Revija za kriminalistiko in kriminologijo / Ljubljana 68 / 2017 / 2, 135–149

Algoritmično nadzorstvo: veliko podatkovje, algoritmi in družbeni nadzor

Aleš Završnik[1]

V prispevku so predstavljeni načini in posledice uporabe velikega podatkovja in algoritmičnega napovedovanja v družbenem nadzorstvu. Po definiciji velikega podatkovja so najprej prikazane njegove posledice za produkcijo vednosti v podatkovni družbi. Nato se prikaz osredotoči na izbrane domene neformalnega in formalnega družbenega nadzorstva, ki jih algoritmi in podatkovna analitika spreminjajo. Izpostavljeni so zlasti vplivi napovedne podatkovne analitike na ekonomsko-politični sistem, predvsem na demokracijo in vladavino prava, ki ju spreminja v »algokracijo« (vladavino algoritmov), ter posledice avtomatizacije policijskega dela in avtomatizacije delovanja kazenskopravnih sistemov. S prikazom temeljnih značilnosti napovedne policijske dejavnosti in avtomatiziranih načinov odločanja v kazenskem pravosodju, zlasti v pripornih zadevah, pri izbiri in odmeri kazenske sankcije ter v postopkih pogojnega odpusta, prispevek opozori na nekatere omejitve algoritmičnega napovedovanja ter negativne posledice uporabe velikega podatkovja in algoritmičnega napovedovanja v sistemih družbenega nadzorstva. Prispevek se konča s predlogi izboljšav in odprave negativnih učinkov algoritmičnega nadzorstva.

Ključne besede: algoritmi, veliko podatkovje, napovedno policijsko delo, avtomatizirana pravičnost

UDK: 343.9+004.493

1 Uvod

V nadzorstvenem kapitalizmu (Zuboff, 2016) vedno več naših dejavnosti pušča digitalne sledi, ki ustvarjajo velike količine (osebnih) podatkov – veliko podatkovje (angl. *big data*). Slednje prinaša več prednosti za posameznike, podjetja in države, ko, denimo, družbena omrežja priporočajo prijatelje in intimne partnerje (Bridle, 2014) oziroma ko algoritmi, ki osmišljajo veliko podatkovje, opravijo velik del transakcij na borzah, organom odkrivanja in pregona kažejo, kje in kdaj naj bi se zgodil prihodnji zločin, ali pa vojski pomagajo iskati potencialne teroriste (Naughton, 2016). Analiza velikega podatkovja danes ni več samo del finančne aplikativne matematike internetnih velikanov, ampak je postala orodje delovanja obveščevalnih služb in varnostnih organov ter sredstvo kriminalitetne politike (McCulloch in Wilson, 2015). V financializiranih tehnokratskih družbah prevladuje prepričanje, da bodo digitalne tehnologije z velikim podatkovjem in samoučečimi se algoritmi, ki so srčika t. i. umetne inteligence, rešile številne družbene probleme, vključno s preprečevanjem kriminalitete in odkrivanjem storilcev kaznivih dejanj. Ta »revolucija, ki bo spremenila, kako živimo, kako delamo in kako mislimo« (Mayer-Schönberger in Cukier, 2013), močno vpliva na izvajanje formalnega in neformalnega družbenega nadzorstva, kar je tema tega prispevka.

Napovedno policijsko delo (angl. *predictive policing*) se pomembno spreminja z uporabo algoritmičnih policijskih napovednih računalniških programov, kot je IBM-ov *Blue Crush* (IBM, 2010). Takšni računalniški programi temeljijo na veliki količini policijskih in tudi drugih podatkov, zlasti s spletnih družbenih omrežij. Podatki so zelo raznolike oblike (strojno berljivi in strojno neberljivi) in tudi kakovosti (podatki, ki jih na spletnih družbenih omrežjih objavljajo uporabniki, so lahko neresnični), a vendar ta program izdela verjetnostno poročilo za prihodnjo kriminaliteto. Verjetnost, ki je izračunana, pa zahteva presojo odločevalca – ali sploh in kako se odzvati –, torej odločitev, ki je računalnik ne more »izračunati«. Ta poročila so zelo konkretna, denimo, katera vrsta kaznivega dejanja bo storjena čez 24 ur na specifični lokaciji v mestu (IBM, 2010). Poleg policije, kot temeljnega agenta formalnega družbenega nadzorstva, tudi kazenska sodišča (in drugi organi kazenskega pravosodja) uporabljajo veliko podatkovje in algoritme za napovedovanje prihodnjega vedenja posameznika. To se za zdaj pojavlja v treh fazah pravosodnega odločanja: pri odrejanju omejevalnih ukrepov (npr. pripora) (Leskovec 2015), pri izbiri in odmeri kazenske sankcije in za oceno tveganja povratništva pogojno odpuščenih (več o tem v poglavju o algoritmičnih kazenskih sodiščih).

Algoritmi in veliko podatkovje imajo osrednjo odločevalsko moč tudi pri drugih oblikah nadzora, saj ko govorimo o

[1] Dr. Aleš Završnik, višji znanstveni sodelavec, Inštitut za kriminologijo pri Pravni fakulteti v Ljubljani, in izredni profesor za kriminologijo, Pravna fakulteta Univerze v Ljubljani, Slovenija. E-pošta: ales.zavrsnik@pf.uni-lj.si

družbenem nadzorstvu, govorimo vsaj o formalnem in neformalnem družbenem nadzoru (Pečar 1988, 1991), avtomatizirane oblike odločanja z uporabo algoritmov pa se pojavljajo pri obeh oblikah nadzorstva. Denimo, poleg oblik formalnega nadzora se kažejo tudi v skrbi za zdravje v obliki neformalnega nadzora, pri katerem nas produkti »nosljivega računalništva« (angl. *wearable computing*) usmerjajo k »primernemu« vedenju in »pravemu« življenjskemu slogu (npr. ko naprave štejejo porabljene kalorije, korake, srčni utrip in priporočajo temu »primerne« aktivnosti posameznika). Kaj je primerno vedenje v smislu skrbi za zdravje in pravi življenjski slog, je nekaj, kar je lahko realno določeno le na podlagi analize in pregleda konkretnega posameznika, ti programi (npr. v obliki aplikacij za pametne telefone) in naprave (v obliki posebnih izdelkov »nosljivega računalništva«, tj. »pametnih« zapestnic ali nakita itn.) pa vzbujajo občudovanje in uveljavljajo povprečna – v smislu, kar velja na agregatni ravni za množice, naj velja za konkretnega posameznika – merila zdravega življenja oziroma moralne večine. Gre za silo normalizacije, uravnilovke, torej oblike družbenega nadzorstva, ki se uveljavlja – v opisanem primeru – s potrošniškimi izdelki zabavne elektronike.

Veliko podatkovje in algoritmi pomembno določajo človeške življenjske možnosti in priložnosti v številnih drugih sferah človekovega udejstvovanja. Za ponazoritev: algoritmi določajo posameznikove življenjske možnosti v sistemih zavarovanj (Meek, 2015) in tudi v sistemih bančnega (O'Hara in Mason, 2012) sektorja, kjer oblikujejo personalizirane storitve – zavarovalne premije, prilagojene genski sliki, življenjskemu slogu ali, v drugem primeru, prilagojene obrestne mere, ki ustrezajo finančnemu tveganju specifičnega posameznika. Kakšne krivice pri tem povzročajo netransparentno delujoči algoritmi, kaže primer avtomobilskih zavarovanj, ki jih temnopolti v ZDA plačujejo v višjem znesku kot preostali – to je uspelo dokazati s Pulitzerjevo nagrado nagrajenim raziskovalnim novinarjem in podatkovnim analitikom ProPublice (Angwin, Larson, Kirchner in Mattu, 2017).

Algoritmi oblikujejo življenjske možnosti in priložnosti tudi pri zaposlovanju v podjetjih. Zaposlitveni algoritmi brskajo po javno dostopnih zbirkah podatkov in pripravijo celovito podobo posameznika in njegove osebnostne ter strokovne primernosti za zasedbo specifičnega delovnega mesta (Cohen et al., 2015). Krivice takšnega delovanja so že bile dokumentirane. Nadalje izredna moč velikega podatkovja in algoritmov vpliva tudi na demokratične procese, kot so pokazale ameriške predsedniške volitve v letih 2012 in 2016. Izid zadnje predsedniške tekme je posledica podatkovne moči in boja med republikanskim analitičnim podjetjem Cambridge Analytica (Confessore in Hakim, 2017), ki naj bi brskalo po 500 podatkih o vsakem ameriškem volivcu, ter demokratskim algoritmom Ada (Wagner, 2016). Pri tem za uspeh na volitvah ni bil pomemben samo vsebinski program političnih strank, kar bi pričakovali, temveč podatkovna moč analizirati volivce, doseči neopredeljene in sporočiti volivcem individualno ukrojena politična sporočila – takšna nova vednost targetiranja volivcev je postavila vodjo svetovnega hegemona. Ali natančneje, bogata manjšina, ki si lahko privošči najboljše podatkovne znanstvenike – »najbolj seksi poklic 21. stoletja« (Davenport in Patil, 2012) –, lahko zmaga na državnih volitvah.

Omenjeni raznoliki primeri uporabe velikega podatkovja in algoritmov kažejo, da to ob številnih koristih prinaša tudi številne težave. Te so specifične za posamično domeno – zavarovalniško, bančno, sodno, policijsko –, nekatere pa so skupne algoritmičnemu delovanju. Algoritmi namreč lahko vsebujejo predsodke ali nedovoljene parametre odločanja – nehote zaradi napak pri njihovem oblikovanju ali celo ob njihovi izrecni izključitvi zaradi zmožnosti algoritmov, da prepovedane parametre, kot je veroizpoved ali rasna pripadnost, izračunajo posredno iz drugih značilnosti (npr. nakupovalnih vzorcev, vrste nakupovane hrane v izbranem času). V domeni kazenskega pravosodja, pri algoritmičnem izbiranju in odmeri kazenskih sankcij so v analizi algoritma podjetja Northpointe, ki ga številne zvezne države uporabljajo za oceno tveganja in odločanje o kazenski sankciji (Angwin, Larson, Mattu in Kirchner, 2016), raziskovalci ugotovili, da je delovanje algoritma rasno pristransko. Podobne krivice so povzročile »personalizirane« zavarovalniške storitve, ki minimalizirajo finančna tveganja za zavarovalnice in neupravičeno diskriminirajo uporabnike. Bančna personalizacija namreč onemogoča celotnim segmentom prebivalstva najem ali nakup stanovanja, ker so pripadniki preveč »tvegane« populacije. Algoritmi lahko vsebujejo predsodke, ki sicer že obstajajo v družbi, a jih perpetuirajo in s tem povečujejo družbene razlike. Obstajajo še druge pasti algoritmičnega odločanja, kot so prenos odgovornosti za končne odločitve. Robotski sodnik – tudi v obliki pomagala pri odločanju o priporu ali pogojnem odpustu – zmanjšuje odgovornost sodnika ali komisije za pogojne odpuste, saj se odgovornost delno prenaša tudi na sestavljavce algoritmov in pravosodno upravo. Mnenjske raziskave v sistemih, kjer uporabljajo napovedno analitiko, kažejo, da sodniki radi uporabljajo te sisteme, da bi s tem razpršili odgovornost za sprejete odločitve (Harcourt, 2015).

Te raznolike uporabe velikega podatkovja in algoritmičnega napovedovanja so mogoče le v specifičnem družbeno-političnem kontekstu. To je v kontekstu, v katerem se za reševanje družbenih problemov iščejo tehnološke rešitve in tehnologija služi kot sredstvo neoliberalne politike (McCulloch in Wilson, 2015), s tem pa sredstvo za poglabljanje družbenih neenakosti. Podatkovne analitike si lahko najamejo le najbogatejši. Ta nova vednost, ki je zgrajena na veliki količini na videz nepo-

vezanih podatkov, temelji na težko razumljivih matematičnih algoritmih. Algoritmov praviloma tudi ni mogoče pregledovati, ker so intelektualna lastnina podatkovnih podjetij, to pa ima učinek odločevalske »črne škatle« (Pasquale, 2015). Negativna posledica nekritične uporabe velikega podatkovja in algoritmičnega napovedovanja v sistemu kazenskega pravosodja je, da to krši načelo nedolžnosti, neodvisnega sodnika in pravico do naravnega sodnika, načelo neposrednega sojenja in dolžnega postopanja (angl. *due process*). Avtomatizacija odločanja, ki temelji na velikem podatkovju, ruši hierarhijo dokaznih standardov in briše mejo med nedolžnimi, osumljenimi, obtoženimi in obsojenimi osebami (Marks, Bowling in Keenan, 2015). V ozadju trenutnih in potencialnih rab velikega podatkovja in algoritmov tako vznikajo številni pravni in etični izzivi, ki se nanašajo na družbeno sortiranje prebivalstva (Lyon, 2014), diskriminacijo, zasebnost, načelo enakosti in socialne pravičnosti.

V prispevku so predstavljene nadzorstvene spremembe, ki so posledice velikega podatkovja in algoritmičnega – avtomatiziranega ali polavtomatiziranega – odločanja v družbenem nadzorstvu. V nadaljevanju je najprej opredeljen osrednji označevalec – »veliko podatkovje«. Nato so prikazane številne nadzorne domene, zlasti pa policijsko in pravosodno delo. Na koncu je izražen vpliv velikega podatkovja in algoritmične moči na ekonomsko-politični sistem, saj njihova uporaba »ogroža demokracijo« (Zuboff, 2015), ki jo nadomešča »algokracija« (Morozov, 2013). Ponujenih je tudi nekaj rešitev, ki bi lahko omilile negativne učinke velikega podatkovja in algoritmičnega napovedovanja za temeljne človekove pravice.

2 Kaj je »veliko podatkovje«?

V poslovnem okolju – kar ni nepomembno zaradi prenašanja tamkajšnjih vrednot in ciljev – veliko podatkovje definirajo s tremi ali celo štirimi (IBM, 2016), petimi oziroma šestimi značilnostmi (angl. »six Vs«) (Marr, 2016): 1) velika količina (angl. *volume*) podatkov, 2) hitrost (angl. *velocity*) obdelovanja podatkov, ki poteka v realnem ali skoraj realnem času, 3) večja raznolikost podatkov (angl. *variety*), saj so uporabljene različne oblike podatkov (npr. strojno (ne)berljivi, (ne)strukturirani), 4) točnost podatkov (angl. *veracity*), ki se nanaša na dvomljivo kakovost podatkov, 5) vrednost podatkov (angl. *value*) in 6) ranljivost podatkov (angl. *vulnerability*).

Kako *veliko* je veliko podatkovje, kaže podatek, da smo v letu 2016 proizvedli toliko podatkov kot v celotni človeški zgodovini (Helbing et al., 2017), 90 % podatkov na svetu pa je nastalo v zadnjih dveh letih (podatek za 2013 (Sintef, 2013)). Viri podatkov so različni in naraščajo, denimo: podatki se zbirajo v »pametnih mestih« iz prometne, električne, vodovodne idr. infrastrukture. Zbirajo se pri vedno večjem številu »pametnih« reči, povezanih z internetom, in oblikujejo t. i. »internet stvari« (angl. *Internet of Things*). Podatki se zbirajo zaradi načina delovanja javnih telekomunikacijskih omrežij (npr. za obračunavanje stroškov in zagotavljanje storitve se zahtevata beleženje in shranjevanje podatkov). Vedno več podatkov prostovoljno zagotavljajo tudi uporabniki sami: Facebook zbira 63 različnih podatkov za svoj aplikacijski programski vmesnik, gumb za všečkanje je uporabljen 2,7-milijardokrat na dan (Smith, 2014). Uporabniki Twitterja so sredi leta 2013 vsako sekundo objavili 143.199 tvitov. Objavijo približno milijardo tvitov vsaka dva dneva ali več deset milijard vsak mesec, zato je to »največji register pogovorov, kar jih obstaja« (Dredge, 2014). Deroča reka tvitov je priložnost za vpogled v novice in informacije, ki ljudi zanimajo, in to v realnem času. Ker »Twitter zagotavlja močno novo lečo, skozi katero opazujemo svet – kot platforma za stotine milijonov potrošnikov, poslovnih strokovnjakov in kot sintetizator trendov«, meni predsednica IBM Ginni Rometty (IBM, 2014), se za te podatke zanimajo tudi nepodatkovna podjetja (Dredge, 2014) in oblasti. Senzorji v cestni infrastrukturi, »pametnih« hišah, »pametnih« avtomobilih itn., naj bi do leta 2025 dosegli 11,1 trilijona dolarjev ekonomskih učinkov na letni ravni (Manyika et al., 2015). Količina podatkov bo zelo verjetno rasla, z njo pa možnosti podatkovnega nadzora.

Poleg obsega in virov velikega podatkovja je za analizo njegovih družbenih učinkov ključna obljuba izboljšati človekove odločitve, in to z natančnejšim algoritmičnim napovedovanjem. Napovedna moč je razlog, zakaj sta veliko podatkovje in algoritmično odločanje zanimiva za kriminologijo. Kriminologija se je kot znanost oblikovala kot odgovor na vprašanji, kako kriminaliteto razumeti in kako se nanjo odzivati, s tem pa jo narediti uporabno za penalno oblast (Garland, 1992). Podobno danes oblasti zanima, kako velike količine podatkov, ki jih organi formalnega družbenega nadzorstva že zbirajo ali do njih lahko dostopajo, narediti operativne (angl. *actionable data*) za specifične kriminalitetno-politične cilje. Nova vednost, ki jo matematični jezik algoritmov proizvaja, spreminja oblast (Desrosières, 2002). Ključno je zato danes vprašanje, kako algoritmični vpogled v družbo spreminja mehanizme oblasti, ali drugače, kako se spreminja nerazdružljiva dvojica vednosti in oblasti (Foucault, 2004).

3 Algoritmi in spremembe vednosti

Veliko podatkovje in nova analitična orodja pomenijo novo znanstveno paradigmo: nova nista le množično zbiranje in shranjevanje podatkov, temveč tudi analitika velikega podatkovja, ki ga osmišlja in »omogoča nove epistemološke pristope pri osmišljanju sveta« (Kitchin, 2014: 2). Spreminja

se način, kako je proizvedena vednost, kako so opravljeni posli in kako je izvajano upravljanje družbe (Mayer-Schönberger in Cukier, 2013). Sprememba se ne nanaša le na globino in obseg podatkov, temveč na epistemološki pristop, torej na to, kako se preoblikujejo znanstvena vprašanja, kako spoznavamo svet okrog sebe, kakšne so značilnosti in kategorizacija realnosti. Avtomatizacija raziskovalnega procesa spreminja definicijo vednosti, kar je po oceni Boydove in Crawfordove (2011) primerljivo s preskokom, ki ga je fordistična industrijska avtomatizacija naredila v primerjavi z dotlejšnjo obrtno organizacijo proizvodnje.

Avtorji, ki verjamejo v veliko moč velikega podatkovja, menijo, da to signalizira novo obdobje proizvodnje vednosti, ki ga v temeljnem označuje »konec teorije« (Anderson, 2008). Podatkovna »povodenj« naj bi povzročila, da je znanstvena metoda zastarela (Anderson, 2008). Če je bila doslej ideja preveriti teorijo z analizo podatkov, nova analitična orodja niso namenjena preverjanju teorije (hipoteze), ampak temu, da iz vpogleda v podatke sama izdelajo teorijo – vpogled naj bi nastal iz podatkov samih (Kitchin, 2014). Takšna nova »empirična epistemologija« izhaja iz več (spornih) domnev (Kitchin, 2014: 4–5): 1) da veliko podatkovje lahko zajame celotno domeno, ki jo želi analizirati, 2) da ni potrebe po vnaprejšnji teoriji, 3) da podatki »govorijo zase«, brez človeških predsodkov in uokvirjanja (Captain, 2015) in 4) da izračunani pomen transcendira kontekst ali vednost specifične (analizirane) domene in rezultate lahko interpretira vsak, ki lahko dekodira vizualizacijo (produkt analitike). Te predpostavke so problematične in kažejo na ideologijo velikega podatkovja. Domnevna apriorna vednost, očiščena vrednostnih in interesnih prvin ter drugih kulturnih ostankov, je fikcija, zaradi katere je ta nova vednost izredno privlačna za penalno oblast. Pri boju zoper kriminaliteto namreč postane vprašanje odziva na kriminaliteto zreducirano na moč informacijskega sistema, kar ne zahteva preizpraševanja o vzrokih kriminalitete in tudi ne o interesih, ki podpirajo takšno analitiko: komu koristita in komu škodujeta takšno razumevanje in odziv ter katere interese v razredno in interesno razklani družbi ta vednost podpira.

Ta nova vednost, ki temelji na veliki količini na videz nepovezanih podatkov, premešča družbeno nadzorstvo na nove akterje. Kar ni presenetljivo, saj je bila matematična racionalnost vedno vpeta v mehanizme družbenega nadzora in od vznika moderne države dalje je bila nepogrešljiva za legitimacijo moči vlad (Desrosières, 2002). Sodobni algoritmi so le nov jezik za legitimacijo te moči; kot metaforično meni Desrosières (2002), danes matematika diktira dolžnosti držav in meri njihove (ne)uspehe. Nova vednost pa premešča družbeno moč. Podatkovna podjetja, ki imajo podatke – metaforično imenovani »novo gorivo« (angl. »*Data is the new oil*!«) kot nafta in premog v industrijski dobi –, to moč delijo odplačno, najboljšemu ponudniku. Podatki niso razumljeni kot javno dobro, ampak so privatizirani. Podatkovna podjetja imajo zato veliko večjo družbeno moč. Dvojica oblasti in vednosti se tako spreminja v številnih domenah znotraj formalnega in neformalnega družbenega nadzora, zato v nadaljevanju prikažemo različne domene neformalnega in formalnega družbenega nadzora, kjer veliko podatkovje in algoritmi izzivajo spremembe.

4 Algoritmi vsakodnevnega življenja

Skrita diskriminacija algoritmičnega delovanja se kaže pri vsakodnevnih rutinah slehernika. Študentka MBA je aprila 2016 v iskalniku Google iskala »neprofesionalne pričeske za delo« in rezultati iskanja so ji ponudili temnopolte ženske z naravno afropričesko, medtem ko je iskanje »profesionalnih pričesk« pokazalo pretežno ženske bele polti (Leigh, 2016). Različni profesionalni in neprofesionalni slogi pričesk niso bili toliko različni, kolikor je bila različna barva kože. Podobno nesorazmerje je bilo mogoče prepoznati v primeru prvega lepotnega tekmovanja, v katerem so bili (raz)sodniki lepote tekmujočih algoritmi (Levin, 2016). Ti naj bi uporabljali objektivne parametre za izračun lepote, kot so na primer obrazna simetrija. Zgodilo pa se je, da računalniki med najlepših deset tekmovalk in tekmovalcev niso izbrali niti enega temnopoltega tekmovalca ali temnopolte tekmovalke – v glavnem le belce. Pri tem je pomembno, da računalničarji, ki so gradili algoritem, tega niso zasnovali tako, da bi dajal prednost beli polti ali da bi slednjo označevala večja stopnja lepote v primerjavi z drugo poltjo. A »nevtralni« podatki so na koncu kljub temu privedli do tega, da so robotski sodniki prišli do odločitve, ki je očitno diskriminatorna.

Navedeni primeri so manj škodljivi in manj usodni za družbeni položaj in pravice posameznika: nekdo zaradi tega, ker ni zmagal na lepotnem tekmovanju ali ker je dobil slabo priporočilo o pričeski na Googlu, ni utrpel večje škode. Vendarle pa ima pretirano zanašanje na takšne avtomatizirane odločevalske sisteme usodnejše reperkusije v drugih družbenih domenah. Raziskovalci so že dokazali spolno pristranost Googlovih algoritmov pri ponujanju oglasov za zaposlitve – oglase za bolj prestižne službe prejemajo moški uporabniki iskalnika v večji meri kot ženske (Sweeney, 2013). Podobno usodnejše reperkusije, kar pojasnjujemo v nadaljevanju, so imele napačne novice, moderirane z algoritmi, in algoritmično tarčno naslavljanje volivcev po spletnih družbenih omrežjih, ki so pomembno vplivali na izid ameriških volitev v letu 2016.

5 Algoritmi v demokratičnem procesu

V politični domeni algoritmi izkrivljajo »normalno« delovanje demokratičnega procesa. Skupina avtorjev Helbing et al. (2017) se v članku *Will Democracy Survive Big Data and Artificial Intelligence?* v reviji *Scientific American* sprašuje, ali veliko podatkovje vodi v totalitarizem. Denimo, pri izvedbi volitev kot osrednjega demokratičnega mehanizma imata veliko podatkovje in algoritmično napovedovanje moč, da spremenita izid volitev, torej začrtata smer prihodnjega družbenega razvoja. Težava je, da v nasprotju s preteklostjo, ko so bile javnomnenjske raziskave izvedene na vzorcih populacije in vnaprej objavljene ter dostopne vsem, algoritmi uživajo pravno zaščito – plašč pravic intelektualne lastnine. To pomeni, da jih ni mogoče pregledovati. Krepijo bogato manjšino, ki lahko najame najboljša podatkovna podjetja in se skrije z instrumentarijem prava intelektualne lastnine. Za ponazoritev omenjamo primer predsedniških volitev svetovnega hegemona.

Tik pred predsedniškimi volitvami v ZDA v letu 2016 so lažne novice, kot je bil članek, ki je navajal, da je zmagovalca Trumpa javno podprl kar papež, zakrožile po spletnih družbenih omrežjih (Sherwood, 2016). Podobno je na preveliko moč algoritmov pokazal primer perpetuiranja lažnih sporočil v podporo Trumpu, kar naj bi omogočali zaslužkarski mladi na Balkanu. Makedonska mladina je zgradila posebno »domačo obrt« za proizvodnjo Trumpu naklonjenih spletnih strani z lažnimi vsebinami, da bi pridobili nekaj oglaševalskega denarja, obljubljenega za primere »viralnih« zgodb (Silverman in Alexander, 2016). Njihove lažne novice so bile lahko uspešne le, če jim je uspelo zavesti uporabnike, da gre za »pomembne novice«, z večanjem števila ogledov pa so jih kot takšne prepoznali tudi algoritmi v iskalnikih, ki so pomembno prispevali k njihovemu razširjanju. Po tretji, težko preverljivi razlagi naj bi imel internet veliko vlogo pri Trumpovem uspehu, ker je učinkovito angažiral naročene uporabniške klike na plačljivih »klik farmah« v Aziji (Casilli, 2016). Te so sestavljene iz digitalnih tovarn plačljivih všečkov, retvitov ali lažnih spletnih strani, ki naj izboljšajo priljubljenost v največjih spletnih iskalnikih. Torej, »digitalne znojilnice« (angl. *sweatshops*), ustreznice tekstilnih (Badalič, 2010), so v državah globalnega juga prehitele demokratski algoritem z imenom Ada. Po četrti razlagi je za poraz demokratske kandidatke krivo pretirano zaupanje demokratskih podatkovnih ekspertov v lasten algoritem »Ada« – »nevidno roko predvolilne strategije« –, ki naj bi ga po prvotnih načrtih zmagoslavno razkrili javnosti po volitvah. Ada je priporočala, kdaj in kam usmeriti kandidatko ter bataljon njenih namestnikov, kje in kdaj reklamirati oglase po televiziji in kdaj je bolje molčati (Wagner, 2016). Vendarle pa Ada ni analizirala vseh podatkov, posebno ne tistih, ki niso digitalno aktivni, podcenila je moč podeželskih volivcev v revnejših industrijskih državah severovzhoda (t. i. *Rust Belt states*) (Wagner, 2016).

Predsedniške volitve v ZDA v letu 2016 so tako javnosti dostopen primer, ki je razkril družbeni kapital podatkovne analitike in njeno dejansko moč, pa tudi zanesljivost in varnost podatkov. Za raven demokratičnega ustroja družbe je ta moč algoritmov pomembna, ker imajo vlogo metamedijev, čeprav so uporabljeni na domnevno nevtralnih digitalnih platformah. Ker algoritmi spletnih družbenih omrežij delujejo tako, da uporabnike razvrščajo in filtrirajo v »mnenjske balone«, posredno vplivajo na osrednjo demokratično pravico do svobode mišljenja in izmenjave mnenj.

6 Algoritmi kot regulatorji svobode izražanja

Moč algoritmičnega širjenja novic kaže pravno-politične in upravljavske (angl. *governance*) spremembe, ki segajo globoko v procese demokratičnega odločanja in sistemov zavor ter ravnovesij. Nemoč neodvisnih medijev – »četrte veje oblasti«, kot jo je opisal Thomas Carlyle leta 1841 z nanašanjem na novinarsko galerijo v angleškem parlamentu – je razkril »uredniški« spor med Facebookom na eni ter norveškim osrednjim dnevnikom in norveško prvo ministrico na drugi strani. Časopis Aftenposten je septembra 2016 objavil fotografije, ki so »spremenile potek vojskovanja« (Hansen, 2016). Med njimi je bila tudi fotografija 9-letne Kim Phúc, ki gola in požgana teče pred napalmskim napadom v Vietnamu leta 1972. Fotografija, ki je »pretresla ameriško vest« v času vojne v Vietnamu in pomagala končati ameriško invazijo, je bila odstranjena z Aftenpostenovega profila na Facebooku z razlago, da gre za zlorabo otrok, ker so na sliki vidne tudi genitalije 9-letne Kim. Glavni in odgovorni urednik se je uprl cenzuri Facebooka in na naslovnici Aftenpostna je izšla navedena fotografija, skupaj s pozivom Marku Zuckerbergu, glavnemu izvršnemu direktorju podjetja Facebook, naj še enkrat presodi cenzuro in se zazre vase glede svojega metauredniškega ravnanja (Hansen, 2016). Facebook se je odzval z razlago, da priznava, da je fotografija »ikonična«, ampak da je algoritme težko naučiti razlikovati med golimi otroki v enem primeru od golih otrok v drugih primerih. Zato so navedeno fotografijo odstranili. Razlaga je spodbudila premierko Norveške, da je na svojem profilu na Facebooku še sama objavila fotografijo 9-letne Kim. Tudi ta je bila odstranjena z enakim pojasnilom. Spletno družbeno omrežje zanika vlogo urednika, ker se izogiba obveznostim, ki veljajo za uredniško moderirane vsebine.

Na to, da je nevarno algoritmom podeliti preveliko moč pri reguliranju meje med svobodo izražanja in njeno zlorabo, kaže tudi primer Microsoftove virtualne asistentke Tay v letu 2016, ki se je zelo hitro naučila jezika interneta: v 48 urah je postala rasistična promotorka in je začela širiti neonacistične poglede po Twitterju. Podoben spodrsljaj se je zgodil tudi Facebooku, ko je odslovil urednike novic na spletnem druž-

benem omrežju, algoritem, ki jih je nadomestil, pa je začel po 24 urah kot glavne novice promovirati lažne in vulgarne zgodbe (Newitz, 2016).

Meje svobode izražanja v sodobni družbi tako posredno določajo algoritmi, kot kaže primer Facebookove cenzure – ustanovitelj podatkovnega podjetja je dal lekcijo premierki demokratične države. Kaj se spreminja s tem, ko številne družbene podsisteme urejamo računalniško in preveč zaupamo moči algoritmov?

7 Algoritmični kapitalizem – algokracija

Način delovanja nadzorstvenega kapitalizma se spreminja v smeri večje avtomatizacije osrednjega mehanizma – borze in trgovanja z vrednostnimi papirji. Največji *hedge* skladi nadomeščajo zaposlene s programi umetne inteligence. Podjetje Preqin, ki skrbi za upravljanje 1.360 *hedge* skladov s 197 milijardami dolarjev premoženja, sprejema odločitve o trgovanju z uporabo računalniških modelov. Če so bili v preteklosti to statični modeli, je zdaj govor o bitki med »globokim učenjem«, »evolucijskim računanjem« in »nevralnimi mrežami«, ki posnemajo nevronske možganske povezave. Ideja algoritmične družbe je »videti stvari, še preden se zgodijo«, in to na finančnem področju pomeni večjo akumulacijo tistim z boljšo napovedno analitiko.

Algoritmična podatkovna podjetja izpostavljajo vprašanje primernosti več pravnih režimov: varstvo konkurence, varstvo osebnih podatkov, davčno, kazensko in policijsko pravo. Miller (v Solon, 2016) tako navaja, da od vsakega dolarja, ki se zapravi za oglaševanje, samo Facebook in Google (»nevtralni pomožni podjetji«) prejmeta tri četrtine te vrednosti. McChesney (v Solon, 2016) zato navaja, da velike družbe niso le grožnja demokraciji, temveč tudi kapitalizmu.

Algoritmi podpirajo celoten finančni sektor, od katerega je »financializirana« družba popolnoma odvisna. Algoritmične napovedi ne določajo »samo« posameznikovih življenjskih možnosti, npr. pri odločanju o kreditni sposobnosti za nakup stanovanja, temveč celo delovanje večjih svetovnih borz temelji na algoritmičnih napovedih. Visokofrekvenčno trgovanje med Čikagom in New Yorkom je prispevalo h gradnji novih podatkovnih povezav za izboljšanje hitrosti posredovanja podatkov med mestoma.

Težavnost vseh napovednih algoritmov je, da preveliko zaupanje in odvisnost od kvantificiranega odločanja izrinjata, ne samo dopolnjujeta, etično in moralno presojo (Marks et al., 2015; Helbing et al., 2017). Doslej človeško delo se tako standardizira, da ga bodo lahko opravljali kar roboti. Iz tega Sample sklepa, da vznika »odvečni razred« (Sample, 2016), drugi avtorji pa smiselno podobno menijo, da nastaja »podelavska družba« (Srnicek in Williams, 2015).

Ko se torej sprašujemo, kdo (nam) vlada, vidimo, da gre za sprego (nekaterih) vlad in korporacij. Če je Eisenhower govoril o »vojaško-industrijskem kompleksu«, ga je danes treba parafrazirati – gre za »nadzorstveno-industrijski kompleks« (Ball in Snider, 2013). Ko so podatki postali nova nafta, se je svet podredil diktaturi podatkov. Grožnja demokraciji se kaže v tem, da jo nadomešča »algokracija« – vladavina algoritmov (Morozov, 2013).

Vladarji sveta postajajo podatkovna podjetja, države, ki z algoritmi vladajo svetu, oziroma sprege obojih, kadar so razlike med njima zabrisane. To so podjetja, kot je Uber, največje taksi podjetje na svetu, ki nima v lasti niti enega vozila; podjetje Airbnb, ponudnik namestitev, ki nima v lasti nobene nepremičnine; Facebook kot posrednik novic, ki ne ustvarja vsebine; filmske hiše, ki nimajo v lasti nobenega kinematografa (npr. Netflix); prodajalci programske opreme, ki ne pišejo aplikacij (npr. Apple z App Store ali Google z Google Play).

Schneier (2006) zato govori o novem digitalnem fevdalizmu, Morozov (2014) tudi o (ponovnem) »koncu politike«.

Z vidika upravljanja družbe je to pomembno, ker smo priča odstranitvi subjekta iz procesov odločanja, in to povsod, kjer obstaja strah, da bi lahko prišlo do sistemsko neželenih odločitev. Če je industrijska revolucija v cilju povečati proizvodnjo standardizirala delo na enake enote – kot temelj »fordistične družbe« – in je nato proces »mcdonaldizacije« (Ritzer, 2007) dodatno standardiziral delovni proces na preproste dovolj majhne enote tako, da je bilo mogoče delavce hitro menjati iz dneva v dan in jih popolnoma prekarizirati, smo danes priča novemu koraku v to smer. Sistem bo popolnoma učinkovit le, če bo subjekt – mesto negotovosti in potencialno mesto upora – popolnoma odstranjen iz odločevalskih procesov. V tem smislu je konec politične subjektivitete posameznika. Po novem lahko politiko določajo algoritmi z branjem razpoloženja prebivalstva (angl. *sentiment analysis*) (Pang in Lee, 2008). Ta analiza pa ni pasivna, ampak mogoča intervencije: razpoloženje prebivalstva je mogoče spreminjati in poljubno manipulirati, kot je pokazal eksperiment s slabim milijonom uporabnikov Facebooka (Kramer, Guillory in Hancock, 2014). V takšnem sistemu podatkovni lordi lahko učinkovito zatrejo razvoj alternativnih idej in poljubno dozirajo vsebino posredniške demokracije.

8 Algoritmična policija

Analiza velikega podatkovja z napovednimi algoritmi je že postalo orodje delovanja obveščevalnih služb in varnostnih organov ter sredstvo kriminalitetne politike (McCulloch in Wilson, 2015; Perry, McInnis, Price, Smith in Hollywood, 2013). Napovedni policijski računalniški programi, kot je *PredPol* ali IBM-ov *Blue Crush*, izdelajo verjetnostna poročila o prihodnji kriminaliteti. Program za vizualizacijo napovedi kriminalitete podjetja Hitachi bodo kmalu uporabljala številna ameriška mesta (Captain, 2015): »Človek preprosto ne more obvladati več deset ali več 100 spremenljivk, ki lahko vplivajo na kriminaliteto, kot so vreme, objave na družbenih omrežjih, bližina šol, železniških postaj, podatki iz strelnih senzorjev, klici 911.«

Program *TrapWire*, ki je namenjen izdelovanju ocen tveganj za posamezne potnike – potencialne teroriste (Trapwire, 2017), kot je razkril WikiLeaks leta 2012 (Shane, 2012) – podatke pridobi iz videonadzornih sistemov javnega prostora, okrepljenih s programi za prepoznavanje obrazov, in jih primerja s podatki iz različnih policijskih podatkovnih zbirk. Enaka podatkovna analitika deluje pri izdelavi seznamov ljudi, ki jim je prepovedano leteti (angl. »no-fly« lists). Programi vključujejo raznolike podatke, katerih vsebina ni v celoti znana, gotovo pa je, da vključujejo vse od objav na spletnih družbenih omrežjih do profiliranja glede na oglede na Youtubu, tudi analize obiskov spletnih strani (Goede in Sullivan, 2016). Programi, kot je npr. *SentiStrength*, lahko merijo tudi čustvena stanja ljudi (angl. *emotion analysis techniques*) (SentiStrenght, 2017). Za takšen nadzor spletnih družbenih omrežij in brskanje po podatkih za ugotavljanje stališč prebivalstva o poljubnih vprašanjih (angl. *opinion mining*) se uporablja oznaka »napovedno policijsko delo« (angl. *predictive policing*).

»Napovedno policijsko delo« je anglo-ameriškega izvora in Rand Corporation ga opredeljuje kot »uporaba analitičnih tehnik – posebej kvantitativnih – za identifikacijo verjetnih tarč policijske intervencije, kriminalitetne prevencije ali preiskovanja kaznivih dejanj s statističnimi napovedmi« (Perry et al., 2013: xiii). Cilj je s kriminalitetnimi verjetnostnimi poročili kriminaliteto razumeti enako kot vremenska služba, ki izdaja napovedi pred nevihto (Goode, 2011). Napovedi sestavljata dva elementa: 1) napovedni model, ki z algoritmom identificira možnosti povečanega tveganja pred kriminaliteto, in 2) povezane strategije za spopadanje s tem tveganjem in/ali za njegovo zmanjševanje (Ridgeway, 2013; Beck in McCue, 2009). Ideja je, da podatkovna napovedna analitika omogoča izdelavo natančnejših napovedi od tradicionalne analize kriminalitete (Saunders, Hunt in Hollywood, 2016; Berk in Bleich, 2013).

Razvojno gledano je napovedno policijsko delo nova faza oblike »policijskega dela, temelječega na vročih točkah« (angl. *hot spots policing*) (Eman, Györkös, Lukman in Meško, 2013). Če se je ta usmerjala na žarišča kriminalitete v urbanih predelih, naj bi bili algoritmično podprti sistemi manj statični upravljavski sistemi, ki izračunavajo napovedi o tem, kje se bo posamično kaznivo dejanje izbranega dne zgodilo v realnem času, s takojšnjimi »podatki za ukrepanje« (angl. *actionable data*). Priljubljeni policijski program *PredPol*, denimo, oglašujejo kot program, ki je »več kot *hot spot policing*«, ker ne uporablja le GIS-mapiranja, temveč pomaga varnostnim organom napovedati in preprečiti kriminaliteto z »na dokazih temelječo intervencijo« (angl. *evidence-based intervention*) (PredPol, 2017).

Ideja napovednega policijskega dela je poiskati »iglo v kupu sena« (angl. *needle-in-a-haystack problem*). Kritiki dodajajo, da več sena na kupu ne bo olajšalo iskanja igle: bolje bi bilo postaviti ljudi na čelo preiskovanja potencialnih kriminalnih načrtov in jim prepustiti vodenje računalnikov, namesto da se slednjim daje glavno vlogo in sledi njihovim verjetnostnim izračunom, koga in kdaj preiskovati (Schneier, 2006). Več zbranih podatkov, npr. o potnikih v Direktivi (EU) 2016/681 o uporabi podatkov iz evidence podatkov o potnikih (PNR) za preprečevanje, odkrivanje, preiskovanje in pregon terorističnih in hudih kaznivih dejanj (2016), bo zato težko pomagalo poiskati »speče teroriste« (Završnik, 2015).

Primeri napovednega policijskega dela vključujejo, denimo, program londonske policije, ki v novi generaciji policijskega dela v skupnosti uporablja programsko orodje, ki ga proizvajalci imenujejo »orodje za sistemsko optimizacijo«: spremlja 30 virov informacij (npr. bloge, 3,3 milijona tvitov na dan in druga spletna družbena omrežja), jih združuje v skupine, zaznava razpoloženje državljanov in identificira vplivne posameznike v skupnosti (Wood, 2014). Iz objav uporabnikov razbira skupne teme in ugotavlja razpoloženje ob teh temah. Če se nezadovoljstvo nevarno stopnjuje v nered, policija ravna proaktivno in opravlja razgovore z občani (Kelion, 2014).

Podatkovna analitika je posebno primerna za nadzor nad delovanjem finančnih transakcij in preprečevanje finančne kriminalitete. Ameriška komisija za trg vrednostnih papirjev in nadzor nad poslovanjem z njimi (*U.S. Securities and Exchange Commission*) pregleduje veliko večje število podatkov svetovalnih podjetij in uporablja napovedno analitiko, da bi zaznala opozorilne znake zelo verjetne kršitve. Ko pridejo v podjetje, že točno vedo, kam naj se usmeri preiskava (Skinner, 2014). Nadzorne institucije lahko pregledajo celotne nize podatkov za več let, in ne samo za naključno izbrane dneve ali mesece, kot je bilo v preteklosti.

Pri napovedovanju kriminalitete se je algoritmična analiza usmerila tudi v telo. Xiaolin Wu in Xi Zhang (2016), avtorja algoritma za analizo fotografij obrazov, zatrjujeta, da je mogoče na podlagi obraznih potez avtomatizirano pri-

pisati osebi stopnjo »kriminalnosti«. Algoritmično analizo Lombrosovega tipa sta opravila na 1.856 ljudeh, od katerih je bila polovica obsojencev, potem pa sta opazovala, iz katerih obraznih delov bi lahko sklepali na kriminalnost. Ugotovila sta, da kriminalnost napovedujejo oblika/zaobljenost ustnic, razdalja med notranjima kotoma očesa ter kot med nosom in usti. Podobno usmerjena je uporaba velikega podatkovja kot detektorja laži. Z uporabo videoposnetkov s kazenskih sojenj so raziskovalci razvili algoritem, ki lahko razbere laž iz specifičnih kretenj in obrazne mimike. Če človek le s težka spremlja več kot deset neverbalnih znakov v komunikaciji, računalnik lahko spremlja načeloma neomejeno količino obraznih premikov, tudi spremembe v srčnem utripu in nihanja v temperaturi, ki odražajo spremembe v pretoku krvi. Raziskovalci so ugotovili nekaj prevladujočih znakov laganja, kot so grimase s celim obrazom (pri ljudeh, ki lažejo, so te navzoče v 30 %, pri preostalih le v 10 %), očesni stik (pri ljudeh, ki lažejo, neposreden stik z izpraševalcem v 70 %, pri preostalih v 60 %), burna gestikulacija ali pogostejša uporaba besednih mašil.

Napovedovanje prihodnjega zločina z napovedno analitiko obsega osredotočanje na osebe, prostore ali predmete. Denimo, policijski »vroči seznam« v Čikagu (angl. *Heat-list* ali *Strategic Subject List*) (Statewatch, 2014; Saunders et al., 2016) uporablja policijske podatke za izdelavo indeksa približno 400 ljudi, ki so najverjetneje vključeni v nasilno kriminaliteto. To niso nujno ljudje, ki so v preteklosti storili kaznivo dejanje, ampak bolj tisti, ki imajo povezave ali se družijo s tistimi, ki so bili storilci kaznivih dejanj. Napovedovanje kriminalitete je mogoče s ciljanjem *krajev* (angl. *crime mapping* (Eman et al., 2013)) in *predmetov*. Zadnje je v rabi pri specifičnih oblikah kriminalitete: a) za sledenje denarju (npr. *EU-US Terrorist Finance Tracking Program* – TFTP poteka za mednarodni transfer denarja, ki je posredovan Ministrstvu za finance ZDA (*US Treasury*) za analizo in izdelavo ocene tveganja), b) za sledenje orožju (npr. Interpol uporablja analitiko velikega podatkovja, imenovano *Odyssey,* za sledenje uporabi orožja in streliva (Ward, 2014)) in c) za sledenje prepovedanemu gradivu (npr. Interpolova mednarodna zbirka posnetkov spolnega izkoriščanja otrok omogoča identifikacijo žrtev z napredno obdelavo gradiva – tj. avtomatizirano analizo pohištva ali zaves v ozadju fotografij, zvoka v ozadju avdiovizualnih posnetkov (Plesničar M. in Klančnik, 2015)).

9 Algoritmična kazenska sodišča

Sistemi odločanja, ki temeljijo na računalniški pomoči, že pomagajo sodiščem in drugim pravosodnim organom v fazi predkazenskega postopka, v postopkih izbire in odmere kazenske sankcije ali v fazi odločanja o pogojnem odpustu.

Algoritmično napovedovanje v fazi odločanja o omejevalnih ukrepih je bilo preizkušeno v raziskavi (Kleinberg, Lakkaraju, Leskovec, Ludwig in Mullainathan, 2017). V prispevku *Zakaj se sodniki motijo*? je Leskovec (Leskovec, 2015) prikazal modeliranje računalniškega odločanja o izrekanju varščine v ZDA, ki je temeljilo na: 1) podatkih 360.000 primerov odločanja o varščini zvezne države Kentucky, kjer sodniki ob plačilu varščine izpustijo na prostost povprečno 73 % obtožencev, od tega pa jih nato 17 % ponovi kaznivo dejanje ali se izmika sojenju, in 2) zveznih podatkih presojanja o varščini o milijonu kazenskih zadev. Neljuba dogodka – povratništvo in izmikanje sodišču – sta bila opredeljena kot posledica slabega predvidevanja sodnikov: če bi ti domnevali, da bo prišlo do enega od teh dogodkov, ne bi spustili obsojenca na prostost ob plačilu varščine. Algoritmična obdelava pripornih zadev je temeljila na 40 objektivnih značilnostih vsake zadeve, kot so: starost obtoženca ob prvi aretaciji, resnost kaznivega dejanja, število zapornih nalogov v preteklosti, predkaznovanost, število primerov družinskega nasilja, ali gre za prvo aretacijo obtoženca. Cilj je bil izdelati napovedni model, ki bi bil boljši od povprečja sodniških odločitev: če sodnikom v Kentuckyju ne uspe pravilno napovedati vedenja obtožencev v 17 % – ko obtoženec ponovi dejanje in/ali se izmika sodišču –, ali lahko algoritem ob enaki stopnji izpuščenih ob plačilu varščine doseže boljši rezultat in zmanjša število »neljubih dogodkov«? Raziskava je hipotezo potrdila: ob vsakem izbranem odstotku izpuščenih osumljencev je računalnik dosegel nižjo stopnjo povratništva oziroma izmikanja sodišču. Vprašanje, ki se ob tem zastavlja, je, ali sodnik upošteva kakšne druge parametre, ki pomembno vplivajo na končno odločitev. V tem primeru bi te dodatne parametre lahko upošteval tudi samoučeči se algoritem, ki bi z razvojem upošteval vedno večje število parametrov. A tudi ta bi bil še vedno »zaklenjen« v pretekle odločitve in bi prezrl robne primere ter potrjeval kritiko algoritmičnega odločanja o »začaranem krogu« (o tem več v nadaljnjem besedilu).

Algoritmi lahko pomagajo pri zgodnjih ocenah sodnega primera, omogočajo napovedovanje izidov pravnih problemov in končnih postopkov (Ashley in Brüninghaus, 2006). Bili so že testirani za napovedovanje izida sodnih primerov najvišjih sodišč, tj. vrhovnega sodišča ZDA (Kravets, 2014), in sicer s 70-odstotno pravilno napovedjo izida (razveljavitve odločitve nižjega sodišča), in Evropskega sodišča za človekove pravice (Aletras, Tsarapatsanis, Preoțiuc-Pietro in Lampos, 2016), kjer so raziskovalci izdelali modele z 79-odstotno zmožnostjo napovedovanja sodniških odločitev (analizirane so bile odločitve, ki so se nanašale na kršitve 3. (Prepoved mučenja), 6. (Pravica do poštenega sojenja) in 8. člena (Pravica do spoštovanja zasebnega in družinskega življenja) Evropske konvencije o človekovih pravicah (Svet Evrope, 1994)).

Postopki odločanja o kazenski sankciji z uporabo algoritmov so doživeli največji razvoj. T. i. »na dokazih temelječe kaznovanje« (angl. *evidence-based sentencing*) (Starr, 2013) ima velik vpliv zaradi siceršnjega anglo-ameriškega usmerjanja sodniške proste presoje v postopkih odločanja o sankciji s kaznovalnimi smernicami. V ZDA že v polovici zveznih držav komisije za odločanje o pogojnih odpustih uporabljajo sisteme, ki izračunavajo, kakšna je verjetnost, da bo pogojno odpuščeni v naslednjih dveh letih prekršil pogoje pogojnega odpusta in ponovil dejanje. Takšna ureditev je primerna, če zmanjšuje razlike med sodišči in vodi do boljše obrazložitve izbire in odmere sankcije, ni pa primerna, če gre za obligatorno vezanost sodnika na takšne vnaprej določene parametre izračunov. Značilen primer uporabe velikega podatkovja in podatkovne analitike za napovedovanje povratništva pogojno odpuščenih uporablja probacijska služba v Filadelfiji (ZDA). Služba ima 295 uslužbencev, ki povprečno nadzirajo skoraj 50.000 posameznikov. Algoritem vnaprej izračuna, za katere od njih je verjetneje, da bodo v prihodnjih dveh letih ponovili kaznivo dejanje. Za vsako izpuščeno osebo – preden ta odide iz zapora – izračunajo oceno tveganja (nizko, srednje ali visoko tveganje), od katere je odvisna intenzivnost probacijskega nadzora: nadzorniki, ki so jim bili dodeljeni posamezniki z nizkim tveganjem, nadzorujejo do 400 odpuščenih, medtem ko tisti, ki so jim bili dodeljeni posamezniki z visokim tveganjem povratništva, le 50. Statistični model napovedovanja je bil sprva zasnovan na 100.000 rešenih primerih in 36 napovednih dejavnikih (npr. starost in spol storilca, soseska kaznivega dejanja in bivanja, predkaznovanost), pozneje pa so uporabili podatke iz več kot 50-letne kazenske statistike. Za specifična kazniva dejanja so dodali dodatna merila, da bi algoritem naučili napovedati specifično vedenje. Rezultati so tako pokazali, da so že storjena kazniva dejanja slab kazalnik prihodnjih prestopkov. Večjo napovedno vrednost imajo starost in spol ob storitvi prvega kaznivega dejanja ter časovni intervali med prvim in nadaljnjimi prestopki.

10 Negativni učinki algoritmičnega nadzorstva

Veliko podatkovje je lahko slepo orodje, ki ne vidi konteksta in nians. To se občasno pokaže ob analizi delovanja izbranih algoritmov, uporabljenih v pravosodju, kar je dokazala ProPublica (Angwin et al., 2016). Pokaže se ob slabih predvolilnih izračunih, npr. kar kaže primer algoritma Ada demokratske predsedniške kandidatke v letu 2016 (Lohr in Singer, 2016), napačnih napovedih pandemij z Google Trend Flu (Lazer, Kennedy, King in Vespignani, 2014) ali takrat, ko Facebookovi algoritmi odstranijo fotografijo, nagrajeno s Pulitzerjevo nagrado (Hansen, 2016). Kritične podatkovne študije (angl. *critical data studies*) opozarjajo na epistemološko naivnost uporabe algoritmov v družbenih sistemih (Barocas in Selbst, 2014; Aradau in Blanke, 2015), pri čemer izhajajo iz politične kritike statistike in odstiranja moči, ki jo ima ta pri upravljanju družbe (Desrosières, 2002). Pri odzivanju na kriminaliteto so analize specifičnih programov velikega podatkovja pokazale diskriminacijo oseb, ki živijo na določenem geografskem območju, ali rasno pristranskost sistemov za napovedovanje povratništva pogojno obsojenih (Angwin et al., 2016).

Negativni učinki se kažejo tudi zaradi napačnih zadetkov (angl. *false positives*). Če je na primer 80 % ljudi, ki živijo pod poštno številko 1.000, vključenih v kriminalne dejavnosti, to ne pomeni, da je konkretna oseba tudi vključena vanje. Napačni zadetki, ki v industrijski domeni, denimo pri oglaševanju, nimajo učinka na človekove pravice, v boju zoper kriminaliteto zelo pomembno kršijo posameznikove pravice, npr. pravico do zasebnosti ali svobodnega gibanja pri »no-fly« seznamih letalskih družb (Goede in Sullivan, 2016).

Netransparentnost osnovnih parametrov odločanja je ključna pri avtomatiziranih sistemih odločanja v pravosodju. ProPublica, ki je analizirala algoritem za pogojno odpuščene, ni imela dostopa do algoritma zaradi pravne zaščite algoritma s pravicami intelektualne lastnine (Angwin et al., 2016).

Varstvo osebnih podatkov in zasebnosti je ključen negativni učinek algoritmičnega nadzorstva. Na to so opozorili številni mednarodni nadzorni organi, ki se ukvarjajo z varovanjem zasebnosti. Delovna skupina iz 29. člena v *Izjavi o učinkih razvoja velikega podatkovja na zaščito posameznikov pri obdelovanju njihovih osebnih podatkov v EU* (Delovna skupina iz 29. člena, 2014) opozarja, da bo osebne podatke s podatkovnim rudarjenjem in samoučečimi se algoritmi mogoče pridobiti tudi iz na videz anonimnih podatkov. Podobno je bila na 36. Mednarodni konferenci informacijskih pooblaščencev sprejeta *Resolucija o velikem podatkovju* (International Conference of Data Protection & Privacy Commissioners, 2014). Mednarodna delovna skupina o varstvu podatkov v telekomunikacijah je v dokumentu *Veliko podatkovje in zasebnost: Načela zasebnosti pod pritiskom analitike velikega podatkovja* (International Working Group on Data Protection in Telecommunications, 2014) opozorila na več izzivov: 1) nevarnost podatkovnega maksimiranja (*vis-à-vis* temeljnemu načelu minimiziranja, ki velja v režimu varstva osebnih podatkov), 2) pomanjkanje transparentnosti, 3) združevanje podatkov, ki lahko odkrije kategorijo posebno občutljivih osebnih podatkov, 4) tveganje reidentifikacije, 5) varnostne implikacije, 6) težavnost povezanih z nepravilnimi podatki, 7) nesorazmerje moči, 8) podatkovni determinizem in diskriminacija, 9) zastraševalni učinek na pravice (angl. *Chilling effect*), 10) ustvarjanje »mnenjskih balonov« in »eho soban« (angl. *Echo chambers*) pri personaliziranih storitvah.

Varstvo pred družbenim sortiranjem je naslednji učinek velikega podatkovja. Avtomatizirano odločanje in zmanjševanje diskrecijske pravice odločevalcev hitro posežeta v pravico do zakonitega pravnega postopka (angl. *due process*) (Lyon, 2014: 8). Upravni postopki pred organi, pristojnimi za izvrševanje kazenskih sankcij, se zaradi avtomatizacije spreminjajo v smeri »opuščanja diskrecijskega modela administrativnega prava« (Citron in Pasquale, 2014). Zakonit pravni postopek pomeni, da morajo imeti državljani pravico podvomiti o avtomatiziranih odločitvah, ampak pogosto se zgodi, da se sploh ne zavedajo, da je bila odločitev o njihovih pravicah sprejeta na podlagi določenih podatkov, niti ne vedo, kakšni podatki so bili podlaga odločitve o njihovih pravicah (posebno opazno v domeni bančništva in zavarovalništva).

Samouresničujoče se prerokbe in nastanek začaranega kroga sta naslednji posledici algoritmičnih napovedi. V domeni družbenega nadzorstva to pomeni, da so »tvegane« skupine bolj pod nadzorom, a ker so bolj nadzorovane, se pri njih odkrije več kaznivih dejanj in so posledično tudi v prihodnosti bolj nadzorovane. Primer tega so napovedni policijski programi, ki so rasno pristranski in krepijo nadzor nad že tako deprivilegiranimi (angl. *overpolicing*).

Težave so sodni primeri, ki izstopajo iz povprečja. Robne primere oziroma slepe pege algoritmičnega sistema lahko prepozna le človeški odločevalec, saj gre v osnovi za vrednostna tehtanja. Argument zagovornikov velikega podatkovja je, da samoučeči se algoritmi to že v naslednjem primeru prepoznajo sami. To vodi v zaostajanje *ad infinitum* — pri pravnem odločanju lahko vedno nastopi nova okoliščina primera in to kot »novo« opredeli človeška presoja, ki v bistvenem obrne izid presoje primera.

Predsodki, ki jih imajo ljudje, so lahko v napovedni model integrirani hote ali nehote. Algoritem se lahko prek obvodov dokoplje tudi do podatkov, ki so izrecno prepovedani (npr. odločanje na podlagi rase, spola, etnične pripadnosti).

Pretirana uporaba podatkov lahko še krepi predsodke. Če, denimo, podatkovni posrednik v podatkovni zbirki najemnikov označi tiste, ki jim je banka zavrnila kredit, ker živijo v predelu, ki velja za finančno tveganega (angl. *red lining*), ta podatkovna zbirka pa je del podatkov, ki jih analizira algoritem za zaposlovanje in pregledovanje prijaviteljev za službo, bodo rezultati najema delavcev zelo verjetno rasno pristranski. Vendarle pa bo pozneje razloge za to skoraj nemogoče rekonstruirati.

Domneva nedolžnosti kot regulator uporabe sredstev fizičnega prisiljevanja v kazenskem postopku pade, če je dejavnost policije preveč vodena po ocenah preteklih podatkov, npr. če že sama pripadnost družbeni skupini – znani po večji nasilnosti – zadostuje za povečan nadzor konkretnega posameznika. Marks et al. (2015) v poročilu *Avtomatizirana pravičnost?* ugotavljajo, da matematični analitični postopki brišejo meje med nedolžnimi, osumljenimi, obtoženimi, obsojenimi, meje začetka in konca postopka kazenskopravnega odzivanja na kriminaliteto in meje med zbiranjem dokazov, testiranjem njihove vrednosti, razsojanja in kaznovanja. Njihova ključna ugotovitev je, da tovrstni postopki minimizirajo človeški vpliv in kršijo načelo dolžnega ravnanja (angl. *due process*) (Marks et al., 2015).

11 Kako omejiti algoritmični nadzor?

V prispevku so opisane številne domene, v katerih imajo algoritmi negativen učinek. Tako poskuša prispevek zaokrožiti metapripoved o algoritmični družbi, tj. družbi, katere bistvene odločitve se sprejemajo na podlagi velike količine podatkov in algoritmov, ki te podatke osmišljajo. Za razumevanje učinkov takšnega matematično-računskega razumevanja sveta je pomembno poznati izvor velikega podatkovja. Algoritmi so bili namreč najprej uporabljeni v industrijskem sektorju, v katerem je bil cilj povečati prodajo in izboljšati tarčno oglaševanje ter zadetke v iskalnikih (Watson, 2015). Slabo delovanje je lahko pomenilo, da dobički niso bili visoki. Ko pa so enkrat algoritmi uporabljeni za iskanje potencialnih teroristov, za odločanje o posameznikovih pravicah, odločanje o pogojnem odpustu ali omejitvi svobode gibanja, potem ima njihovo slabo delovanje, npr. v obliki napačnih zadetkov (angl. *false positives*), usodne posledice za posameznikov (pravni in dejanski) položaj.

Razvoj velikega podatkovja ima daljnosežne posledice, saj lahko pričakujemo razvoj umetne inteligence in popolne avtomatiziranosti, ki iz odločanja izpušča človeški nadzor, kar naj bi se zgodilo v novi »točki singularnosti« (Alarie, 2016). Zato je treba dvigniti zavest o tej možnosti, ki vsaj po mnenju nekaterih realno obstaja (Illing, 2017). Denimo, pri izdelavi orožja vidimo, da to ni samo avtomatizirano, torej takšno, da lahko izvaja določene funkcije na daljavo, a še vedno pod nadzorom človeka (npr. napadi z brezpilotnimi letali pomenijo le, da pilota ni na krovu), temveč so sistemi tudi avtonomni, ko v odločitvah o napadu sploh ni več človeške presoje. Policijska tehnologija se razvija v enaki smeri, npr. avtomatizirana tehnologija za zatiranje protestov, ki ima pomembne učinke za uresničevanje človekovih pravic (Crowley, 2015; McLaughlin, 2015).

Pri omejevanju negativnih učinkov algoritmičnega nadzora je treba tudi vztrajati pri posebnostih varovanja osebnih podatkov v EU. Unija namreč kljub nasprotujočim si težnjam – držati močno varstvo pravic posameznika in hkrati omogočati

konkurenčno okolje digitalnim podjetjem – relativno bolje od drugih delov sveta varuje pravico do varstva osebnih podatkov. Kjer obstajajo etične in pravne omejitve tehnološkega razvoja, daje prednost avtonomiji in kantovskemu subjektu, kar poskuša doseči z instituti, kot je »vgrajena zasebnost« (angl. *privacy by design*), in instrumentom vnaprejšnje presoje vplivov na zasebnost (angl. *privacy impact assessment*). Etična tveganja novih tehnologij je mogoče upoštevati že pri tehnološki zasnovi.

Al-Rodhan (2014) meni, da je potrebna nova družbena pogodba 2.0. Veliko podatkovje pomaga vladam, ki imajo podatke, onemogočati razvoj alternativnih političnih idej. Primer pred Evropskim sodiščem za človekove pravice Zakharov proti Rusiji (Evropsko sodišče za človekove pravice, 2015) je to ustrezno pokazal: ruska vlada – ali katera koli druga s takšno tehnologijo – lahko z nadzorom vseh telekomunikacij nadzoruje vse posameznike, meri razpoloženje ljudi in išče (in zatre) centre politične alternative.

Algoritme je treba narediti transparentne (Pasquale, 2015). Inteligentno urejena družba mora zagotoviti, da so ključne odločitve poštene, nediskriminatorne in odprte za kritiko. Odločitve glavnih igralcev na Wall Streetu in v Silicijevi dolini, ki so zavite v tajnost in kompleksnost, so dolgo veljale za nevtralne – samo »tehnične«. Vendar so posamični primeri, ki so prišli v javnost, pokazali, da avtomatizirano presojanje ni nevtralno: uniči ugled posameznika, povzroči propad podjetja ali zamaje nacionalno ekonomijo; primer zadnjega so hitra nihanja vrednosti funta v obdobju otoškega referenduma o brexitu (angl. *flash-crash* učinkov visokofrekvenčnega oziroma algoritmičnega trgovanja) (Kamal, 2016). V računalniški kodi, zaščiteni s pravnimi pravili, sta lahko skrita aroganca in izkoriščanje. Regulatorji so šibki v primerjavi z giganti in močne interesne skupine izkoriščajo pravne režime tajnosti podatkov in intelektualne lastnine (Pasquale, 2015).

Algoritme moramo razumeti, saj so del računalniškega opismenjevanja. To ne vključuje samo pravice dostopa do izvirne kode, ampak tudi sposobnost kritike kode in njenega spreminjanja. Za upravljanje umetne inteligence (npr. samovozečih se vozil, avtonomnih orožij ali genetskih manipulacij) bo po mnenju nekaterih avtorjev treba ustanoviti posebne upravne organe na državni ravni, denimo v obliki t. i. oddelka za prihodnost (Webb, 2016).

12 Sklep

Algoritmična družba prinaša veliko koristi, a tudi izzive in družbeno škodljive posledice. Povečuje neenakost, ruši temeljne demokratične ureditve, npr. enake možnosti, načelo delitve oblasti in načelo svobode. Priča smo izgradnji planetarnega digitalnega živčnega sistema, ki krepi nadzorstveni kapitalizem in algoritmično nadzorstvo. V podatkovnem nadzorstvenem kapitalizmu se pričakuje, da bodo algoritmi tisti, ki bodo postavljali boljše diagnoze od zdravnikov ter preprečili finančne krize, teroristične napade in druga kazniva dejanja. A kam vodi pot, lahko opazujemo v ultimativnem »socialnem laboratoriju« v Singapurju, kjer tehnokratska elita z uporabo velikega podatkovja in napovedne analitike izvaja popoln množični nadzor. »Sistem popolnega informacijskega zavedanja« (angl. *total information awarness system*) združuje videoposnetke iz videonadzora javnega prostora, podatke iz prometne signalizacije, podatke o internetnem prometu (e-pošta, spletna iskanja itn.), podatke o rezervacijah poletov in hotelskih rezervacijah, zdravniške izvide itn. Sistem, ki ga je razvila DARPA (to je tista ameriška agencija, ki je zaslužna za razvoj interneta), so sicer začeli razvijati zaradi zgodnjega odkrivanja epidemij (Sars), a se danes uporablja za preprečevanje nemirov, zatiranje sovražnega govora, za načrtovanje proračuna, gospodarske napovedi, načrtovanje politike priseljevanja, raziskovanje nepremičninskega trga in številne druge državne politike (Harris, 2014). Podoben sistem razvija Kitajska, ki naj bi do leta 2020 razvila omnipotenten sistem »družbenega točkovanja« – ocenjevanja, koliko je posamičen državljan vreden zaupanja. Ta ogromna podatkovna zbirka naj bi vsebovala finančne, davčne podatke ljudi, vključno z manjšimi prometnimi prestopki, ki bi jih prevedla v posamično številko, namenjeno rangiranju vsakega državljana (Hatton, 2015). Sistem polno zavedajočega se družbenega organizma, pri katerem bo mogoče meriti še čustveni utrip posameznikov in razpoloženje ljudi, se razvija tako, kot ga slika znanstvenofantastična nanizanka *Black Mirror*.

Nad razvojem in uporabo algoritmov mora biti ne nazadnje človeško argumentiranje in tudi človeška »intuicija« ali konkretneje – sodniku »sodniški pravni občutek«. Gre za svobodo in pestrost življenja in kulture. Torej, na vprašanje, koliko bomo zaradi pametnih naprav pametnejši, je mogoče zanesljivo odgovoriti mimobežno: zagotovo bo zaradi njih manjšina bogatejša, poneumljena množica pa bo puščena potrošniškim napravam, ki zagotavljajo vedno nove osebne podatke.

Literatura

1. Al-Rodhan, N. (2014). The social contract 2.0: Big data and the need to guarantee privacy and civil liberties. *Harvard International Review*. Pridobljeno na http://hir.harvard.edu/article/?a=7327
2. Alarie, B. (2016). The path of the law: Towards legal singularity. *University of Toronto Law Journal*, *66*(4), 1–13.
3. Aletras, N., Tsarapatsanis, D., Preoţiuc-Pietro, D. in Lampos, V. (2016). Predicting judicial decisions of the European Court of Human Rights: A natural language processing perspective. *PeerJ Computer Science*, *2*, 1–93.

4. Anderson, C. (23. 6. 2008). The end of theory: The data deluge makes the scientific method obsolete. *Wired*. Pridobljeno na http://www.wired.com/2008/06/pb-theory/
5. Angwin, J., Larson, J., Kirchner, L. in Mattu, S. (5. 4. 2017). Minority neighborhoods pay higher car insurance premiums than white areas with the same risk. *ProPublica*. Pridobljeno na https://www.propublica.org/article/minority-neighborhoods-higher-car-insurance-premiums-white-areas-same-risk
6. Angwin, J., Larson, J., Mattu, S. in Kirchner, L. (23. 5. 2016). Machine bias: There's software used across the country to predict future criminals. and it's biased against blacks. *ProPublica*. Pridobljeno na https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing
7. Aradau, C. in Blanke, T. (2015). The (big) data-security assemblage: Knowledge and critique. *Big Data & Society*, *2*(2), 1–12.
8. Ashley, K. D. in Brüninghaus, S. (2006). Computer models for legal prediction. *Jurimetrics*, *46*(3), 309–352.
9. Badalič, V. (2010). *Za 100 evrov na mesec. Proizvodni sistem globalnega kapitalizma.* Ljubljana: Založba Krtina.
10. Ball, K. in Snider, L. (ur.). (2013). *The surveillance-industrial complex: A political economy of surveillance*. Abingdon, Oxon; New York: Routledge.
11. Barocas, S. in Selbst, A. D. (2014). *Big data's disparate impact*. Rochester: Social Science Research Network.
12. Beck, C. in McCue, C. (2009). Predictive policing: What can we learn from wal-mart and amazon about fighting crime in a recession? *The Police Chief Magazine*, *76*(11). Pridobljeno na http://acmcst373ethics.weebly.com/uploads/2/9/6/2/29626713/police-chief-magazine.pdf
13. Berk, R. A. in Bleich, J. (2013). Statistical procedures for forecasting criminal behavior. *Criminology & Public Policy*, *12*(3), 513–544.
14. Boyd, D. in Crawford, K. (2011). *Six provocations for big data*. Rochester: Social Science Research Network.
15. Bridle, J. (9. 2. 2014). The algorithm method: how internet dating became everyone's route to a perfect love match. *The Guardian*. Pridobljeno na https://www.theguardian.com/lifeandstyle/2014/feb/09/match-eharmony-algorithm-internet-dating
16. Captain, S. (2015). *Hitachi says it can predict crimes before they happen*. Fast Company. Pridobljeno na http://www.fastcompany.com/3051578/elasticity/hitachi-says-it-can-predict-crimes-before-they-happen
17. Casilli A. A. (20. 11. 2016). Never mind the algorithms: the role of click farms and exploited digital labor in Trump's election. *Casilli.fr.* Pridobljeno na http://www.casilli.fr/2016/11/20/never-mind-the-algorithms-the-role-of-exploited-digital-labor-and-global-click-farms-in-trumps-election/
18. Citron, D. K. in Pasquale, F. A. (2014). The scored society: Due process for automated predictions. *Washington Law Review*, *89*(1), 1–34.
19. Cohen, J. E., Hoofnagle, C. J., McGeveran, W., Ohm, P., Reidenberg, J. R., Richards, N. M., Willis, L. E. et al. (2015). *Information privacy law scholars' brief in Spokeo, Inc. v. Robins*. Rochester: Social Science Research Network.
20. Confessore, N. in Hakim, D. (6. 3. 2017). Data firm says »secret sauce« aided Trump; Many scoff. *The New York Times*. Pridobljeno na https://www.nytimes.com/2017/03/06/us/politics/cambridge-analytica.html
21. Crowley, M. (2015). *Tear gassing by remote control*. London: Remote Control Project.
22. Davenport, T. H. in Patil, D. J. (1. 10. 2012). Data scientist: The sexiest job of the 21st century. *Harvard Business Review*. Pridobljeno na https://hbr.org/2012/10/data-scientist-the-sexiest-job-of-the-21st-century
23. Delovna skupina iz 29. člena. (2014). *Statement on Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU*, 16. september 2014. Pridobljeno na http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp221_en.pdf
24. Desrosières, A. (2002). *The politics of large numbers: A history of statistical reasoning*. Cambridge: Harvard University Press.
25. Dredge, S. (5. 11. 2014). Twitter: Why #SoggyFries make for a tasty future in big-data revenue. *The Guardian*. Pridobljeno na http://www.theguardian.com/technology/2014/nov/05/twitter-soggy-fries-big-data-advertising
26. Eman, K., Györkös, J., Lukman, K. in Meško, G. (2013). Crime mapping for the purpose of policing in Slovenia – Recent developments. *Revija za kriminalistiko in kriminologijo*, *64*(3), 287–308.
27. Direktiva (EU) 2016/681 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o uporabi podatkov iz evidence podatkov o potnikih (PNR) za preprečevanje, odkrivanje, preiskovanje in pregon terorističnih in hudih kaznivih dejanj. (2016). *Uradni list EU*, (119/132).
28. Evropsko sodišče za človekove pravice. (2015). Odločba št. 47143/06 z dne 4. 12. 2015.
29. Foucault, M. (2004). *Nadzorovanje in kaznovanje: nastanek zapora*. Ljubljana: Krtina.
30. Garland, D. (1992). Criminological knowledge and its relation to power: Foucault's genealogy and criminology today. *British Journal of Criminology*, *32*(4), 403–422.
31. Goede, M. de in Sullivan, G. (2016). The politics of security lists. *Environment and Planning D: Society and Space*, *34*(1), 67–88.
32. Goode, E. (15. 8. 2011). Data-crunching program guides Santa Cruz Police before a crime. *The New York Times*. Pridobljeno na http://www.nytimes.com/2011/08/16/us/16police.html
33. Hansen, E. E. (9. 8. 2016). Dear Mark Zuckerberg. I shall not comply with your requirement to remove this picture. *Aftenposten*. Pridobljeno na http://www.aftenposten.no/article/ap-604156b.html
34. Harcourt, B. E. (2015). Risk as a proxy for race. *Federal Sentencing Reporter*, *27*(4), 237–243.
35. Harris, S. (29. 7. 2014). The social laboratory. *Foreign Policy*. Pridobljeno na http://foreignpolicy.com/2014/07/29/the-social-laboratory/
36. Hatton, C. (26. 10. 2015). China »social credit«: Beijing sets up huge system. *BBC News*. Pridobljeno na http://www.bbc.com/news/world-asia-china-34592186
37. Helbing, D., Frey, B. S., Gigerenzer, G., Hafen, E., Hagner, M., Hofstetter, Y. et al. (2017). Will democracy survive big data and artificial intelligence? *Scientific American*. Pridobljeno na https://www.scientificamerican.com/article/will-democracy-survive-big-data-and-artificial-intelligence/
38. IBM. (2010). *Memphis police department reduces crime rates with IBM predictive analytics software.* Pridobljeno na https://www-03.ibm.com/press/us/en/pressrelease/32169.wss
39. IBM. (2016). *The four V's of big data*. Pridobljeno na http://www.ibmbigdatahub.com/infographic/four-vs-big-data
40. IBM. (29. 10. 2014). *Twitter and IBM form global partnership* [CTB10]. Pridobljeno na http://m.ibm.com/http/www-03.ibm.com/press/us/en/pressrelease/45265.wss
41. Illing, S. (8. 3. 2017). How worried should we be about artificial intelligence? I asked 17 experts. *Vox*. Pridobljeno na http://www.

vox.com/conversations/2017/3/8/14712286/artificial-intelligence-science-technology-robots-singularity-automation

42. International Conference of Data Protection & Privacy Commissioners. (2014). *Resolution Big Data*. Pridobljeno na https://icdppc.org/wp-content/uploads/2015/02/Resolution-Big-Data.pdf
43. International Working Group on Data Protection in Telecommunications. (2014). *Working Paper on Big Data and Privacy. Privacy principles under pressure in the age of Big Data analytics*, 5.–6. maj 2014, Skopje. Pridobljeno na https://datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt/working-papers-and-common-positions-adopted-by-the-working-group
44. Kamal, A. (7. 10. 2016). Flash crash sees the pound gyrate in Asian trading. *BBC News*. Pridobljeno na http://www.bbc.com/news/business-37582150
45. Kelion, L. (29. 10. 2014). London police trial gang violence »predicting« software. *BBC News*. Pridobljeno na http://www.bbc.com/news/technology-29824854
46. Kitchin, R. (2014). Big data, new epistemologies and paradigm shifts. *Big Data & Society*, *1*(1), 1–12.
47. Kleinberg, J., Lakkaraju, H., Leskovec, J., Ludwig, J. in Mullainathan, S. (2017). *Human Decisions and Machine Predictions* (Working Paper No. 23180). Cambridge: National Bureau of Economic Research.
48. Kramer, A. D. I., Guillory, J. E. in Hancock, J. T. (2014). Experimental evidence of massive-scale emotional contagion through social networks. *Proceedings of the National Academy of Sciences*, *111*(24), 8788–8790.
49. Kravets, D. (30. 7. 2014). Algorithm predicts US Supreme Court decisions 70% of time. *Ars Technica*. Pridobljeno na https://arstechnica.com/science/2014/07/algorithm-predicts-us-supreme-court-decisions-70-of-time/
50. Lazer, D., Kennedy, R., King, G. in Vespignani, A. (2014). The parable of Google flu: Traps in big data analysis. *Science*, *343*(6176), 1203–1205.
51. Leigh, A. (4. 8. 2016). Do Google's »unprofessional hair« results show it is racist? *The Guardian*. Pridobljeno na https://www.theguardian.com/technology/2016/apr/08/does-google-unprofessional-hair-results-prove-algorithms-racist-
52. Leskovec, J. (2015). *Zakaj se sodniki motijo*. Pridobljeno na http://videolectures.net/okroglamizapravo2015_leskovec_sodniki/
53. Levin, S. (8. 9. 2016). A beauty contest was judged by AI and the robots didn't like dark skin. *The Guardian*. Pridobljeno na https://www.theguardian.com/technology/2016/sep/08/artificial-intelligence-beauty-contest-doesnt-like-black-people
54. Lohr, S. in Singer, N. (10. 11. 2016). How data failed us in calling an election. *The New York Times*. Pridobljeno na http://www.nytimes.com/2016/11/10/technology/the-data-said-clinton-would-win-why-you-shouldnt-have-believed-it.html
55. Lyon, D. (2014). Surveillance, Snowden, and big data: Capacities, consequences, critique. *Big Data & Society*, *1*(2), 1–13.
56. Manyika, J., Chui, M., Bisson, P., Woetzel, J., Dobbs, R., Bughin, J. et al. (2015). *Unlocking the potential of the Internet of things | McKinsey & Company*. McKinsey & Company. Pridobljeno na http://www.mckinsey.com/business-functions/business-technology/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world
57. Marks, A., Bowling, B. in Keenan, C. (2015). *Automatic justice? Technology, crime and social control*. Rochester: Social Science Research Network.
58. Marr, B. (20. 12. 2016). Big data: The 6th »V« everyone should know about. *Forbes*. Pridobljeno na http://www.forbes.com/sites/bernardmarr/2016/12/20/big-data-the-6th-v-everyone-should-know-about/
59. Mayer-Schönberger, V. in Cukier, K. (2013). *Big data: A revolution that will transform how we live, work, and think* (1st ed.). Boston: Eamon Dolan/Houghton Mifflin Harcourt.
60. McCulloch, J. in Wilson, D. (2015). *Pre-crime: Pre-emption, precaution and the future*. Abingdon, Oxon; New York: Routledge.
61. McLaughlin, J. (12. 2. 2015). Specter of drones firing tear gas on crowds worries human rights group. *The Intercept*. Pridobljeno na https://theintercept.com/2015/12/01/specter-of-drones-firing-tear-gas-on-crowds-worries-human-rights-group/
62. Meek, A. (14. 9. 2015). Data could be the real draw of the internet of things – but for whom? *The Guardian*. Pridobljeno na https://www.theguardian.com/technology/2015/sep/14/data-generation-insights-internet-of-things
63. Morozov, E. (20. 7. 2014). The rise of data and the death of politics. *The Guardian*. Pridobljeno na http://www.theguardian.com/technology/2014/jul/20/rise-of-data-death-of-politics-evgeny-morozov-algorithmic-regulation?CMP=twt_gu
64. Morozov, E. (2013). *To save everything, click here: Technology, solutionism, and the urge to fix problems that don't exist*. London: Allen Lane.
65. Naughton, J. (21. 2. 2016). Death by drone strike, dished out by algorithm. *The Guardian*. Pridobljeno na http://www.theguardian.com/commentisfree/2016/feb/21/death-from-above-nia-csa-skynet-algorithm-drones-pakistan
66. Newitz, A. (2016). Facebook fires human editors, algorithm immediately posts fake news. *Ars Technica*. Pridobljeno na http://arstechnica.com/business/2016/08/facebook-fires-human-editors-algorithm-immediately-posts-fake-news/
67. O'Hara, D. in Mason, L. R. (30. 3. 2012). How bots are taking over the world. *The Guardian*. Pridobljeno na https://www.theguardian.com/commentisfree/2012/mar/30/how-bots-are-taking-over-the-world?CMP=Share_AndroidApp_E-po%C5%A1ta
68. Pang, B. in Lee, L. (2008). Opinion mining and sentiment analysis. *Foundations and Trends in Information Retrieval*, *2*(1–2), 1–135.
69. Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Cambridge: Harvard University Press.
70. Pečar, J. (1988). *Formalno nadzorstvo. Kriminološki in kriminalitetnopolitični pogledi*. Ljubljana: Delavska enotnost.
71. Pečar, J. (1991). *Neformalno nadzorstvo. Kriminološki in sociološki pogledi*. Ljubljana: Didakta.
72. Perry, W. L., McInnis, B., Price, C. C., Smith, S. in Hollywood, J. S. (2013). *Predictive policing*. Pridobljeno na http://www.rand.org/pubs/research_reports/RR233.html
73. Plesničar M., M. in Klančnik, A. T. (2015). Sodobne rešitve pri pregonu spolne kriminalitete nad otroki. *Pravna praksa*, *34*(47), 11–14.
74. PredPol. (2017). *PredPol: More than just hot spot policing*. Pridobljeno na http://www.predpol.com/hot-spot-policing/
75. Ridgeway, G. (2013). Linking prediction and prevention. *Criminology & Public Policy*, *12*(3), 545–550.
76. Ritzer, G. (2007). *The McDonaldization of society*. Thousand Oaks: Sage.
77. Sample, I. (20. 5. 2016). AI will create »useless class« of human, predicts bestselling historian. *The Guardian*. Pridobljeno na https://www.theguardian.com/technology/2016/may/20/silicon-assassins-condemn-humans-life-useless-artificial-intelligence

78. Saunders, J., Hunt, P. in Hollywood, J. S. (2016). Predictions put into practice: a quasi-experimental evaluation of Chicago's predictive policing pilot. *Journal of Experimental Criminology*, (2016), 1–25.
79. Schneier, B. (9. 3. 2006). Why data mining won't stop terror. *Wired*. Pridobljeno na http://archive.wired.com/politics/security/commentary/securitymatters/2006/03/70357?currentPage=all
80. SentiStrenght. (2017). *A sentiment analysis (opinion mining) program*. Pridobljeno na http://sentistrength.wlv.ac.uk
81. Shane, S. (13. 8. 2012). TrapWire antiterrorist software leaks set off web furor. *The New York Times*. Pridobljeno na http://www.nytimes.com/2012/08/14/us/trapwire-antiterrorist-software-leaks-set-off-web-furor.html
82. Sherwood, H. (7. 12. 2016). Pope Francis compares fake news consumption to eating faeces. *The Guardian*. Pridobljeno na https://www.theguardian.com/world/2016/dec/07/pope-compares-fake-news-consumption-to-eating-faeces-coprophilia
83. Silverman, C. in Alexander, L. (4. 11. 2016). How teens in the Balkans are duping Trump supporters with fake news. *BuzzFeed*. Pridobljeno na https://www.buzzfeed.com/craigsilverman/how-macedonia-became-a-global-hub-for-pro-trump-misinfo
84. Sintef. (22. 5. 2013). Big Data, for better or worse: 90% of world's data generated over last two years. *ScienceDaily*. Pridobljeno na www.sciencedaily.com/releases/2013/05/130522085217.htm
85. Skinner, L. (2014). *As regulators tap into big data, advisers need to up compliance attention.* Pridobljeno na http://www.investmentnews.com/article/20141106/FREE/141109944/as-regulators-tap-into-big-data-advisers-need-to-up-compliance
86. Smith, C. (18. 1. 2014). Social big data: The user data collected by each of the world's largest social networks – And what it means. *Business Insider Australia*. Pridobljeno na http://www.businessinsider.com.au/social-big-data-the-type-of-data-collected-by-social-networks-2-2014-1
87. Solon, O. (12. 12. 2016). 2016: The year Facebook became the bad guy. *The Guardian*. Pridobljeno na https://www.theguardian.com/technology/2016/dec/12/facebook-2016-problems-fake-news-censorship
88. Srnicek, N. in Williams, A. (2015). *Inventing the future: Postcapitalism and a world without work*. Brooklyn: Verso.
89. Starr, S. B. (2013). *Evidence-based sentencing and the scientific rationalization of discrimination*. Rochester: Social Science Research Network.
90. Statewatch. (2014). *Note on big data, crime and security: Civil liberties, data protection and privacy concerns.* Statewatch. Pridobljeno na http://www.statewatch.org/analyses/no-242-big-data.pdf
91. Svet Evrope. (1994). Evropska konvencija o varstvu človekovih pravic in temeljnih svoboščin. *Uradni list RS,* (33/94).
92. Sweeney, L. (2013). Discrimination in Online Ad Delivery. *ACM Queue*, 11(3). Pridobljeno na: https://arxiv.org/pdf/1301.6822.pdf
93. Trapwire (2017). *Trapwire. The intelligent security method.* Pridobljeno na https://www.trapwire.com
94. Wagner, J. (9. 11. 2016). Clinton's data-driven campaign relied heavily on an algorithm named Ada. What didn't she see? *Washington Post*. Pridobljeno na https://www.washingtonpost.com/news/post-politics/wp/2016/11/09/clintons-data-driven-campaign-relied-heavily-on-an-algorithm-named-ada-what-didnt-she-see/
95. Ward, M. (3. 8. 2014). Crime fighting with big data weapons. *BBC News*. Pridobljeno na http://www.bbc.com/news/business-26520013
96. Watson, S. M. (2015). Data is the New »___«. *DIS Magazine*. Pridobljeno na http://dismagazine.com/discussion/73298/sara-m-watson-metaphors-of-big-data/
97. Webb, A. (13. 12. 2016). Why the government needs a Department of the Future. *The Agenda*. Pridobljeno na http://politi.co/2hqYrJT
98. Wood, D. (2014). *Introduction to big data.* Pridobljeno na https://www.brighttalk.com/webcast/8913/119899
99. Wu, X. in Zhang, X. (2016). Automated inference on criminality using face images. *arXiv*. Pridobljeno na http://arxiv.org/abs/1611.04135
100. Završnik, A. (2015). Nadzor potnikov post-Charlie Hebdo. *Pravna praksa*, *34*(3-4), 45.
101. Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, *30*(1), 75–89.
102. Zuboff, S. (3. 5. 2016). The secrets of surveillance capitalism. *Frankfurter Allegemeine Zeitugn*. Pridobljeno na http://www.faz.net/-gsf-8eaf4

Algorithmic Surveillance: Big Data, Algorithms, and Social Control

Aleš Završnik, Ph.D., Senior Research Fellow at the Institute of Criminology at the Faculty of Law in Ljubljana and Associate Professor at the Faculty of Law, University of Ljubljana, Slovenia. E-mail: ales.zavrsnik@pf.uni-lj.si

This paper focuses on the uses and consequences of big data and predictive analytics in social control. After tackling the issue of defining "big data", the paper presents the implications of big data in the production of knowledge. It then focuses on selected domains of informal and formal social control, such as policing and criminal justice systems, which are being reshaped by big data and predictive analytics. By focusing on the impacts of predictive analytics on economic-political systems and democratic processes, the author claims that democracy and the rule of law are being reshaped into an "algorcracy" – the rule of the algorithm. This paper then focuses on automatization in policing and criminal justice settings by presenting specific predictive analytics already in use or in testing in pre-trail detention, sentencing, and parole procedures. It concludes by presenting the negative consequences of big data and predictive analytics in social control and by offering remedies for such.

Keywords: algorithms, big data, predictive policing, automated justice

UDC: 343.9+004.493