EUROPEAN DATA PROTECTION SUPERVISOR

# Mnenje 4/2015

# Novi digitalni etiki naproti:

***podatki, dostojanstvo in tehnologija***


11. september 2015

*Evropski nadzornik za varstvo podatkov (ENVP) je neodvisna institucija EU, ki je v skladu s členom 41(2) Uredbe št. 45/2001 „v zvezi z obdelavo osebnih podatkov" odgovorna „[…] za zagotovitev, da institucije in organi Skupnosti spoštujejo temeljne pravice in svoboščine fizičnih oseb ter predvsem njihovo pravico do zasebnosti" ter „[…] za svetovanje institucijam in organom Skupnosti ter posameznikom, na katere se nanašajo osebni podatki, o vseh zadevah v zvezi z obdelavo osebnih podatkov". Skupaj s svojim pomočnikom je bil imenovan decembra 2014 s posebnim poslanstvom, in sicer biti konstruktivnejši in proaktivnejši. ENVP je marca 2015 objavil petletno strategijo, v kateri je opisano, kako namerava uresničevati to poslanstvo in za to odgovarjati.*

*To mnenje je nadaljevanje prejšnjega mnenja ENVP o splošni uredbi o varstvu podatkov, katerega namen je bil pomagati glavnim institucijam EU, da dosežejo ustrezno soglasje o izvedljivem in v prihodnost naravnem nizu pravil, ki krepijo pravice in svoboščine posameznika. Kot v mnenju o mobilnem zdravju z začetka leta 2015 se tudi v tem mnenju obravnava izziv „digitalizacije" pri varstvu podatkov, ki je tretji cilj strategije ENVP – „prilagoditev obstoječih načel varstva podatkov svetovni digitalni areni", tudi zaradi načrtov EU za enotni digitalni trg. Skladno je s pristopom delovne skupine iz člena 29 v zvezi z vidiki varstva podatkov, ki jih vključuje uporaba novih tehnologij, kot je „internet stvari", h kateremu je kot redni član te skupine prispeval tudi ENVP.*


| | |
|---|---|
| Dignity | Dostojanstvo |
| Future-oriented rules and enforcement | V prihodnost naravnana pravila in ukrepi |
| Accountable controllers | Odgovorni nadzorniki |
| Empowered individuals | Okrepljena vloga posameznika |
| Innovative privacy engineering | Inovativni inženiring zasebnosti |
| Ethics | Etičnost |

**„Človekovo dostojanstvo je nedotakljivo. Treba ga je spoštovati in varovati.“**

**Člen 1,** Listina EU o temeljnih pravicah

**Za varstvo človekovega dostojanstva nista bili še nikoli tako pomembni temeljni pravici do zasebnosti in do varstva osebnih podatkov.** Zapisani sta v pogodbah EU in Listini EU o temeljnih pravicah. Posameznikom omogočata, da razvijajo svojo osebnost, živijo neodvisno življenje, so inovativni ter uveljavljajo druge pravice in svoboščine. Načela varstva podatkov, ki so opredeljena v Listini EU – nujnost, sorazmernost, pravičnost, zmanjšanje količine podatkov, omejitev namena, soglasje in preglednost –, se uporabljajo za celoten postopek obdelave podatkov, tudi za zbiranje in uporabo.

**Tehnologija ne sme narekovati vrednot in pravic, niti ne sme njihovega odnosa omejiti na lažno dihotomijo.** Digitalna revolucija prinaša ugodnosti za zdravje, okolje, mednarodni razvoj in gospodarsko učinkovitost. V načrtih EU za enotni digitalni trg se šteje, da so računalništvo v oblaku, „internet stvari“, masovni podatki in druge tehnologije ključni za konkurenčnost in rast. Poslovni modeli izkoriščajo nove zmožnosti za obsežno zbiranje, takojšnji prenos, združevanje in ponovno uporabo osebnih podatkov za nepredvidene namene, podlaga zanje pa so dolge in težko razumljive politike glede varovanja zasebnosti. To je še dodatno obremenilo načela varstva podatkov, zato je potreben svež razmislek o načinu njihove uporabe.

**V današnjem digitalnem okolju spoštovanje zakonodaje ni dovolj, upoštevati je treba tudi etično razsežnost obdelave podatkov.** Regulativni okvir EU že dopušča prostor za prožne odločitve in zaščitne ukrepe, ki se med obravnavo osebnih podatkov sprejemajo za vsak primer posebej. Reforma regulativnega okvira pomeni velik korak naprej. Vendar se postavljajo globlja vprašanja glede vpliva, ki ga imajo težnje v podatkovni družbi na dostojanstvo, osebno svobodo in delovanje demokracije.

**Ta vprašanja imajo inženirske, filozofske, pravne in moralne posledice.** V tem mnenju so izpostavljeni nekateri pomembni tehnološki vidiki, ki lahko vključujejo nesprejemljivo obdelavo osebnih podatkov ali posegajo v pravico do zasebnosti. V njem je opisan štiristopenjski „ekosistem za varstvo masovnih podatkov“ kot odziv na digitalni izziv: skupno prizadevanje, ki temelji na etičnih premislekih.

(1) V prihodnost naravnana zakonska ureditev obdelave podatkov ter spoštovanje pravic do zasebnosti in varstva podatkov.

(2) Odgovorni nadzorniki, ki vplivajo na obdelavo osebnih podatkov.

(3) Inženiring in zasnova orodij in storitev obdelave podatkov, ki upoštevata vidik zasebnosti.

(4) Okrepljena vloga posameznika.

**Evropski nadzornik za varstvo podatkov želi spodbuditi odprto in informirano razpravo v EU in zunaj nje**, v kateri bodo sodelovali civilna družba, oblikovalci, podjetja, akademski krogi ter javni in regulativni organi. Novi odbor EU za etično obdelavo podatkov, ki ga bomo ustanovili pri ENVP, bo prispeval k opredelitvi nove digitalne etičnosti, kar bo omogočilo boljše izkoriščanje tehnoloških prednosti za družbo in gospodarstvo, in sicer na načine, ki krepijo pravice in svoboščine posameznikov.

# KAZALO

# 1. Podatki vsepovsod: težnje, priložnosti in izzivi

Vedno večje količine osebnih podatkov se zbirajo in obdelujejo čedalje bolj nepregledno in zapleteno. S postopnim uvajanjem računalnikov v podjetja in javne uprave v osemdesetih letih prejšnjega stoletja se je razširilo prepričanje, da so prakse mogočnih vlad in korporacij pri obdelavi osebnih podatkov vodile v omejitev vloge posameznikov na le subjekte, na katere se osebni podatki nanašajo, pri čemer so bile ogrožene temeljne pravice in svoboščine. Zdajšnjo integrirano informacijsko in komunikacijsko tehnologijo pa od prejšnjih pristopov ločita njena splošna razširjenost in moč.

Lani so poročali, da je bilo na svetu več priključenih naprav kot ljudi.[1] Izboljšanje procesorske zmogljivosti[2] ter večji shramba in pasovna širina prenosa pomenijo, da je pri obdelavi osebnih podatkov čedalje manj tehničnih omejitev. Pričakuje se, da se bosta „internet stvari“ in analitika masovnih podatkov približala umetni inteligenci, obdelavi naravnega jezika in biometričnim sistemom, da bi se okrepila moč aplikacij s sposobnostjo strojnega učenja za napredno inteligenco. Vlade in podjetja lahko storijo korak naprej od „podatkovnega rudarjenja“ do „družbenostnega rudarjenja“, ki zajema vsakdanje izkušnje, komunikacije in celo misli.[3] Ob tem ko se družba prilagaja zahtevam digitalnega trga, se znova pojavljajo prizadevanja, da se otroci učijo o programiranju.[4] Izkoriščanje teh teženj na področju, na katerem je EU vodilna porabnica, vendar zaostaja pri zagotavljanju teh storitev, je pogosta tematika strategije Evropske komisije za enotni digitalni trg.[5]

Te težnje in številni pojmi, ki se uporabljajo danes, so kljub svoji veljavi nenatančni in se prekrivajo. Da bi pomagali spodbuditi razpravo, želimo nekatere težnje kljub njihovi očitni neizčrpnosti izpostaviti, saj po našem mnenju odpirajo najpomembnejša etična in praktična vprašanja v zvezi z uporabo načel varstva podatkov.

## 1.1 Masovni podatki

„Masovni podatki“[6] se nanašajo na prakso združevanja velikih količin podatkov iz različnih virov in njihovo analizo, pri čemer se pogosto uporabljajo algoritmi samostojnega učenja za informirane odločitve. Ti podatki niso vedno osebni: podatki, pridobljeni s senzorji za spremljanje naravnih ali atmosferskih pojavov, na primer vremena ali onesnaževanja, ali za spremljanje tehničnih vidikov proizvodnih postopkov, se ne nanašajo na „določeno ali določljivo fizično osebo“.[7] Toda ena od največjih vrednosti masovnih podatkov za podjetja in vlade izhaja iz spremljanja vedenja *ljudi*, kolektivno in individualno, in temelji na njegovi predvidljivi zmogljivosti.[8]

Eden od rezultatov je oblikovanje modela za zagotavljanje donosnosti spletnih podjetij, ki temeljijo na spremljanju spletne dejavnosti za optimiziranje ekonomske vrednosti transakcij ponudnikom storitev, in to ne le v ciljnem oglaševanju, ampak tudi po pogojih in premijskih stopnjah zavarovalnih polic, posojil in drugih pogodbenih razmerij. Na trgu tekmovalnosti za pozornost potrošnikov se večina ljudi ne zaveda širokega obsega tega spremljanja.[9] Taki „masovni podatki“ se morajo šteti kot osebni, kljub uporabi tehnik anonimizacije: čedalje lažje je ugotoviti posameznikovo identiteto na podlagi združevanja domnevno „anonimnih“ podatkov z drugimi podatkovnimi nizi, vključno z javno dostopnimi informacijami, na primer v družbenih omrežjih.[10] Kadar se s temi podatki trguje, posebno čez meje in območja pristojnosti, odgovornost za obdelavo informacij postane nejasna in jo je težko ugotoviti ali uveljaviti skladno z zakonodajo o varstvu podatkov, še posebno ob odsotnosti kakršnih koli mednarodnih standardov.

## 1.2 „Internet stvari“

Številne naprave, povezane v splet, so že običajne, na primer pametni telefoni, tablični računalniki ter bankomati in naprave za prijavo za let. Do leta 2020 naj bi povezanost v splet postala običajna, povezanih pa naj bi bilo 25 milijard predmetov (za primerjavo: leta 2015 jih je bilo 4,8 milijarde), in to od telemedicine do vozil, od pametnih merilnikov do zelo raznovrstnih novih nepremičnih in premičnih naprav, da se omogočijo pametna mesta.[11]

Ti senzorji bodo zagotovili takojšnje in urejene informacije, do katerih statistični uradi in raziskave trenutno nimajo dostopa, pri tem pa ni nujno, da so točnejše in so lahko celo zavajajoče.[12] S predvidenimi 1,8 milijarde samodejnih povezav med stroji do leta 2022 bi lahko zmanjšali število nesreč in onesnaževanje, povečali produktivnost in izboljšali samostojnost starejših in invalidov.[13] „Nosljive naprave“, na primer oblačila in ure, bodo osebne podatke obdelovale tako kot druge povezane naprave. Lahko bodo zaznali krvne strdke in spremljali splošno počutje in celjenje ran, povezane tkanine pa bi lahko ščitile v izjemnih okoliščinah, na primer kot oprema za gašenje požarov. Te naprave bodo osebne podatke naložile neposredno v shrambo v oblaku, ki je povezana v družbena omrežja, od tod bodo podatki javno dostopni in bodo omogočali prepoznavanje uporabnikov ter spremljanje vedênja in gibanja posameznikov in večjih skupin.[14]

Način obravnave teh informacij bi lahko vplival na zasebnost uporabnikov naprav, tudi kadar se te uporabljajo na delovnem mestu, in na pravice drugih posameznikov, ki jih naprava opazuje in snema. Čeprav je malo dokazov o dejanski diskriminaciji, je jasno, da je velik obseg osebnih podatkov, ki jih zbira „internet stvari“, zelo pomemben kot sredstvo za povečanje prihodkov, in sicer z bolj posamezniku prilagojenimi cenami, skladno z zaznanim vedênjem, zlasti v sektorju zdravstvenega zavarovanja.[15] Preverila se bodo tudi druga pravila, značilna za zadevno področje, na primer za naprave, ki vključujejo obdelavo zdravstvenih podatkov, niso tehnično opredeljene kot medicinski pripomočki in ne spadajo na področje uporabe uredbe.[16]

## 1.3 Okoljsko računalništvo

**Okoljsko ali nevidno računalništvo** se nanaša na ključno tehnologijo, na kateri temelji „internet stvari“. Ena od njegovih najbolj očitnih aplikacij so „pametne hiše“ in „pametni poslovni prostori“, ki jih sestavljajo naprave z vgrajeno izjemno razvito zmogljivostjo za obdelavo podatkov, ki obetajo večjo energetsko učinkovitost in bolj ozaveščene posameznike, sposobne vplivati na svojo porabo na daljavo (čeprav bi bila ta odvisna od neodvisnosti rezidenta od najemodajalca ali upravitelja stavbe). Treba bo razjasniti, kdo je odgovoren za namen in sredstva obdelave osebnih podatkov, vključenih v aplikacije okoljskega računalništva, ne le za zaščito temeljnih pravic posameznikov, ampak tudi za ustrezno porazdelitev odgovornosti za zagotavljanje spoštovanja splošnih zahtev sistemske varnosti.

## 1.4 Računalništvo v oblaku

Računalništvo v oblaku je znano kot osrednja omogočitvena tehnologija za napredno analitiko in zmogljivosti rudarjenja, zbiranje in analizo masovnih podatkov ter pretok podatkov iz „interneta stvari“, kar trenutno uporablja približno petina posameznikov in podjetij v EU.[17] Omogoča združevanje podatkov iz številnih naprav „interneta stvari“ ter je odvisno od razpoložljivosti in povezljivosti ogromnih količin podatkov v velikih obratih za

shranjevanje in obdelavo po vsem svetu.[18] To, da bosta računalništvo v oblaku[19] širše sprejela zasebni in javni sektor, bi po ocenah lahko k bruto domačemu proizvodu EU-28 prispevalo skupaj 449 milijard EUR (0,71 % celotnega bruto domačega proizvoda EU).

Nadzor nad osebnimi podatki se pogosto deli med stranko in ponudnikom storitev v oblaku, odgovornost glede obveznosti za varstvo podatkov pa ni vedno jasna. To bi lahko pomenilo, da v praksi prevladuje nezadostna zaščita. Te obveznosti niso odvisne od **fizične lokacije shranjevanja podatkov**. **In ne samo to:** čeprav je v ozadju le tehnologija, ki podpira poslovne aplikacije, lahko prav infrastruktura računalništva v oblaku postane kritična infrastruktura in poveča neskladja v tržni moči, saj je namreč 30 % podjetij nedavno trdilo, da imajo težave pri odjavi ali zamenjavi ponudnika.[20]

### 1.5 Poslovni modeli, ki temeljijo na osebnih podatkih

Te tehnologije so omogočile nove poslovne modele, ki temeljijo na informacijah, zbranih z zagotavljanjem storitev in iz drugih virov, na primer s prisotnostjo v družbenih omrežjih za oceno tveganja in kreditne sposobnosti ter za povečanje prihodkov. Pomemben poslovni model danes zaznamujejo platforme, ki povezujejo prodajalce in kupce ter tako omogočajo izmenjavo in prerazporeditev izdelkov, storitev, spretnosti in znanja in sredstev. Pogosto se označujejo kot „ekonomija delitve“, „skupna poraba“ ali spletne in mobilne vzajemne poslovne platforme,[21] te platforme pa lahko omogočajo klasične gospodarske učinkovitosti, spodbujajo konkurenčnost na trgih in zmanjšajo količine odpadkov. Ocenjuje se, da se bo njihova svetovna vrednost v naslednjih letih povečala za štirikrat, s 26 na 110 milijard USD.[22] Tovrstni poslovni modeli, ki temeljijo na osebnih podatkih, že ustvarjajo ogromne prihodke na področjih skupne uporabe avtomobilov, najema domov, finančne tehnologije in socialnega kreditiranja. Iz izsledkov raziskav je razvidno, da potrošniki cenijo njihovo navidezno večjo dostopnost in uporabnost.[23]

Vrednost takih platform so običajno uporabnikov ugled, strokovne recenzije in preverjanje identitete. To se lahko po možnosti razume kot izboljšanje preglednosti in odgovornosti, vendar ne nujno v razmerju do ponudnika platforme. Velikim deležnikom na teh trgih so oporekali domnevno zadrževanje podatkov o ugledu od posameznih uporabnikov, na katere so se podatki nanašali. Obstaja veliko tveganje, da bi se posameznikom storitve odrekle zaradi ugleda, in to na podlagi netočnih podatkov, ki jih ne morejo izpodbijati ali zahtevati, da se izbrišejo. Opiranje na podatke iz več virov tudi vzbuja dvom glede načela v zakonodaji EU o zmanjšanju količine podatkov. Glede obsega vpliva teh in prihodnjih tehnološko podprtih poslovnih modelov na posameznike in družbo v prihodnje je nujen temeljit premislek.[24]

### 1.6 Brezpilotna letala in samostojna vozila

Brezpilotna letala ali delno samostojni zrakoplovi se trenutno uporabljajo predvsem v vojaške namene, čedalje pogosteje pa se uporabljajo za namene nadzora, kartiranja, prevoza, logistike in javne varnosti, na primer pri silovitih požarih.[25] Fotografije, videoposnetki in drugi osebni podatki, zbrani z brezpilotnimi letali, se lahko izmenjujejo v telekomunikacijskih omrežjih. Njihova uporaba pomeni tveganje resnega posega v zasebnost in negativen učinek na svobodo izražanja. Postavlja se vprašanje, kako je mogoče njihovo zasnovo in uporabo učinkovito urediti, da lahko posamezniki, na katere se osebni podatki nanašajo, uveljavljajo svoje pravice dostopa do podatkov, ki jih zajemajo te naprave.

Samostojna vozila ali vozila brez voznika bodo na terenu spremenila način uporabe in organiziranja posameznega potovanja, saj lahko zabrišejo razliko med zasebnim in javnim

prevozom. Ocenjuje se, da bo do leta 2035 v uporabi 12 milijonov popolnoma samostojnih in 18 milijonov delno samostojnih vozil, med prvimi pa jih bodo sprejeli v Evropi.[26] Algoritmi za usmerjanje avtomobilov bodo vplivali na odločitve, ki se lahko neposredno nanašajo na fizično integriteto in celo življenje ali smrt posameznikov, na primer z izbiro, programirano za primer neizogibnega trčenja. Očitna je tudi potreba po razjasnitvi, kdo je odgovoren in pristojen za nadzor podatkov in varnost podatkov, saj ti programi odpirajo številna etična vprašanja.

### 1.7 Težnje z morebitno večjim in dolgoročnejšim učinkom

**3D-biotiskanje** organskih predmetov, ki s primerki celic bolnikov in kolagenskih „bioobvez“ (tj. občutljivi podatki po zakonodaji EU) nanaša zaporedne vrstice živih celic, naj bi po predvidevanjih kmalu postalo na voljo.[27] Olajšalo bi ponudbo prilagojenih človeških anatomskih delov in bi bilo še posebno dragoceno na revnejših območjih in območjih, na katerih so se končali spopadi, po vsem svetu. Biotiskanje postavlja očitna vprašanja za medicinsko etiko, varovanje intelektualne lastnine in varstvo potrošnikov ter – glede na to, da se nanaša na obdelavo intimnih in občutljivih podatkov v zvezi z zdravjem posameznikov – za uporabo pravil o varstvu podatkov.

**Umetna inteligenca**, na primer robotika, se nanaša na tehnološke zahteve za samostojnost nepremičnih in premičnih strojev. Njihov napredek bo omogočal izjemne možnosti, ki bodo presegale njihovo zdajšnjo uporabo. Računalniki z globinskim pristopom k učenju se sami učijo nalog, in sicer z drobitvijo velikih količin podatkov, za kar uporabljajo (med drugim) nevronske mreže, ki naj bi posnemale možgane. Raziskovalci in podjetja si prizadevajo za izboljšanje nenadzorovanega učenja. Algoritmi lahko že razumejo in prevajajo jezike, prepoznajo slike, pišejo nove članke in analizirajo zdravstvene podatke.[28] V družbenih omrežjih se zberejo velike količine osebnih podatkov, ki so jih pred tem učinkovito označili sami posamezniki. To je lahko ena zadnjih kognitivnih izboljšav za izboljšanje sposobnosti človeških možganov, kot na primer papir ali abak ali integrirano v samostojne stroje oziroma robote, vendar zdaj je čas, da se proučijo širše posledice za posameznike in družbo.[29]

## 2. Ekosistem za varstvo masovnih podatkov

EU ima zdaj priložnost, da pokaže, kako lahko vlade, regulatorji, nadzorniki, oblikovalci, razvijalci in posamezniki bolje sodelujejo za okrepitev pravic in usmerjanje tehnoloških inovacij, a ne njihovo zaviranje. Gibanja, opisana v drugem razdelku, so po mnenju enega od komentatorjev „povečala razkorak med tem, kar je mogoče, in tem, kar je zakonsko dovoljeno“.[30] V nasprotju z nekaterimi trditvami sta zasebnost in varstvo podatkov temelj za trajnostno in dinamično digitalno okolje, ne ovira. Neodvisni organi za varstvo podatkov, kot je ENVP, imajo ključno vlogo, da ovržejo take mite in se odzovejo na resnične pomisleke posameznikov glede izgube nadzora nad lastnimi osebnimi podatki.[31]

Naslednja generacija osebnih podatkov bo posameznikom, na katere se podatki nanašajo, verjetno še manj dostopna. Odgovornost za oblikovanje trajnostnega enotnega digitalnega trga mora biti razpršena, a vzajemna, podobno kot ekosistem, pri čemer v interesu posameznika zahteva učinkovito interakcijo med razvijalci, podjetji in regulatorji. V tem razdelku predstavljamo prispevek teh štirih ključnih deležnikov.

### 2.1 V prihodnost usmerjena uredba

Nedavno smo pozvali EU, naj izkoristi svojo zgodovinsko priložnost za vzpostavitev preprostejših pravil za ravnanje z osebnimi podatki, ki bodo pomembna za celotno

generacijo.[32] Pogajanja o splošni uredbi o varstvu podatkov in direktivi za varstvo podatkov na področjih policije in pravosodja so skoraj pri koncu, pozornost pa se bo kmalu obrnila v prihodnost direktive o e-zasebnosti v elektronskih komunikacijah in v novo uredbo o tem, kako institucije in organi EU sami obdelujejo osebne podatke. Čeprav so ekonomski stroški zbiranja in shranjevanja podatkov skoraj zanemarljivi, bodo morali organi za varstvo podatkov ta pravila uveljaviti dosledno, da se prepreči „moralno tveganje“ pretirane obdelave podatkov.[33]

V strategiji za enotni digitalni trg se prepoznava povezava med nadzorom nad velikimi količinami podatkov in tržno močjo. Tudi v njej se uveljavlja prepričanje, izraženo v našem predhodnem mnenju o „zasebnosti in konkurenčnosti v dobi velikih podatkov“ iz leta 2014, glede potrebe po večji usklajenosti med regulatorji. EU že ima orodja za odpravo neravnovesja moči na digitalnem trgu: trenutni protimonopolni postopki Evropske komisije na primer potrjujejo prevlado mobilnih naprav za dostop do svetovnega spleta. Bolj celostno izvajanje je mogoče v okviru veljavnega pravnega okvira, na primer prek klirinške hiše EU za nadzorne organe, da se prouči, ali lahko posamezni primeri odpirajo vprašanja glede skladnosti s pravili konkurence, potrošnikov in varstva podatkov. Na primer:

- zahteva po večji preglednosti cen (gotovinsko ali kako drugače) storitev lahko zaznamuje in olajša analizo primerov konkurence[34] ter
- zaznavanje nepoštene cenovne diskriminacije na podlagi slabe kakovosti podatkov in nepoštenega profiliranja in korelacij.[35]

S tesnejšim dialog med regulatorji iz različnih sektorjev bi se lahko odzvali na čedalje več pozivov za globalna partnerstva, ki lahko ustvarijo „skupno jedro“ odprtih podatkov, v katerem se lahko pretakajo podatki in zamisli, kot so statistični podatki in zemljevidi, ter so javno dostopni in se izmenjujejo v javnem interesu, z manjšim tveganjem nadzora, pri tem pa se posameznikom omogoča večji vpliv na odločitve, ki jih zadevajo.[36]

### 2.2 Odgovorni nadzorniki

Odgovornost zahteva vzpostavitev notranjih politik in nadzornih sistemov, ki zagotavljajo skladnost in ustrezne dokaze, zlasti neodvisnim nadzornim organom.

Zavzemali smo se za odpravo birokracije v zvezi z zakonodajo o varstvu podatkov, in sicer z zmanjšanjem zahtev za nepotrebno dokumentacijo, da bi se povečale možnosti za odgovornejše pobude podjetij, tem pa bi podporo nudile smernice organov za varstvo podatkov. Načelo, da se morajo osebni podatki obdelovati le na načine, ki so združljivi s posebnimi nameni, za katere so bili zbrani, je poglavitno za spoštovanje legitimnih pričakovanj posameznikov. Na primer, kodeksi ravnanja, revizije, certificiranje, revizije in nova generacija pogodbenih klavzul in zavezujočih korporativnih pravil lahko pomagajo vzpostaviti trdno zaupanje v digitalni trg. Odgovorni za izročitev osebnih podatkov bi morali biti veliko bolj okretni in proaktivni ter opustiti tako imenovano težnjo „črna škatla“ tajnosti in nepreglednosti poslovnih praks, pri čemer pa od strank zahtevajo čedalje večjo preglednost.[37]

### 2.3 Inženiring, ki upošteva vidik zasebnosti

Človeška inovacija je bila vedno rezultat dejavnosti posameznih družbenih skupin in posebnih okoliščin, pri tem pa so se običajno izražale družbene norme časa.[38] Vendar

odločitve v zvezi s tehnološko zasnovo ne bi smele narekovati naših družbenih interakcij in zgradbe naših skupnosti, ampak bi morale podpirati naše vrednote in temeljne pravice.

EU bi morala pripraviti in spodbujati inženirske tehnike in metodologije, ki omogočajo uporabo tehnologij za obdelavo podatkov, da bi se v celoti spoštovali dostojanstvo in pravice posameznika. Sistemski in programski inženirji morajo razumeti in bolje izvajati načela vgrajene zasebnosti novih izdelkov in storitev, in sicer pri zasnovi in tehnologijah. Odgovornost je treba podpreti z več raziskavami metod in orodij ter njihovim razvojem za omogočanje natančnih revizij in ugotavljanje skladnosti nadzornikov in obdelovalcev s pravili, na primer z „označevanjem“ vsake enote osebnih podatkov z „metapodatki“, ki opisujejo zahteve varstva podatkov.

Inženirske rešitve bi morale okrepiti vlogo posameznikov, ki želijo z anonimnostjo ohraniti svojo zasebnost in svobodo. EU bi morala spodbujati oblikovanje in izvajanje algoritmov, ki skrijejo identitete in zbirajo podatke, da bi zaščitili posameznika in sočasno izkoristili predvidljivo moč podatkov.[39]

Danes moramo postaviti temelje za obravnavo teh nalog, tj. z združitvijo razvijalcev programov in strokovnjakov za varstvo podatkov z različnih področij v široke mreže, kakršna je na primer tehnična mreža za spletno zasebnost (Internet Privacy Engineering Network – IPEN), ki pripomorejo k plodni interdisciplinarni izmenjavi zamisli in pristopov.

### 2.4 Okrepljena vloga posameznika

Proizvajalec in potrošnik v enem

Posamezniki niso le pasivni objekti, ki potrebujejo zakonodajno zaščito proti izkoriščanju. Vzgibi po digitalizaciji, opisani zgoraj, prinašajo pozitivne možnosti za krepitev vloge posameznika. Ljudje zdaj na primer proizvajajo in uporabljajo vsebine in storitve ter se lahko čedalje bolj, podobno kot ponudniki storitev, štejejo kot vzajemno odgovorni za obdelavo osebnih podatkov, razen če gre za povsem „domačo“ uporabo[40] (za opis te razvojne spremembe je nastal pojem proizvajalca in potrošnika v enem – „protrošnik“ (ang. prosumer)).[41] Medtem pa virtualne valute uporabnikom zagotavljajo anonimnost in izogibanje preverjanju transakcij, ki ga izvajajo tretje osebe, ter tako znižujejo stroške transakcij pri čezmejnem plačevanju blaga in storitev. Po drugi strani anonimnost in narava teh virtualnih valut, pri čemer velja več pristojnosti (oziroma lahko rečemo odgovornosti), posameznike izpostavljata goljufijam in kriminalnim trgom, ki jih je težko odkriti in raziskati. Poleg dolžnosti regulatorjev, podjetij in inženirjev imajo tudi državljani odgovornost, da so pri sprejemanju odločitev na spletu in zunaj njega skrbni, pozorni, kritični in obveščeni.[42]

Soglasje

V nasprotju s tradicionalnim mišljenjem pa ni mogoče vsega človeškega vedênja razložiti z ekonomskimi načeli, skladno s katerimi se predvideva, da so ljudje popolnoma razumni in dojemljivi za gospodarske spodbude.[43] To je pomembno za prihodnjo vlogo posameznikovega soglasja za obdelavo osebnih podatkov o njem ali zanj. V skladu z zakonodajo EU soglasje ni edina zakonita podlaga za večino podatkovnih obdelav. Tudi v primerih, v katerih ima soglasje pomembno vlogo, se nadzorniki ne morejo izogniti svoji odgovornosti za to, kar storijo s podatki, zlasti kadar je bilo pridobljeno splošno soglasje k obdelavi podatkov za raznovrstne namene.

Nadzor in „lastništvo“ podatkov

Posamezniki morajo imeti možnost opozoriti na napake in nepravične predsodke, ki izhajajo iz logike, ki jo uporabljajo algoritmi za določitev predpostavk in napovedi. Za ponazoritev, v ZDA so v študiji skoraj 3 000 kreditnih poročil, ki vključujejo 1 000 potrošnikov, ugotovili, da jih je 26 odstotkov imelo težave s „stvarnimi“ napakami, ki so bile tako resne, da so vplivale na bonitetno oceno potrošnikov in s tem na stroške pridobitve kredita.[44]

Podatki se pogosto štejejo kot vir, tako kot nafta, s katerim se trguje, najbolje z enako dobro obveščenimi strankami transakcije.[45] Stranke ne dobijo pravičnega nadomestila za svoje osebne podatke, s katerimi se trguje, in nekateri zagovarjajo model lastništva podatkov. Absolutni nadzor nad osebnimi podatki je težko zagotoviti – postavljajo se še druga vprašanja, kot na primer javni interes ter pravice in svoboščine drugih. Nadzor je potreben, vendar ni zadosten.[46] Človeško dostojanstvo pa ostaja stalnica. V skladu z zakonodajo EU analogije lastništva ni mogoče uporabiti za osebne podatke, ki so neločljivo povezani s posameznimi osebnostmi. V zakonodaji EU o varstvu podatkov ni določbe, da bi se posameznik odpovedal tej temeljni pravici.

Druga možna metoda, ki bi posameznikom omogočila boljši nadzor nad lastnimi podatki, kdo lahko dostopa do njih in za kakšen namen, bi lahko bila uporaba trgovin osebnih podatkov ali „podatkovnih zakladnic“.[47] Pojem tovrstne „osebne trgovine“ zahteva varnostne mehanizme, ki zagotavljajo, da lahko do podatkov in le do tistih delov, za katere so pooblaščeni, dostopajo le tisti subjekti, ki so jih za to pooblastili posamezniki, na katere se osebni podatki nanašajo. Trgovine osebnih podatkov bi bile najučinkovitejše, kadar se nanašajo na aktualne in stalno posodobljene informacije, kot so geoprostorski podatki ali življenjski znaki. Poleg tehničnih zaščitnih ukrepov bi morali uporabniki podatkov spoštovati pravila o izmenjavi in uporabi podatkov. Konkurenčnost in možnost zamenjati storitev, ki jo uporablja, sta potrošnikova najučinkovitejša moč, da vpliva na trg storitev, ki so mu na voljo. Zagotavljanje prenosljivosti povezav, vključno z identifikatorji in kontaktnimi informacijami, je potrjeno močno orodje za konkurenco in je učinkovito znižalo cene za potrošnike po liberalizaciji telekomunikacijskega trga. Prenosljivost podatkov, tj. dejanska in praktična možnost prenosa večine posameznikovih lastnih podatkov od enega ponudnika storitev k drugemu, je učinkovito izhodišče za ustvarjanje pogojev za resnično možno izbiro potrošnika.

# 3. Dostojanstvo v središču nove digitalne etike

Gradnike tega digitalnega ekosistema mora podpreti etični okvir. ENVP meni, da bi boljše spoštovanje in varovanje človekovega dostojanstva lahko bila protiutež prodornemu nadzoru in nesimetričnosti moči, s katerima se zdaj spopada posameznik. To mora biti v središču nove digitalne etike.

## 3.1 Dostojanstvo in podatki

Ob vzponu industrijske revolucije v 18. in 19. stoletju si je gibanje za človekove pravice prizadevalo zagotoviti širšo družbeno dobro z zmanjšanjem ovir za spoštovanje posameznika. EU je z Listino o temeljnih pravicah in po sprejetju Splošne deklaracije o človekovih pravicah in Evropske konvencije o človekovih pravicah kot izhodišče sprejela nedotakljivost človekovega dostojanstva. Dostojanstvo človeka ni le temeljna pravica sama po sebi, je tudi temelj nadaljnjih svoboščin in pravic, vključno s pravicama do zasebnosti in varstva osebnih podatkov.[48] Kratenje dostojanstva lahko vključuje objektivizacijo, pri čemer se oseba obravnava kot orodje za izpolnitev namenov nekoga drugega.[49] Zasebnost je sestavni del

človekovega dostojanstva, pravica do varstva podatkov pa je bila prvotno zasnovana v sedemdesetih in osemdesetih letih prejšnjega stoletja, nekako v zameno za vdor v zasebnost in dostojanstvo z obsežno obdelavo osebnih podatkov. V Nemčiji je pravica do „samostojnega odločanja glede informacij“ temeljila na pravicah do osebnega dostojanstva in svobodnega razvoja osebnosti, kot je določeno v členih 1 in 2 nemške ustave.[50]

Vendar se v začetku 21. stoletja od posameznikov čedalje bolj zahteva, da prek spleta razkrijejo veliko več osebnih podatkov, da lahko sodelujejo v družbenih, upravnih in gospodarskih zadevah, pri čemer pa imajo vse manj možnosti za zavrnitev tega. Vse dejavnosti bodo po možnosti potekale vedno prek spleta, kar pomeni močan pritisk na pojem svobodne in informirane privolitve. „Digitalne drobtine“ se pojavijo vsako minuto in se združene v celoto uporabljajo za opredelitev posameznikov v realnem času, da se ustvari več profilov, med katerimi so nekateri tudi napačni. Ti profili se lahko razpošljejo v mikrosekundah brez vednosti posameznikov in se uporabljajo kot podlaga za pomembne odločitve, ki jih zadevajo.

Profili, ki se uporabljajo za napovedovanje vedênja ljudi, so pod pritiskom tveganja stigmatizacije, krepitve obstoječih stereotipov, družbenega in kulturnega razlikovanja in izključevanja,[51] tovrstna „kolektivna inteligenca“ pa ogroža posamezno izbiro in enake možnosti. Taki „filtrirani mehurčki“ ali „osebne zaprte celice“ lahko na koncu ovirajo ustvarjalnost, inovativnost ter pravici do izražanja ter zbiranja in združevanja, ki so omogočile, da so digitalne tehnologije zaživele.

Medtem se z nadaljnjim izrednim stanjem zaradi „varnosti“ upravičujejo večplastne vsiljive tehnike za spremljanje dejavnosti posameznikov.[52] Za razumevanje tega povečanega nadzora je potrebna dolgoročna perspektiva o skupnih učinkih na družbo in vedênje.

EU se mora skupaj s tretjimi državami resno osredotočiti na to, kako zagotoviti, da se te vrednote ne bodo upoštevale le na papirju, v kibernetskem prostoru pa bi se dejansko prezrle. Zlasti EU ima zdaj „kritično okno“ pred množičnim sprejetjem teh tehnologij, da uveljavi vrednote v digitalnih strukturah, ki bodo oblikovale našo družbo.[53] To zahteva novo presojo o tem, ali so morebitne koristi novih tehnologij resnično odvisne od zbiranja in analize informacij za določitev fizične osebe, zbranih od milijard posameznikov. Taka presoja bi lahko pomenila izziv za razvijalce, da bi razvili naprave, s katerimi bi se v realnem času anonimizirale velike količine nerazvrščenih informacij, kar bi otežilo ali onemogočilo izpostavljanje posameznika.

Zavedamo se, da morajo biti nekatere obdelave podatkov, na primer genetskih podatkov, ne le regulirane, ampak bi morali na primer odbori za etiko v povezavi z njimi proučiti morebitna širša družbena vprašanja. Genetski podatki se po svoji naravi nanašajo na nekega posameznika in njegove prednike in potomce. Genetski podatki se uporabljajo za ugotavljanje družinskih razmerij, poleg tega lahko elementi v genih nekega posameznika vsebujejo informacije o njegovih starših in otrocih, nadzorniki pa na njihovi podlagi sprejemajo odločitve, ki vplivajo na njihove možnosti v življenju še pred njihovim rojstvom. Morebitna koncentracija genetskih osebnih podatkov v rokah nekaj velikih tržnih deležnikov ima posledice za tržna gospodarstva in posameznike, na katere se osebni podatki nanašajo. Zaradi naraščajoče odvisnosti od globalnega sistema zbiranja in analize stalnega pretoka podatkov bi lahko bila družba in gospodarstvo bolj izpostavljena izjemnim varnostnim pomanjkljivostim in zlonamernim napadom.

Če ne bomo v prihodnosti razmišljali inovativno, bi lahko obstoječi okvir propadel. Čedalje večji sta zahteva in potreba, da se posameznik, na katerega se osebni podatki nanašajo, obravnava kot posameznik, ne pa le kot potrošnik ali uporabnik. Resnično neodvisni organi za varstvo podatkov imajo odločilno vlogo pri preprečevanju, da bi se posamezniki v prihodnosti opredeljevali z algoritmi in njihovimi nadaljnjimi različicami. Treba jih je ustrezno opremiti za izvajanje „skrbnega ravnanja“ v razmerju do posameznikov in njihovega dostojanstva v svetovnem spletu. Tradicionalni pojmi ter načela zasebnosti in varstva podatkov so že vsebovali etične vidike za zaščito dostojanstva, na primer na področjih zaposlovanja in zdravstva. Današnje težnje pa so odprle povsem nova vprašanja, zato je treba proučiti, ali so načela dovolj zanesljiva za digitalno dobo.[54] Pojem osebnih podatkov se bo zelo verjetno močno spremenil, saj tehnologija posameznikom čedalje bolj omogoča, da so na novo opredeljeni na podlagi domnevno anonimnih podatkov. Poleg tega bosta strojno učenje in združitev človeške in umetne inteligence oslabila posameznikove pravice in odgovornosti.

### 3.2 Evropski svetovalni odbor za etiko

Naš namen ni izrisovati alarmantne podobe distopije. Razprave že potekajo na pravnem, političnem, gospodarskem, družbenem, znanstvenem in celo verskem področju.[55] Preveč poenostavljajoči pristopi, ki dajejo enostransko prednost ekonomskemu dobičku ali nadzoru za varnost, verjetno niso nič bolj uporabni kot pretirano omejujoča uporaba veljavne zakonodaje, ki zavira inovativnost in napredek. ENVP zato predlaga temeljito, široko in multidisciplinarno analizo, na podlagi katere bi se zbrala priporočila, in informirano družbeno razpravo o tem, kako naj se svobodna demokratična družba spopade s tehnološkim izzivom.

Strategija ENVP[56] pozornost namenja razvoju etičnega pristopa do varstva podatkov ter priznava, da „izvedljivo, koristno ali dobičkonosno ni enakovredno trajnostnemu“ in poudarja „pomen odgovornosti nad tehnično skladnostjo s črko zakona“. Nameravamo preseči skupnosti uradnikov EU, pravnikov in strokovnjakov s področja IT ter pristopiti do uglednih oseb, ki so usposobljene za presojo srednje- do dolgoročnih posledic tehnoloških sprememb in regulativnih odzivov. V prihodnjih mesecih bomo v naši neodvisni instituciji ustanovili zunanjo svetovalno skupino za etične razsežnosti varstva podatkov, ki bo raziskovala razmerja med človekovimi pravicami, tehnologijo, trgi in poslovnimi modeli v 21. stoletju.

Naš svetovalni odbor za etiko bo sestavljen iz izbrane skupine uglednih oseb s področij etike in filozofije, sociologije, psihologije, tehnologije in ekonomije, po potrebi pa mu bodo podporo nudili dodatni strokovnjaki z znanjem in strokovnimi izkušnjami na področjih, kot so zdravstvo, promet in energija, družbeni odnosi in mediji, ekonomija in finance, upravljanje in demokracija ter varnost in policija. Povabljeni bodo k proučitvi širših etičnih posledic na to, kako se osebni podatki zbirajo in uporabljajo, njihovo razpravljanje pa bo kar najbolj pregledno.

## 4. Sklepna ugotovitev: čas je za poglobljeno razpravo

Zasebnost in varstvo podatkov sta del rešitve, ne težava. Za zdaj je človek tisti, ki nadzira tehnologijo. Te možne razvojne spremembe je težko urejeno razvrščati na dobre ali slabe, zaželene ali slabe, koristne ali škodljive, še posebno, kadar je treba v istem okviru hkrati upoštevati več morebitnih teženj. Oblikovalci politik, razvijalci tehnologij, nosilci poslovnega razvoja in vsi mi moramo resno razmisliti, ali in kako želimo vplivati na razvoj tehnologije in njeno uporabo. Enako pomembno je, da EU nujno obravnava etične zadržke in prostor, ki ga je treba človeškemu dostojanstvu zagotoviti v tehnologijah prihodnosti.

Načela varstva podatkov dokazano varujejo posameznike in njihovo zasebnost pred tveganji neodgovorne obdelave podatkov. Vendar bo sedanji razvoj stanja morda zahteval povsem svež pristop. Zato odpiramo novo razpravo o zadostnem obsegu uporabe načel, kot sta pravičnost in zakonitost. Organi na področju varstva podatkov lahko prevzamejo novo vlogo tako, da uporabijo obstoječa orodja, kot so predhodna preverjanja in dovoljenja, saj za nadzor take obdelave podatkov niso usposobljeni nobeni drugi organi. Zaradi bliskovitega razvoja tehnologije, globalne inovativnosti in človeške povezanosti imamo priložnost, da pritegnemo pozornost, vzbudimo zanimanje in vzpostavimo soglasje.

Upamo, da bo to mnenje zagotovilo okvir za obsežnejšo in bolj poglobljeno razpravo o tem, kako lahko EU hkrati omogoči celovitost svojih vrednot in prinese koristi novih tehnologij.

V Bruslju, 11. septembra 2015

(**podpis**)

Giovanni BUTTARELLI
Evropski nadzornik za varstvo podatkov

# Opombe

[1] Vir: GSMA Intelligence.

[2] „Moorov zakon“, po katerem se število tranzistorjev, ki jih je mogoče spraviti na mikročip, podvoji vsakih 18 mesecev, na splošno drži. Moore, Gordon E. (19. 4. 1965). „Cramming more components onto integrated circuits“, Electronics. 22. 8. 2011.

[3] Nathan Eagle, Alex (Sandy) Pentland, „Reality mining: sensing complex social systems“, zbornik Personal and Ubiquitous Computing, letnik 10, št. izdaje 4, marec 2006, str. 255–268. Shoshana Zuboff v „Big Other: surveillance capitalism and the prospects of an information civilization“, Journal of Information Technology (2015) 30, str. 75–89, piše: „Kot rezultat prodorne računalniške komunikacije je skoraj vsak svetovni vidik v novi simbolni razsežnosti, dogodki, predmeti, postopki in ljudje pa postanejo opazni, znani in skupni vsem na nov način.“ S. Zuboff predvideva „vzpon nove univerzalne arhitekture“, ki jo imenuje „Veliki Drugi“, „vsesplošna shema omrežnih institucij, v okviru katere se snemajo, spreminjajo in komodificirajo vsakdanje izkušnje, od opekača do teles, od komunikacije do misli, vse z namenom oblikovanja novih poti do monetizacije in dobička“, str. 77, 81.

[4] „BBC Micro Bit computer's final design revealed“, 7. 7. 2015, http://www.bbc.com/news/technology-33409311 (dostop 10. 9. 2015); „No assembler required: How to teach computer science in nursery school“, The Economist, 1. 8. 2015.

[5] Nobeno od desetih najboljših podjetij v tehnološkem sektorju, merjeno po tržni vrednosti, nima sedeža v Evropski uniji (osem jih ima sedež v Združenih državah, eno na Kitajskem, eno pa na Tajvanu), kot je razvidno iz poročila PWC Global Top Ten Companies by Market Capitalisation, posodobljena različica z dne 31. marca 2015.

[6] „Masovni podatki se nanašajo na eksponentno rast dostopnosti in avtomatizirane uporabe podatkov: to so izjemno veliki digitalni podatkovni nizi korporacij, vlad in drugih velikih organizacij, ki se nato obširno analizirajo (od tod tudi ime: analitika) z računalniškimi algoritmi;“ Mnenje skupine iz člena 29 3/2013 o omejitvi namena. V poročilu Bele hiše iz leta 2014 se masovni podatki opisujejo kot „čedalje večja tehnološka sposobnost za zajemanje, zbiranje in obdelavo vse večjega obsega, hitrosti nastanka in raznovrstnosti podatkov“, glej Big Data: Seizing Opportunities, Preserving Values, Executive Office of the President („Podesta-report“), maj 2014.

[7] Skladno z zakonodajo EU „osebni podatki“ pomenijo „katero koli informacijo, ki se nanaša na določeno ali določljivo fizično osebo (‚posameznik, na katerega se nanašajo osebni podatki‘); določljiva oseba je tista, ki se lahko neposredno ali posredno identificira, predvsem s sklicevanjem na identifikacijsko številko ali na enega ali več dejavnikov, ki so značilni za njeno fizično, fiziološko, duševno, ekonomsko, kulturno ali socialno identiteto“; člen 2(a) Direktive 95/46/ES. Ta opredelitev je na splošno primerljiva z opredelitvijo Sveta Evrope v Konvenciji o varstvu posameznikov glede avtomatske obdelave osebnih podatkov (znana kot Konvencija št. 108) in z opredelitvijo v Smernicah OECD o varovanju zasebnosti in čezmejnem prenosu osebnih podatkov. Za poglobljeno analizo glej delovna skupina iz člena 29: „Mnenje št. 4/2007 o pojmu osebnih podatkov“, WP 136.

[8] Glej na primer govor predsednice Zvezne komisije za trgovino Združenih držav Amerike iz leta 2014: „Spodbujanje uvajanja povezanih naprav, znižanje stroška za zbiranje, shranjevanje in obdelavo podatkov ter sposobnost posrednikov podatkov in drugih za združevanje podatkov na spletu in zunaj njega pomeni, da lahko podjetja zbirajo pravzaprav neomejene količine podatkov o potrošnikih in jih shranjujejo neomejen čas. Na podlagi napovedne analize lahko iz teh podatkov o vsakomer od nas izvedo presenetljivo veliko.“ Uvodne besede predsednice Zvezne komisije za trgovino Edith Ramirez, „Big Data: A Tool for Inclusion or Exclusion?“, Washington, 15. september 2014. Kot pojasnjuje Sandy Pentland, je „družbena fizika kvantitativna družboslovna veda, ki opisuje zanesljive, matematične povezave med informacijami in pretokom zamisli na eni strani in vedênjem ljudi na drugi ... Z njo lahko predvidevamo produktivnost majhnih skupin, oddelkov v podjetjih in celo

celotnih mest“. To „je tisto, kar je potrebno, da bi nastali boljši družbeni sistemi“ (str. 4, 7) in „bi (vladnim uradnikom, vodilnim v podjetjih in državljanom) omogočilo uporabljati orodja za spodbujanje družbenega mreženja, da bi se *vzpostavile nove vedênjske norme*“ (str. 189) (naš poudarek); Pentland, *Social Physics: How Good Ideas Spread: The Lessons from a New Science*.

[9] Posebna raziskava Eurobarometra 431 o varstvu podatkov, junij 2015, in panelna raziskava Pew Research iz januarja 2014 o mnenju javnosti o zasebnosti in varnosti v obdobju po Snowdnovem razkritju. Kot kažejo izsledki raziskave, je ob povprečnem obisku enega spletnega mesta 56 primerov zbiranja podatkov, meni Julia Angwin v delu *Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance*, 2012). V poročilu Bele hiše iz leta 2014 o masovnih podatkih je navedeno, da „izjemni računalniška moč in razvitost [...] ustvarjata nesimetričnost moči med tistimi, ki imajo podatke, in tistimi, ki jih hote ali nehote dobavljajo“; „nekateri od največjih izzivov, izpostavljenih v tem intervjuju, pa se nanašajo na to, kako lahko analize masovnih podatkov [...] ustvarjajo nejasno okolje sprejemanja odločitev, v katerem se posameznikova samostojnost izgubi v nerazumljivem nizu algoritmov“.

[10] Na podlagi javnih anonimnih podatkov, zbranih s popisom leta 1990, bi 87 % prebivalcev Združenih držav lahko prepoznali na podlagi njihove petmestne poštne številke v kombinaciji s spolom in datumom rojstva; glej Paul Ohm: „Broken promises of privacy: responding to the surprising failure of anonymisation“, UCLA Law Review, 2010, in „Record linkage and privacy: issues in creating new federal research and statistical info“, april 2011. DNK je edinstvena (razen pri enojajčnih dvojčkih) in se ne spreminja vse življenje. Vsebuje informacije o etnični pripadnosti, nagnjenja k boleznim in z njo se lahko prepoznajo drugi družinski člani. Januarja 2013 je raziskovalcem uspelo na podlagi anonimnih podatkov o DNK iz javno dostopnih genealoških podatkovnih zbirk prepoznati posameznike in družinske člane; Gymrek, M., McGuire, A. L., Golan, D., Halperin, E. in Erlich, Y. *Science* 339, 321–324 (2013). Glej tudi „Poorly anonymized logs reveal NYC cab drivers' detailed whereabouts“, 23. 6. 2014, http://arstechnica.com/tech-policy/2014/06/poorly-anonymized-logs-reveal-nyc-cab-drivers-detailed-whereabouts/ (dostop 10. 9. 2015). Glej tudi Mnenje delovne skupine iz člena 29 št. 4/2007 o pojmu osebnih podatkov, Mnenje skupine iz člena 29 št. 3/2013 o omejitvi namena, Mnenje skupine iz člena 29 št. 6/2013 o odprtih podatkih in ponovni uporabi informacij javnega sektorja in Mnenje skupine iz člena 29 št. 5/2014 o anonimizaciji.

[11] Vir: Gartner.

[12] Glej na primer panelno razpravo „What is the future of official statistics in the Big Data era?“, Royal Statistical Society, London, 19. januar 2015, http://www.odi.org/events/4068-future-official-statistics-big-data-era (dostop 10. 9. 2015).

[13] Ten technologies which could change our lives: potential impacts and policy implications, Oddelek za znanstvene napovedi, Služba za parlamentarne raziskovalne storitve, januar 2015.

[14] Te razvojne spremembe podpira delovni program EU Obzorje 2020 za obdobje 2016–2017, vključno z obsežnimi pilotnimi projekti, ki bodo pozornost namenili zasebnosti in etičnim vprašanjem.

[15] Zavarovanje je opisano kot „izvorni poslovni model za internet stvari“, „From fitness trackers to drones, how the ‚Internet of Things‘ is transforming the insurance industry“, Business Insider, 11. 6. 2015. Diskriminacija pri cenah v konkurenčnem pravu, kot izhaja iz člena 102 PDEU in ki prevladujočemu podjetju na trgu prepoveduje „neposredno ali posredno določanje nepoštenih nakupnih ali prodajnih cen ali drugih nepoštenih pogojev poslovanja“, je močno sporna, glej na primer Damien Gerardin in Nicolas Petit: Price Discrimination Under EC Competition Law: Another Antitrust Theory in Search of Limiting Principles (julij 2005), Global Competition Law Centre, Working Paper, izdaja št. 7/2005. O masovnih podatkih in njihovi (po mnenju avtorjev še neizkoriščenem) zmogljivosti za spodbujanje posamezniku prilagojenega določanja cen glej Executive Office of the President of the United States: Big Data and Differential Pricing, februar 2015, in nedavno analizo, katere sklepna ugotovitev navaja, da posamezniku prilagojeno določanje

cen na splošno vključuje obdelavo osebnih podatkov in mora zato upoštevati načelo preglednosti iz zakonodaje o varstvu podatkov, po katerem morajo podjetja obvestiti ljudi o namenu obdelave njihovih osebnih podatkov: če podjetja posamezniku prilagajajo cene, morajo to tudi povedati. Če podjetje uporablja piškotke za prepoznavanje posameznikov, mora skladno z direktivo o e-zasebnosti obvestiti posameznika o namenu piškotkov, Frederik Borgesius: „Online Price Discrimination and Data Protection Law“, delovni osnutek. Dostopno na: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2652665 (dostop 10. 9. 2015).

[16] Medicinski pripomočki so opredeljeni v zakonodaji EU, in sicer v Direktivi Sveta 93/42/EGS o medicinskih pripomočkih, kakor je bila spremenjena z Direktivo 2007/47/ES Evropskega parlamenta in Sveta z dne 5. septembra 2007. O posledicah „mobilnega zdravja“ na varstvo podatkov glej Mnenje ENVP 1/2015.

[17] Po podatkih Eurostata 21 % posameznikov in 19 % podjetij v EU uporablja storitve shranjevanja v oblaku.

[18] „Če bi bil svetovni splet ena država, bi bila dvanajsta največja porabnica električne energije na svetu, približno med Španijo in Italijo. To pomeni približno 1,1 do 1,5 odstotka svetovne porabe električne energije (od leta 2010) in toplogrednih plinov, ki jih letno povzroča 70 do 90 velikih (500-megavatnih) premogovnih elektrarn.“ Natural Resources Defense Council, Data Centre Efficiency Assessment: Scaling Up Energy Efficiency Across the Data Centre Industry: Evaluating Key Drivers and Barriers, 2014.

[19] Poročilo o raziskavi „SMART 2013/0043 - Uptake of Cloud in Europe“.

[20] Vir: Eurostat.

[21] Izraz „ekonomija delitve“ se označuje kot zavajajoč: „Ekonomija delitve ne pomeni nikakršnega deljenja“, Giana M. Eckhardt in Fleura Bardhi, Harvard Business Review, 28. 1. 2015.

[22] Rachel Botsman in 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“, junij 2015.

[24] Glej delavnico Zvezne komisije za trgovino Združenih držav Amerike z dne 9. junija 2015 na temo „Competition, Consumer Protection, and Economic Issues Raised by the Sharing Economy“, https://www.ftc.gov/news-events/events-calendar/2015/06/sharing-economy-issues-facing-platforms-participants-regulators/ (dostop 10. 9. 2015).

[25] Glede posledic brezpilotnih letal ali daljinsko vodenih zračnih sistemov na varstvo podatkov glej mnenje ENVP o Sporočilu Komisije Evropskemu parlamentu in Svetu z naslovom „Nova doba letalstva – Odprtje letalskega trga za varno in trajnostno civilno uporabo daljinsko vodenih zračnih sistemov“, november 2014.

[26] Vir: Boston Consulting Group.

[27] Gartner.

[28] Facebookov algoritem za prepoznavo obrazov DeepFace ima po poročanju 97-odstotni uspeh in je učinkovitejši od ljudi, DeepFace: Closing the Gap to Human-Level Performance in Face Verification, objavljeno v poročilu na konferenci IEEE o računalniškem vidu in vzorcih prepoznavanja, junij 2014.

[29] Robo je bil opredeljen kot „stroj, ki je v svetu, ki občuti, misli in deluje“, Bekey, G.: Current trends in robotics: technology and ethics, in Robot Ethics - The ethical and social implications of robotics, MIT Press2, 2012, str. 18. Ocenjuje se, da se bo med letoma 2013 in 2016 prodalo 22 milijonov storitvenih robotov; IRF World Robotics Report, 2013. Glede umetne inteligence glej Rise of the Machines, Economist, 9. 5. 2015, in Pew Research Centre Internet Project, 2014. Podjetje, ki deluje na področju umetne inteligence in ga je leta 2014 prevzelo vodilno tehnološko podjetje, je prevzem

pogojevalo z ustanovitvijo odbora za etiko in varnostna vprašanja in s prepovedjo uporabe rezultatov dela umetne inteligence za vojaške ali obveščevalne namene, Forbes, Inside Google's Mysterious Ethics Board, 3. 2. 2014.

[30] Pentland: *Social physics*, str. 147.

[31] Glej opombo 9 zgoraj. Pentland: *Social Physics*, str. 153: „Veliki skoki na področjih zdravstvenega varstva, prevoza, energije in varnosti so res mogoči ..., glavne ovire za doseganje teh ciljev pa so pomisleki glede zasebnosti in dejstvo, da še vedno ni sklenjeno soglasje glede kompromisa med osebnimi in družbenimi vrednotami.“ Razprava glede pandemije ebole leta 2014 v Zahodni Afriki je nazoren primer, kako nastane napačno ločevanje med zasebnostjo posameznika in potrebami družbe. Bolezni so se spremljale in njihova življenjska doba se je merila z raziskavami in popisi, ki zelo hitro zastarajo in na podlagi katerih je težko predvideti, kje se bodo naslednjič pojavile. Obstaja nekaj primerov uporabe „masovnih podatkov“ za spremljanje izbruhov malarije v Namibiji in Keniji in za spremljanje učinkovitosti vladnih zdravstvenih opozoril v letu 2009 med mehiško krizo zaradi prašičje gripe. En vir podatkov je evidenca mobilnih klicev, iz katere je razvidno, kako bazna postaja obravnava klice in lahko v realnem času zagotovi grob približek lokacije ljudi in njihovega gibanja. Zbiranje vseh teh evidenc ni ciljno usmerjeno – ne more razlikovati med tistimi z ebolo ali brez nje. Švedska neprofitna organizacija je geografsko opredelila gibanje prebivalstva v Zahodni Afriki, vendar podatki niso bili uporabljeni, ker jih operaterji mobilne telefonije niso želeli izročiti pooblaščenim zunanjim raziskovalcem in so trdili, da potrebujejo vladna navodila, vlade pa so se sklicevale na pomisleke glede zasebnosti, ki je skladno z zakonodajo EU ni bilo mogoče zagotoviti, http://www.pri.org/stories/2014-10-24/how-big-data-could-help-stop-spread-ebola (dostop 10. 9. 2015).

[32] Mnenje ENVP 3/2015.

[33] Pri masovnih podatkih se domneva, da „N = vsi“ pomeni, da se upoštevajo vse podatkovne točke, ne le vzorec, Viktor Mayer-Schönberger in Kenneth Cukier: *The Rise of Big Data: How it's changing the way we think about the world*, 2013. Lizbonski svet in inštitut za progresivno politiko sta trdila, da se bo blaginja izboljšala s povečanjem „digitalne gostote“ – tj. „količine podatkov, uporabljenih na prebivalca v gospodarstvu“, http://www.lisboncouncil.net/component/downloads/?id=1178 (dostop 10. 9. 2015). Mednarodna delovna skupina o varstvu podatkov v telekomunikacijah (znana kot „berlinska skupina“) je za masovne podatke predlagala odstopanja od načel varstva podatkov, http://www.datenschutz-berlin.de/attachments/1052/WP_Big_Data_final_clean_675.48.12.pdf (dostop 10. 9. 2015). Svetovni gospodarski forum je pozval k osredotočenosti na uporabo in ne zbiranje ter k odmiku od zahteve glede soglasja za zbiranje osebnih podatkov, Unlocking the Value of Personal Data: From Collection to Usage, 2013.

[34] Glej predhodno mnenje ENVP o zasebnosti in konkurenčnosti v dobi velikih podatkov.

[35] Člen 21 Listine EU o temeljnih pravicah prepoveduje „kakršno koli diskriminacijo na podlagi spola, rase, barve kože, narodnostnega ali socialnega porekla, genetskih značilnosti, jezika, vere ali prepričanja, političnega ali drugega prepričanja, pripadnosti nacionalni manjšini, premoženja, rojstva, invalidnosti, starosti ali spolne usmerjenosti“. Številne od teh kategorij podatkov („ki razkrivajo rasno ali etnično poreklo, politično prepričanje, versko ali filozofsko prepričanje, članstvo v sindikatu in obdelavo podatkov v zvezi z zdravjem ali spolnim življenjem“) so skladno s členom 8 Direktive 95/46/ES dodatno zaščitene.

[36] Glede zamisli o digitalnem skupnem jedru glej Ambition numérique: Pour une politique française et européenne de la transition numérique, French Digital Council, junij 2015, str. 276; Bruce Schneier zagovarja, da se na svetovnem spletu ustvarijo „javni prostori brez lastnika“, kot na primer javni parki, *Data and Goliath*, str. 188–189; Sandy Pentland pa se zavzema za „skupno jedro javnih podatkov“, *Social Physics*, str. 179. Glede presoje varnosti objave zbirnih podatkovnih nizov kot odprtih podatkov glej Mnenje skupine iz člena 29 št. 6/2013 o odprtih podatkih in ponovni uporabi informacij javnega sektorja.

[37] „Während die Einzelnen immer transparenter werden, agieren viele Unternehmen hochgradig intransparent“, http://crackedlabs.org/studie-kommerzielle-ueberwachung/info. O ustrezni preglednosti glej na primer 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*, ur. Andrew Zimbalist, 1979. Glej tudi Judy Wacjman: *Pressed for Time: The Acceleration of Life in Digital Capitalism*, 2014, str. 89–90, in Zuboff: „Big Other“ (omenjen v opombi 3 zgoraj).

[39] Mnenje št. 5/2014 o anonimizacijskih tehnikah, sprejeto 10. aprila 2014 (WP 216).

[40] O ozki razlagi izjeme iz pravil o varstvu podatkov za izključno osebne ali domače namene glej sodbo Sodišča Evropske unije v zadevi C-212/13, *František Ryneš proti Úřad pro ochranu osobních údajů.*

[41] Avtor izraza prosumer (proizvajalec in potrošnik v enem) je Alvin Toffler: *The Third Wave*, 1980. Za razpravo o „proizvajalcu in potrošniku v enem – „protrošnik“ in o tem, kako naj bi bilo to urejeno, glej Ian Brown in Chris Marsden: *Regulating Code*, 2013.

[42] Mnenje Evropske skupine za etiko na področju znanosti in novih tehnologij, predloženo Evropski komisiji: Ethics of Security and Surveillance Technologies, Mnenje št. 28, 20. 5. 2015, str. 74.

[43]Glej na primer Homer Economicus: The Simpsons and Economics, ur. Joshua Hall, 2014.

[44] Po najbolj konservativni opredelitvi napake to pomeni, da je stvarne napake v potrošnikovem poročilu imelo 23 milijonov Američanov. Pet odstotkov udeležencev v raziskavi je imelo napake, po odpravi katerih se je njihova bonitetna ocena tako izboljšala, da bi lahko kredit dobili po nižji ceni, Zvezna komisija za trgovino: poročilo kongresu v skladu z oddelkom 319 zakona Fair And Accurate Credit Transactions Act iz leta 2003, december 2012; Chris Jay Hoofnagle: How the Fair Credit Reporting Act Regulates Big Data (10. september 2013). Delavnica foruma Future of Privacy o masovnih podatkih in zasebnosti: Making Ends Meet, 2013. Dostopno na SSRN: http://ssrn.com/abstract=2432955.

[45] Svetovni gospodarski forum opredeljuje podatke kot koristno sredstvo posameznika, čigar pravice do posedovanja, uporabe in izbrisa se lahko prenesejo na podjetja in vlade v zameno za storitve. Glej nedavne govore, tudi govor podpredsednika Evropske komisije Ansipa, na primer z dne 7. 9. 2015 na Brueglovem letnem srečanju z naslovom „Productivity, innovation and digitalisation - which global policy challenges?“: „Lastništvo in upravljanje pretokov podatkov, uporaba in vnovična uporaba podatkov. Upravljanje in shranjevanje podatkov. Ti so temelj za pomembne nastajajoče sektorje, kot so računalništvo v oblaku, internet stvari in masovni podatki.“

[46] „Kdo ima torej pravico uporabljati informacije in podatke, ki v resnici niso njegova last?“ To vprašanje presega meje trgovanja, etike in morale ter vodi do vprašanj o zasebnosti in varstvu zasebnosti“, Al-Khouri, november 2012, http://www.academia.edu/6726887/Data_Ownership_Who_Owns_My_Data_036. Glej tudi Margaret Jane Radin: Incomplete Commodification in the Computerized World v: Commodification of Information 3, 17, Niva Elkin-Koren in Neil Weinstock Netanel, ur., 2002: „Gre za veliko razliko, če se zasebnost razume kot človekova pravica, ki pripada osebam na podlagi njihovega sebstva, ali kot lastninska pravica, nekaj, kar imajo osebe lahko v lasti in to lahko nadzirajo. Človekove pravice so predvidoma tržno neodtujljive, lastninske pravice pa so predvidoma tržno odtujljive.“

[47] Cilji projekta laboratorija za računalništvo in umetno inteligenco MIT Crosscloud, ki ga podpira več podjetij s sedežem v EU, sta „1) poenostaviti razvoj večuporabniške (‚družbene‘) programske opreme le z razvojem na strani odjemalcev in spoštovanjem pravic in zasebnosti uporabnikov ter 2) uporabnikom omogočiti svoboden prehod med aplikacijami, platformami strojne platforme in

družbenimi omrežji, z ohranitvijo lastnih podatkov in družbenih povezav“, http://openpds.media.mit.edu/#architecture (dostop 10. 9. 2015).

[48] Glej pojasnilo k členu 1 Listine o temeljnih pravicah.

[49] Martha Nussbaum: Objectification v: Philopsophy and Public Affairs 24(4), 1995.

[50] Sodba z dne 15. decembra 1983, BVerfGE 65, 1-71, Volkszählung.

[51] Glej Evropska skupina za etiko na področju znanosti in novih tehnologij: Opinion on Ethics and Surveillance, str. 75. V študiji je bilo ugotovljeno, da je algoritem za ciljanje oglasov diskriminatoren, saj iskanje v povprečju najde oglase za bolje plačana delovna mesta za moške, tudi kadar spletišča s ponudbo delovnih mest obiščejo ženske, Carnegie Mellon University and the International Computer Science Institute. Glede težnje, da se digitalnim pomočnikom privzeto dodeli ženski glas, glej na primer Judy Wajcman: Feminist theories of technology. Cambridge Journal of Economics, 34(1), str. 143–152, 2010.

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

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

[54] BBC: Information watchdog investigates ‘charity data sales’, 1. 9. 2015.

[55] Glej pismo Future of Life Institute. Papeževa okrožnica *Laudato Si:* „K vsemu temu je treba dodati dinamiko javnih občil in digitalnega sveta, ki, potem ko se zalezejo v vse pore, ne pospešujejo sposobnosti modrega življenja, globokega mišljenja in velikodušne ljubezni. V teh časih bi veliki misleci preteklosti tvegali, da bodo njihovo modrost zadušili v zmedenem trušču informacijske zasičenosti. Zato se moramo potruditi, da se bodo sredstva obveščanja spremenila v pospeševalce novega kulturnega razvoja človeštva in ne v uničevalce njegovega največjega bogastva. Prave modrosti, sadu refleksije, dialoga in plemenitega srečevanja ljudi, ni mogoče pridobiti s kopičenjem podatkov; to se konča v prenasičenosti in zmedenosti, v neke vrste umski onesnaženosti. Hkrati pa skušajo realne stike z drugimi, z vsemi izzivi, ki jih ti prinašajo, nadomestiti z neke vrste posredno komunikacijo po spletu. Ta omogoča izbiranje in zavračanje stikov po lastni presoji; tako se pogosto rojeva nova vrsta čustvovanja, ki si daje več opraviti z napravami in zasloni kot z ljudmi in naravo. Današnja občila omogočajo, da komuniciramo med sabo, sklepamo poznanstva in zveze. Vendar pa nam včasih tudi preprečujejo neposreden stik s tesnobo, drgetom, veseljem drugega in z njegovo celovito osebno izkušnjo. Zato ni nič čudnega, da hkrati z neznosno ponudbo teh izdelkov narašča globoko in melanholično nezadovoljstvo v medsebojnih razmerjih ali pa škodljiva osamljenost.“

[56] Glej ukrep 4 v strategiji ENVP za obdobje 2015–2019 o razvoju etične razsežnosti varstva podatkov.