bilo kakvu diskriminaciju na temelju bilo kojeg razloga kao što su spol, rasa, boja kože, etničko ili društveno porijeklo, genetičke osobine, jezik, religija ili uvjerenje, političko ili drugo mišljenje, pripadnost nacionalnoj manjini, imovinskom statusu, rođenju, invalidnosti, dobi ili spolnoj orijentaciji”. Mnoge od ovih kategorija podataka („koje otkrivaju rasno ili etničko podrijetlo, političko mišljenje, vjerska ili filozofska uvjerenja, članstvo u sindikatu i obradu podataka o zdravlju ili spolnom životu”) dobile su veću zaštitu prema članku 8. Direktive 95/46/EZ.

<sup>36</sup> Za ideju digitalnih javnih dobra vidjeti *Ambition numérique: Pour une politique française et européenne de la transition numérique*, French Digital Council, lipanj 2015. str. 276; Bruce Schneier zagovara stvaranje „javnih prostora ni u čijem vlasništvu” (*unowned public spaces*) na internetu, poput javnih parkova, *Data and Goliath*, str. 188 – 189; Sandy Pentland zalaže se za „javne podatke kao zajedničko dobro”, *Social Physics*, str. 179. Za procjenu sigurnosti objavljivanja prikupljenog skupa podataka kao otvorenih podataka vidjeti Mišljenje 06/2013 o otvorenim podacima i ponovnoj upotrebi informacija javnog sektora Radne skupine iz čl. 29.

---

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

<sup>38</sup> „Iza tehnologije koja utječe na društvene odnose nalaze se isti ti društveni odnosi“, David Noble, „Social Choice in Machine Design: The Case of Automatically Controlled Machine Tools“, u *Case Studies in the Labor Process*, ur. Andrew Zimbalist, 1979. Vidi također Judy Wacjman, *Pressed for Time: The Acceleration of Life in Digital Capitalism*, 2014. str. 89 – 90; i Zuboff, „Big Other“ (navedeno u prethodnoj bilješci 3).

<sup>39</sup> Mišljenje 05/2014 o tehnikama anonimizacije usvojeno 10. travnja 2014. (Radna skupina 216.)

<sup>40</sup> Za usko izuzeće od pravila za zaštitu podataka isključivo u osobne ili kućanske svrhe vidjeti Presudu slučaja Suda Europske unije C-212/13 *František Ryneš v Úřad pro ochranu osobních údajů*.

<sup>41</sup> Pojam protrošač skovao je Alvin Toffler u *Trećem valu*, 1980. Za raspravu o „protrošačkom okruženju“ i kako ga treba regulirati vidjeti Ian Brown i Chris Marsden, *Regulating Code*, 2013.

<sup>42</sup> Mišljenje Europske skupine za etiku u znanosti i novim tehnologijama Europskoj komisiji: Etika sigurnosti i tehnologije za nadziranje, mišljenje br. 28, 20. 5. 2015., str. 74.

<sup>43</sup> Vidjeti primjerice, Homer Economicus: *The Simpsons and Economics*, ur. Joshua Hall, 2014.

<sup>44</sup> Prema najkonzervativnijoj definiciji pogreške, to znači da 23 milijuna Amerikanaca ima značajne pogreške u izvješćima potrošača. Pet posto sudionika u istraživanju imalo je pogreške koje su, kada su ispravljene, poboljšale njihovu kreditnu ocjenu pa su mogli dobiti kredit po nižoj cijeni; Federalna trgovinska komisija, izvješće Kongresu prema odjeljku 319 Zakona o poštenim i točnim kreditnim transakcijama iz 2003., prosinac 2012; Chris Jay Hoofnagle, *How the Fair Credit Reporting Act Regulates Big Data* (10. rujna 2013.). Radionica foruma za budućnost privatnosti (Future of Privacy Forum) o velikoj količini podataka i privatnosti: *Making Ends Meet* (Spajanje kraja s krajem), 2013. Dostupno na SSRN: <http://ssrn.com/abstract=2432955>.

<sup>45</sup> Svjetski gospodarski forum (WEF) predstavlja podatke kao vrijednu imovinu pojedinca čija se prava posjedovanja, uporabe i zbrinjavanja mogu predati poduzećima i vladama u zamjenu za usluge. Također vidjeti najnovije govore potpredsjednika Komisije Ansipa, na primjer 7. 9. 2015. na godišnjem sastanku u institutu Bruegel pod nazivom „Produktivnost, inovacija i digitalizacija – koji izazovi globalne politike?“. „Vlasništvo i upravljanje protocima podataka, uporabom i ponovnom uporabom podataka. Upravljanje i pohranjivanje podataka. Oni podržavaju važne sektore u nastajanju poput računalstva u oblaku, interneta stvari i obrade velikih količina podataka“.

<sup>46</sup> „Tko, dakle, ima pravo na korištenje informacijama i podacima koji ne pripadaju zaista nama samima? To je pitanje koje nadilazi granice trgovine, etike i morala, što dovodi do pitanja privatnosti i zaštite privatnosti“; Al-Khouri studeni 2012., [http://www.academia.edu/6726887/Data\\_Ownership\\_Who\\_Owns\\_My\\_Data\\_036](http://www.academia.edu/6726887/Data_Ownership_Who_Owns_My_Data_036). Vidjeti također Margaret Jane Radin, *Incomplete Commodification in the Computerized World*, u *The Commodification of Information* 3, 17, Niva Elkin-Koren i Neil Weinstock Netanel ur. 2002.: „Od iznimne je važnosti promatra li se privatnost kao ljudsko pravo koje se pripisuje ljudima na temelju njihove osobnosti, ili kao pravo vlasništva, nešto što može biti u nečijem vlasništvu i pod nečijom kontrolom. Ljudska su prava vjerojatno neotuđiva od tržišta, dok su prava vlasništva vjerojatno otuđiva od tržišta“.

<sup>47</sup> Cilj je projekta *Crosscloud* MIT-ovog Laboratorija za računalnu znanost i umjetnu inteligenciju koji podržava nekoliko poduzeća sa sjedištem u Europskoj uniji „1) olakšati razvoj višekorisničke („društvene“) programske opreme samo s pomoću razvojnog okruženja i uz poštivanje prava i privatnosti korisnika. I 2) omogućiti korisnicima slobodu da se lako prebacuju između aplikacija, hardverskih platformi i društvenih mreža, uz čuvanje njihovih podataka i društvenih veza“; <http://openpds.media.mit.edu/#architecture> (pristupljeno 10. 9. 2015.).

<sup>48</sup> Vidjeti objašnjenje uz članak 1. Povelje o temeljnim pravima.

---

<sup>49</sup> Martha Nussbaum, Objectification, u *Philosophy and Public Affairs* 24. 4. 1995.

<sup>50</sup> Presuda od 15. prosinca 1983., BVerfGE 65, 1 – 71, Volkszählung.

<sup>51</sup> Vidjeti Europsku skupinu za etiku u znanosti i novim tehnologijama, Mišljenje o etici i nadzoru, str. 75. Istraživanje je pokazalo da je algoritam za ciljano oglašavanje diskriminirajući; pretraživanjem se u prosjeku nailazi na oglase za bolje plaćene poslove za muškarce u usporedbi sa ženama koje posjećuju stranice s poslovima; Sveučilište Carnegie Mellon i Međunarodni institut za računalnu znanost (ICSI). Za sklonost da se digitalnim asistentima po defaultu daje ženski glas vidjeti primjerice Judy Wajcman, *Feminist theories of technology*. *Cambridge Journal of Economics*, 34 (1). str. 143 – 152, 2010.

<sup>52</sup> Giorgio Agamben, *State of Exemption*, 2005.

<sup>53</sup> Neil Richards, Neil i Jonathan King, *Big Data Ethics* (19. svibnja 2014.), *Wake Forest Law Review*, 2014.

<sup>54</sup> BBC, novinari „psi čuvari” (*watchdog*) istražuju „dobrotvornu prodaju podataka”, 1. 9. 2015.

<sup>55</sup> Vidjeti pismo organizacije Future of Life Institute. Papinska enciklika „Laudato Si’”: „kada mediji i digitalni svijet postanu sveprisutni, zbog njihovog će utjecaja ljudi prestati učiti kako mudro živjeti, duboko razmišljati i velikodušno voljeti. U tom kontekstu postoji opasnost da će veliki mudraci iz prošlosti postati nepoznati uslijed buke i ometanja koja su rezultat preopterećenja informacijama. Potreban je trud kako bi se pomoglo ovim medijima da postanu izvor novog kulturnog napretka za čovječanstvo, a ne prijetnja našim najvećim bogatstvima. Istinska mudrost, kao plod samoispitivanja, dijaloga i velikodušnog susreta između osoba, ne stječe se pukim prikupljanjem podataka koje na kraju rezultira preopterećenjem i zbunjenošću, nekom vrstom mentalnog zagađenja. Stvarne odnose s drugima, sa svim izazovima koje podrazumijevaju, sada je zamijenila neka vrsta internetske komunikacije koja nam omogućuje da hirovito biramo ili eliminiramo odnose, što omogućuje razvoj nove vrste neprirodne emocije koja ima više veze s uređajima i zaslonima, nego s drugim ljudima i prirodom. Današnjim nam mediji doista omogućuju da komuniciramo i podijelimo svoje znanje i osjećaje. Pa ipak, povremeno nas također štite od izravnog kontakta s boli, strahovima i radostima drugih te kompleksnosti njihovih osobnih iskustava. Iz tog razloga, trebali bismo biti zabrinuti što se, uz uzbudljive mogućnosti koje ovi mediji nude, mogu pojaviti i duboko te melankolično nezadovoljstvo međuljudskim odnosima ili štetan osjećaj izolacije”.

<sup>56</sup> Vidjeti Akciju 4 Strategije EDPS-a 2015 – 2020 koja razvija etičke dimenzije za zaštitu podataka.