REPUBLIKA SLOVENIJA
ZAGOVORNIK NAČELA ENAKOSTI

REPUBLIKA SLOVENIJA
ZAGOVORNIK NAČELA ENAKOSTI

Podpisnik:Miha Lobnik
Izdajatelj certifikata:Republika Slovenija
Serijska št. certifikata:5c 9c 18 4a 00 00 00 00
Datum poteka certifikata:10.03.2026
Datum in čas podpisa:15:45, 28.05.2021
Referenčna številka:0070-1/2019/5

Železna cesta 16, 1000 Ljubljana
01 4735 531
gp@zagovornik-rs.si

Ministrstvo za pravosodje
Župančičeva ulica 3
1000 Ljubljana

E: gp.mp@gov.si

Številka: 0070-1/2019/5
Datum: 28. 5. 2021

Zadeva: **Priporočilo Zagovornika načela enakosti glede osnutka predloga novega Zakona o varstvu osebnih podatkov (ZVOP-2)**

Spoštovani,

Zagovornik načela enakosti je 3. 5. 2021 prejel dopis Ministrstva za pravosodje št. IPP 007-87/2019, v katerem ste nam v strokovno usklajevanje posredovali predlog novega Zakona o varstvu osebnih podatkov (EVA: 2018-2030-0045 – redni postopek) (v nadaljevanju: ZVOP-2). V dopisu navajate, da se s predlogom na sistemski ravni izvajajo določbe Splošne uredbe o varstvu osebnih podatkov (GDPR) ter uvajajo druge nove rešitve ter da predlog ohranja visoke standarde varstva osebnih podatkov v Sloveniji. Za posredovani dopis in povabilo k strokovnemu usklajevanju se vam zahvaljujemo.

Zagovornik je osnutek predloga zakona proučil tako z vidika povezave prava varstva osebnih podatkov in Zagovornikovega izvajanja nalog in pristojnosti v skladu z Zakonom o varstvu pred diskriminacijo (ZVarD), kot tudi z vidika varstva pred diskriminacijo širše. Zagovornik posebej podpira, da se v predlogu izrecno ureja vprašanje obdelave osebnih podatkov o narodnosti in/ali etničnem poreklu v javnem sektorju. Na to potrebo je Zagovornik opozoril že v svojih priporočilih na prejšnje različice ZVOP-2, in sicer z vidika potrebe po pridobivanju (statističnih in agregiranih) podatkov o enakopravnosti, enaki obravnavi in enakih možnostih (ang. *equality data*).

Upoštevajoč navedeno in z namenom izboljšanja predloga zakona Zagovornik pripravljavcu ZVOP-2 priporoča, da:

1. **v obrazložitvi k 7. členu predloga doda, da se pogoj »odločanje o položaju in pravicah posameznika« iz šestega odstavka tega člena nanaša tudi na situacije, kadar je zbiranje osebnih podatkov o narodni oziroma etnični pripadnosti potrebno v okviru izvajanja posebnih ukrepov v smislu 17. člena ZVarD;**
2. **na koncu šestega odstavka 7. člena predloga zakona doda, da določba tega odstavka ne velja za ukrepanje državnih organov na področju ugotavljanja in odpravljanja diskriminacije, če jim takšno pristojnost določa zakon;**
3. **v 20. členu predloga ZVOP-2, ki določa izjeme glede uveljavljanja zahtevka posameznika prek zakonitega zastopnika glede zdravstvene dokumentacije, ne uporabi termina »odvzete poslovne sposobnosti«;**
4. **za 81. členom predloga zakona ali drugem primernem mestu doda nov člen, ki bo uredil varstvo osebnih podatkov v okviru uporabe novih tehnologij, ki temeljijo na umetni inteligenci, z vidika varstva temeljnih pravic, zlasti prepovedi diskriminacije.**

S spoštovanjem,

Miha Lobnik
ZAGOVORNIK NAČELA ENAKOSTI

Priloga:
- Obrazložitev strokovne službe Zagovornika k priporočilu št. 0070-1/2019/5

Poslano:
- naslovniku (e-pošta)
- zbirka dok. gradiva

V vednost:
- Varuh človekovih pravic (info@varuh-rs.si)

UTEMELJITEV STROKOVNE SLUŽBE ZAGOVORNIKA K PRIPOROČILU ŠT. 0070-1/2019/5

1.

Zagovornik pripravljavcu ZVOP-2 priporoča, da v obrazložitvi k 7. členu predloga doda, da se pogoj »odločanje o položaju in pravicah posameznika« iz šestega odstavka tega člena nanaša tudi na situacije, kadar je zbiranje osebnih podatkov o narodni oziroma etnični pripadnosti potrebno v okviru izvajanja posebnih ukrepov v smislu 17. člena ZVarD.

Prva točka Zagovornikovega priporočila je povezana z vprašanjem zbiranja **podatkov o enakopravnosti, enaki obravnavi in enakih možnostih (ang. *equality data*)**. Priročnik[1] Evropske komisije (EK) jih opredeljuje kot informacije kvantitativne ali kvalitativne narave, ki se uporabljajo za opisovanje in analizo aktualnega stanja na področju enake obravnave oseb z določenimi osebnimi okoliščinami. Vključujejo agregirane (statistične) podatke, ki odražajo neenakosti v družbi ter njihove vzroke in učinke. Za pripravo statistik o stanju na področju enake obravnave in enakih možnosti se uporabljajo različni podatkovni viri, med katerimi so zelo pomembne uradne evidence, ki jih vodijo organi v javnem sektorju in ki vsebujejo osebne podatke ljudi z določenimi osebnimi okoliščinami. Cilj pridobivanja agregiranih podatkov iz zbirk osebnih podatkov v nobenem primeru ni in ne sme biti identifikacija posameznikov, na katere se osebni podatki nanašajo, temveč **kvantitativna statistična analiza, na podlagi katere se lahko oblikujejo učinkovite protidiskriminacijske politike**.[2]

Zagovornik pri svojem delovanju že več let opozarja na pomanjkanje podatkov o enakopravnosti, enaki obravnavi in enakih možnostih (*equality data*) v Sloveniji. To izpostavlja tudi v komunikaciji z različnimi ministrstvi in vladnimi službami ter v svojih rednih letnih poročilih.[3] Potrebo po oblikovanju sistemske pravne podlage, ki bi omogočila zbiranje in obdelavo osebnih podatkov za namene priprave statističnih analiz na področju enake obravnave in enakih možnosti ljudi z določenimi osebnimi okoliščinami je Zagovornik izpostavil že v svojem priporočilu k prvi različici predloga ZVOP-2 marca 2019.[4]

Na pomanjkanje oziroma odsotnost podatkov o enakopravnosti, enaki obravnavi in enakih možnostih (*equality data*) Slovenijo **opozarjajo tudi mednarodne institucije**. Poročilo EK o pravnih okvirih in praksah zbiranja in obdelave tovrstnih podatkov kaže, da jih v Sloveniji na sistemski ravni skorajda ni, pri čemer izpostavlja skoraj popolno odsotnost podatkov v zvezi z etnično pripadnostjo.[5] Poročilo EK, ki analizira zakonsko ureditev zbiranja teh podatkov ter njihovo zanesljivost, veljavnost, celovitost in uporabo, kaže, da je Slovenija najslabše ocenjena prav na področju zakonske ureditve zbiranja teh podatkov, med osebnimi okoliščinami pa sta kot delno urejeni omenjeni zgolj starost in invalidnost.[6] K vzpostavitvi sistema zbiranju podatkov, razčlenjenih po etnični pripadnosti, namenjenih varstvu pred diskriminacijo, Slovenijo med drugim poziva tudi Evropska komisija za boj proti rasizmu in nestrpnosti pri Svetu Evrope, ki je leta 2019 glede tega državi podala prednostno priporočilo.[7]

K zbiranju podatkov, razčlenjenih po narodnosti oziroma etnični pripadnosti, pozivajo države članice EU tudi nekateri nedavno objavljeni **strateški dokumenti EK**. *Strateški okvir EU za enakost, vključevanje in udeležbo Romov*[8] tako npr. prvič predvideva spremljanje učinkovitosti nacionalnih

[1] EK (2016) *European Handbook on Equality Data – 2016 Revision*, str. 15, dostopno na: http://ec.europa.eu/newsroom/just/document.cfm?action=display&doc_id=43205.
[2] EK (2018) *Guidelines on improving the collection and use of equality data*, High Level Group on Non-discrimination, Equality and Diversity, Subgroup on Equality Data, str. 4-5. Dostopno na: https://ec.europa.eu/info/sites/default/files/final_guidelines_4-10-18_without_date_july.pdf.
[3] Zagovornikova redna letna poročila so dostopna na http://www.zagovornik.si/letno-porocilo-2/. Glej str. 132-133 (RLP 2020), str. 185-187 (RLP 2019) in str. 135-136 (RLP 2018).
[4] Priporočilo je dostopno na http://www.zagovornik.si/wp-content/uploads/2020/09/Komentar-in-priporo%C4%8Dilo-Zagovornika-na%C4%8Dela-enakosti-v-zvezi-s-predlogom-Zakona-o-varstvu-osebnih-podatkov-ZVOP-2.pdf
[5] Evropska komisija (2017) *Analysis and comparative review of equality data collection practives in the European Union: Legal framework and practice in the EU member states*, str. 160-161. Dostopno na: https://ec.europa.eu/newsroom/just/document.cfm?action=display&doc_id=45792.
[6] Evropska komisija/Thomas Huddleston (2017) *Analysis and comparative review of equality data collection practives in the European Union: Equality data indicators: Methodological approach*, str. 6 in 49. Dostopno na: https://ec.europa.eu/newsroom/just/document.cfm?action=display&doc_id=45793.
[7] https://rm.coe.int/fifth-report-on-slovenia-slovenian-translation-/168094caff
[8] https://ec.europa.eu/info/sites/default/files/eu_roma_strategic_framework_for_equality_inclusion_and_participation_for_2020_-_2030_0.pdf

ukrepov za izboljšanje položaja romskega prebivalstva na različnih področjih družbenega življenja s **kvantitativnimi indikatorji**. Prav tako EK v *Akcijskem načrtu za boj proti rasizmu za obdobje 2020-2025*[9] poziva države članice k zbiranju podatkov, razčlenjenih po narodnosti oziroma etnični pripadnosti, za namene oblikovanja učinkovitih politik na področju, ki ga ureja akcijski načrt.

*

Šesti odstavek 7. člena predloga ZVOP-2 določa, da je obdelava osebnega podatka o narodni ali etnični pripadnosti posameznika, na katerega se nanašajo osebni podatki, v javnem sektorju izjemoma dopustna, če to določa zakon, ki določa tudi podajanje privolitve posameznika, na katerega se nanašajo osebni podatki. Z zakonom se obdelavo iz prejšnjega stavka določi za primere, ko je to nujno za odločitev o osebnem stanju ali pravicah posameznika, na katerega se nanašajo osebni podatki.

Pozdravljamo, da se z navedeno določbo izrecno urejajo pravna podlaga in pogoji za zbiranje in obdelavo osebnih podatkov o narodnosti in/ali etnični pripadnosti. K temu je Zagovornik pozval že v prejšnjih priporočilih k predlogu ZVOP-2. Ob tem se zavedamo, da določba ni neposredno uporabna in zahteva dodatno ureditev v področni zakonodaji, ki mora določati tudi privolitev posameznika k obdelavi osebnega podatka o narodni oziroma etnični pripadnosti. Privolitev posameznika, zahteva po kateri (kot je pojasnjeno tudi v obrazložitvi k 7. členu predloga zakona) izhaja iz pravice do svobodnega izražanja narodne pripadnosti iz 61. člena Ustave RS, je sicer skladna tudi z mednarodno uveljavljenim **načelom samoopredelitve**. To predstavlja najbolj primeren in zaželen pristop k zbiranju uradnih podatkov, razčlenjenih po narodnosti oziroma etnični pripadnosti, ki so namenjeni spodbujanju enake obravnave in enakih možnosti.[10] Hkrati načelo samoopredelitve pomembno poudarja, da je **zbiranje podatkov o enakopravnosti, enaki obravnavi in enakih možnostih (*equality data*)**, ki temeljijo na obdelavi občutljivih osebnih podatkov (posebne vrste osebnih podatkov v smislu GDPR) **proces**, ki ne more temeljiti zgolj na zakonodajnih ukrepih, ampak mora biti voden v tesnem sodelovanju s skupnostmi, na pripadnike katerih se zbiranje in obdelava teh osebni podatkov nanaša. Od tega sodelovanja je nenazadnje odvisna tudi popolnost podatkov za namene statistične analize na področju enake obravnave in enakih možnosti.[11]

Omenjena določba predloga ZVOP-2 po oceni Zagovornika zato predstavlja pomemben prvi korak k izboljšanju stanja na področju zbiranja podatkov o položaju oseb, ki pripadajo določenim narodnim oziroma etničnim skupnostim. Vendar pa pri tem izpostavljamo, da **iz dikcije pogoja za dopustnost obdelave osebnih podatkov o narodni oziroma etnični pripadnosti** – tj., da je obdelava »nujna za *odločitev o osebnem stanju ali pravicah* posameznika« – **ni jasno, ali ta obsega tudi obdelavo podatkov za določene protidiskriminacijske namene**.

Pri tem gre izpostaviti zlasti obdelavo predmetnih osebnih podatkov za namene izvajanja **posebnih ukrepov** v smislu 17. člena Zakona o varstvu pred diskriminacijo (ZVarD), ki so namenjeni uresničevanju »pravice do enakega obravnavanja, enake možnosti ali dejansko enakost in udeležbo na področjih družbenega življenja oseb, ki so v manj ugodnem položaju zaradi določene osebne okoliščine« (t.i. **pozitivna diskriminacija**). Takšni ukrepi morajo biti v skladu z 18. členom ZVarD utemeljeni na ustreznih analizah, ki dokazujejo njihovo primernost in sorazmernost, hkrati pa se s temi analizami preverja njihova utemeljenost in upravičenost nadaljnjega izvajanja.

V obrazložitvi šestega odstavka 7. člena predloga ZVOP-2 sta primeroma izpostavljeni le dve praktični situaciji, in sicer posebna volilna pravica pripadnikov in pripadnic italijanske in madžarske narodne skupnosti ter odločanje o mednarodni zaščiti. Z vidika zakonskih pristojnosti in nalog Zagovornika zato predlagamo, da **se v obrazložitvi dodatno pojasni, da je zbiranje osebnih podatkov o narodni oziroma etnični pripadnosti v okviru te določbe predloga ZVOP-2 dopustno tudi za namen priprave in izvajanja t.i. posebnih ukrepov**. V slovenski zakonodaji in praksi tovrstni primeri že obstajajo. Zakon o urejanju trga dela v prvem odstavku 123. člena določa, da se med skupnimi osebnimi podatki v evidenci brezposelnih oseb, evidenci oseb, ki so začasno nezaposljive, evidenci oseb, vključenih v programe aktivne politike zaposlovanja in evidenci iskalcev zaposlitve (lahko) vodi tudi podatek o »pripadnosti posameznika k romski skupnosti«, če se posameznik o tem izjavi. Namen

[9] https://ec.europa.eu/info/sites/default/files/a_union_of_equality_eu_action_plan_against_racism_2020_-2025_sl.pdf
[10] Glej npr. EK (2016), opomba 1 zgoraj, str. 38-40.
[11] V okviru raziskave Agencije EU za temeljne pravice (FRA) EU-MIDIS je **65% vprašanih izrazilo načelno podporo zbiranju podatkov o njihovi etnični pripadnosti za namene boja proti diskriminaciji**. Glej FRA (2010) *EU-MIDI: Data in Focus Report: Rights Awareness and Equality Bodies*, str. 12. Dostopno na: https://fra.europa.eu/sites/default/files/fra_uploads/854-EU-MIDIS_RIGHTS_AWARENESS_EN.PDF.

vodenja tega podatka je prav v načrtovanju, izvajanju in spremljanju posebnih ukrepov na področju zaposlovanja.

2.

Zagovornik pripravljavcu ZVOP-2 priporoča, da na koncu šestega odstavka 7. člena predloga zakona doda, da določba tega odstavka ne velja za ukrepanje državnih organov na področju ugotavljanja in odpravljanja diskriminacije, če jim takšno pristojnost določa zakon.

Druga točka Zagovornikovega priporočila je povezana z delovanjem državnih organov, ki so po zakonu pristojni za **ukrepanje na področju ugotavljanja in odpravljanja diskriminacije**. Pravni red Republike Slovenije na področju varstva pred diskriminacijo mnogim državnim organom določa tovrstne pristojnosti, v okviru katerih ti odločajo o »položaju in pravicah« posameznikov v smislu šestega odstavka 7. člena predloga ZVOP-2 – tj. o pravici posameznika do enakega obravnavanja ne glede na njegovo narodno ali etnično pripadnost (ali katerokoli drugo njegovo osebno okoliščino).

V skladu z ZVarD so za vodenje postopkov ugotavljanja in odpravljanja diskriminacije pristojni Zagovornik in pristojni inšpektorati. Po Zakonu o delovnih razmerjih (ZDR-1) je Inšpektorat RS za delo izrecno pristojen za inšpekcijski nadzor nad uresničevanjem 6. člena ZDR-1, ki določa prepoved diskriminacije na področju dela in zaposlovanja. Upravno sodišče Republike Slovenije odloča o upravnih sporih zoper odločitve Zagovornika in/ali pristojnih inšpektoratov na področju varstva pred diskriminacijo. Delovna in socialna sodišča odločajo v delovnih sporih, ki se tičejo prepovedi diskriminacije. Sodišča splošne pristojnosti odločajo v primerih tožb zaradi diskriminacije v skladu z 39. členom ZVarD. Policija in tožilstvo pri obravnavi kaznivega dejanja kršitve enakopravnosti (131. člen Kazenskega zakonika) obdelujeta podatek o relevantni osebni okoliščini oškodovanca, ki hkrati predstavlja zakonski znak tega kaznivega dejanja.

Navedeno so zgolj nekateri primeri, v katerih **državni organi na podlagi z zakonom določenih pristojnosti ukrepajo na področju ugotavljanja in odpravljanja diskriminacije** (tudi) zaradi narodne oziroma etnične pripadnosti. V vseh teh primerih državni organi odločajo o pravici posameznika (do enakega obravnavanja). V postopku pred temi organi stranke, ki zatrjujejo diskriminacijo zaradi predmetnih osebnih okoliščin, slednje tudi nujno razkrijejo, saj to predstavlja bistven element postopka, v katerem je potrebno dokazati vzročno povezavo med osebno okoliščino žrtve in ravnanjem domnevnega kršitelja. Obdelava osebnega podatka narodne oziroma etnične pripadnosti stranke med postopkom je neizogibna. Vendar državni organi za obdelavo tega osebnega podatka od stranke ne pridobijo njene izrecne privolitve.

Ob upoštevanju zgornjega menimo, da namen določbe šestega odstavka 7. člena predloga ZVOP-2 sicer ni bil posegati v omenjene postopke in izvajanje pristojnosti državnih organov pri navedenem ukrepanju na področju ugotavljanja in odpravljanja diskriminacije. Pridobivanje privolitve stranke v postopku za obdelavo njenega osebnega podatka o narodni oziroma etnični pripadnosti bi brez potrebe pomenilo dodatne pogoje oziroma zahteve v okviru postopka, hkrati pa ne bi dosegalo namena ZVOP-2, tj. varstva osebnih podatkov osebe, na katero se ti nanašajo. V izogib nejasnostim zato ocenjujemo, da bi se tovrstno ravnanje državnih organov moralo jasno izvzeti iz obsega uporabe predmetne določbe. **Na podlagi navedenega zato predlagamo, da se kot zadnji stavek šestega odstavka 7. člena predloga ZVOP-2 doda sledeče besedilo: »Določba tega odstavka se ne uporablja za ukrepanje državnih organov na področju ugotavljanja in odpravljanja diskriminacije, če jim takšno pristojnost določa zakon.«**.

3.

Zagovornik pripravljavcu ZVOP-2 priporoča, da v 20. členu predloga ZVOP-2, ki določa izjeme glede uveljavljanja zahtevka posameznika prek zakonitega zastopnika glede zdravstvene dokumentacije, ne uporabi termina »odvzete poslovne sposobnosti«.

Predlog ZVOP-2 v 20. členu določa posebno izjemo glede uveljavljanja zahtevka posameznika prek zakonitega zastopnika glede zdravstvene dokumentacije, pri čemer, kot izhaja iz obrazložitve člena, s tem določa strožje varstvo pravic posebej ranljivih oseb.

Medtem, ko gre uveljavitev strožjega varstva pravic v danem primeru podpreti, pa opozarjamo na neustrezno uporabo terminologije v tem členu. Po uveljavitvi Družinskega zakonika (v nadaljevanju: DZ) in novega Zakona o nepravdnem postopku (v nadaljevanju: ZNP-1) s 15. 4. 2019 odvzemi poslovne sposobnosti niso več možni. Po prehodnih določbah DZ vsebina sodnih odločb o odvzeti poslovni sposobnosti oziroma položaju osebe, nad katero je bila podaljšana roditeljska pravica, sicer v celoti ostaja v veljavi. Pri tem se namesto navedenih statusov za navedene osebe šteje, da so postavljene pod (t.i. totalno) skrbništvo. Spremenilo se je zlasti poimenovanje, pogojno rečeno še naslovni »status« teh oseb. Vendar to po Zagovornikovi presoji ne pomeni, da lahko ta status ostaja nespremenjen v nedoločljivo prihodnost. Položaji, v katerih je tem ljudem odvzeta poslovna sposobnost, so vsebinsko sporni z vidika prevzetih obveznosti po Konvenciji o pravicah invalidov (v nadaljevanju: MKPI).

Zagovornik šteje, da se je z ureditvijo po DZ in ZNP-1 dosledneje pristopilo k harmonizaciji nacionalne zakonodaje z MKPI. Namen MKPI je po prvem odstavku 1. člena »spodbujati, varovati in osebam z invalidnostmi zagotavljati polno in enako uživanje vseh temeljnih pravic ter spodbujati spoštovanje njihovega prirojenega dostojanstva.« V 12. členu (z naslovom enakost pred zakonom) MKPI terja, da mora biti osebam z invalidnostmi načeloma zagotovljena polna pravna (in v tem okviru tudi poslovna) sposobnost. MKPI v drugem odstavku 12. člena določa, da države pogodbenice osebam z invalidnostmi priznavajo pravno sposobnost na vseh področjih življenja enako kot drugim. MKPI je temeljna referenčna točka in predstavlja velik premik v razumevanju človekovih pravic oseb z invalidnostmi.

Odbor OZN za pravice oseb z invalidnostmi (Odbor CRPD) že od leta 2011 v svoji ustaljeni razlagi MKPI zastopa stališče, da **odvzemi poslovne sposobnosti zaradi invalidnosti niso dopustni**. O tem je Odbor MKPI zavzel načelno stališče že v Splošnem komentarju št. 1 k 12. členu MKPI o enakem priznanju pred zakonom,[12] ponovno pa tudi v Splošnem komentarju št. 6 o enakosti in nediskriminaciji.[13] Odbor MKPI je ob obravnavi poročila Slovenije (2018)[14] ter poročila EU (2015)[15] izrecno ugotavlja, da gre pri ureditvi odvzemanja pravne in poslovne sposobnosti osebam z invalidnostmi za kršitev pravic varovanih z MKPI. Poudarjamo, da gre ob odvzemu poslovne sposobnosti tudi za vprašanje varstva »pravice do nedotakljivosti posameznikove duševne integritete iz 35. člena Ustave. Po presoji Ustavnega sodišča pomeni vsak, tudi delni odvzem poslovne sposobnosti hud poseg v to človekovo pravico«[16].

DZ izrecno in natančno ureja le vprašanje sposobnosti sklepati pravne posle (tj. sposobnost za sklepanje oziroma urejanje civilnih pravno-poslovnih razmerij). Ta zakon izrecno ne ureja drugih splošnih vidikov izražanja pravne (voljne) oziroma poslovne sposobnosti, npr. v drugih pravnih sferah, za opravljanje najrazličnejših pravnih dejanj in izjav volje s pravnimi posledicami. DZ ne ureja zmožnosti uživati vse človekove pravice (npr. pravice do varstva osebnih podatkov, zasebnosti in do spoštovanja dostojanstva posameznika oziroma posameznice), kot tudi ne vprašanj procesne sposobnosti za njihovo uveljavljanje in varovanje. Vse možnosti posegov v obseg poslovne

[12] Glej General comment No 1 (2014), Article 12: Equal recognition before the law, CRPD/C/GC/1, sprejet 11. aprila 2014. Dostopno na: https://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CRPD/C/GC/1&Lang=en.
[13] Glej 30. točko kjer našteva primere sistemskih diskriminacij.
[14] Odbor je na svoji 386. seji 5. marca 2018 sprejel Sklepne ugotovitve glede uvodnega poročila Slovenije (CRPD/C/SVN/CO/1), glej zlasti 19. točko. Besedilo je v slovenskem jeziku dostopno v Rednem letnem poročilu Zagovornika načela enakosti za leto 2018, str. 167, dostopno na http://www.zagovornik.si/letno-porocilo-2/.
[15] Glej Concluding observations on the initial report of the European Union, CRPD/C/EU/CO/12, Oktober 2015, zlasti 37. točko, dostopno na: https://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CRPD%2FC%2FEU%2FCO%2F1.
[16] Up-1178/18-23, dostopno na: https://www.us-rs.si/media/up-1178-18.pdf

sposobnosti in uživanja različnih pravic je, posebej pa izven sfere pravno-poslovnih razmerij, treba zato tolmačiti izrazito restriktivno.
Zagovornik zato meni, da bi moral biti tak položaj osebe z »odvzeto poslovno sposobnostjo« (oz. pod t,i. totalnim skrbništvom) le začasen, do ustreznejše ureditve položaja teh oseb, usklajenega z novo zakonodajo, tako da bi bile morebitne omejitve poslovne sposobnosti po obsegu omejene. Zagovornik pripravljavce zakonov vztrajno opozarja, da je uporaba terminov, ki dajejo videz, da so odvzemi poslovne sposobnosti še vedno običajni in neproblematični, neprimerna in vsebinsko sporna.

Zato predlagamo, da se v besedilu predloga 20. člena predloga ZVOP-2 črta besedii »**ali odvzeto**«, ki se nanašata na poslovno sposobnost posameznika. Taka ureditev bi po razlagalnem načelu v prid varstva pravic ter »kar vsebuje manj, vsebuje tudi več«, še vedno omogočala tudi ustrezno zaščito oseb, ki so še pod t.i. totalnimi skrbništvi.

Ocenjujemo, da bi bilo treba v splošnem kontekstu urejanja poslovne sposobnosti ponovno proučiti vprašanje delnih odvzemov poslovne sposobnosti (postavitev pod skrbništvo), kot tudi podaljševanja učinkov popolnih odvzemov poslovne sposobnosti. Namesto delnih odvzemov poslovne sposobnosti in postavitev pod skrbništvo velja, skladno z MKPI, pristopiti k spremembi paradigme in s tem k zagotavljanju podpornega odločanja. Podobna opozorila je Zagovornik pripravljavcu že dal prvič v letu 2019 ob opozorilih na problem odvzemov volilne pravice za volitve poslank in poslancev v Evropski parlament, nedavno pa v strokovnem usklajevanju ob osnutku Predloga Zakona o spremembah in dopolnitvah Zakona o državnem tožilstvu (EVA 2020-2030-0023). Izrecna priporočila, da se ta vprašanja skrbno premisli in ustrezno uredi pa je Zagovornik dal tudi drugim pripravljavcem predpisov, med drugim ob javni razpravi o predlogih novega Zakona o duševnem zdravju ter novel Zakona o lokalnih volitvah in Zakona o osebni asistenci.[17]

[17] Priporočila Zagovornika so dostopna na http://www.zagovornik.si/priporocila-2021-2/.

4.

Zagovornik pripravljavcu ZVOP-2 priporoča, da za 81. členom predloga zakona ali drugem primernem mestu doda nov člen, ki bo uredil varstvo osebnih podatkov v okviru uporabe novih tehnologij, ki temeljijo na umetni inteligenci, z vidika varstva temeljnih pravic, zlasti prepovedi diskriminacije.

Nove tehnologije se tako v javnem kot zasebnem sektorju vse pogosteje uporabljajo za avtomatizirano obdelavo (osebnih in neosebnih) podatkov in avtomatizirano odločanje o posameznikovih pravicah oziroma dostopu do teh pravic. Tovrstno odločanje je lahko avtomatizirano delno ali v celoti. To pomeni, da končno odločitev sprejme fizični odločevalec (človek) na podlagi predloga oziroma priporočila, ki je pripravljeno s pomočjo novih tehnologij in avtomatizirane obdelave podatkov. GDPR v 22. členu določa posebna pravila glede avtomatiziranega odločanja na podlagi obdelave osebnih podatkov, vendar le za primere odločitev, ki temeljijo **zgolj** na avtomatizirani obdelavi, vključno z oblikovanjem profilov, ki imajo pravne učinke v zvezi s posameznikom ali na podoben način nanj znatno vplivajo. Prav tako členi 13(2)(f), 14(2)(g) in 15(1)(h) GDPR določajo pravico posameznika, na katerega se obdelovani osebni podatki nanašajo, do določenih informacij o obstoju avtomatiziranega odločanja, vključno z oblikovanjem profilov.

V kontekstu omenjenih novih tehnologij in procesov obdelave podatkov se vse pogosteje uporabljajo t.i. **tehnologije umetne inteligence** (UI). Čeprav definicija umetne inteligence pravno še ni urejena, na ravni Evropske unije (EU) v zadnjih letih potekajo intenzivna prizadevanja za pravno definicijo in regulacijo tovrstnih tehnologij. Evropska komisija (EK) je aprila 2021 objavila predlog *Uredbe o harmoniziranih pravilih za umetno inteligenco (Akt o UI) in spremembi nekaterih zakonodajnih aktov Unije* (v nadaljevanju: Uredba o UI).[18] Uredba predlaga uvedbo »na prihodnost odporne« (*future proof*) definicije sistemov umetne inteligence kot »programske opreme, ki je razvita z uporabo ene ali več tehnik in pristopov iz Priloge 1 in lahko, za namene določenih človeško-definiranih ciljev, ustvarja rezultate, kot so vsebina, napovedi, priporočila ali odločitve, ki vplivajo na okolje, s katerim je v interakciji«. Namen predloga UI je t.i. *ex ante* regulacija UI, ki bo za visoko tvegane sisteme UI vzpostavila določene obvezne zahteve glede (uporabljenih) podatkov, dokumentacije in sledljivosti, zagotavljanja informacij in transparentnosti, človeškega nadzora, robustnosti in natančnosti. Visoko-tvegani sistemi UI so po področjih in namenih uporabe definirani v Prilogi 4 predloga Uredbe o UI.

Čeprav uporaba tehnologij UI dokazano prinaša številne prednosti, ki lahko izboljšajo življenje posameznikov, pa hkrati **dokazano prinaša tudi pomembna tveganja za temeljne pravice**, zlasti na področju varstva pred diskriminacijo ter varstva osebnih podatkov. To jasno izpostavlja tudi Bela knjiga EK o UI,[19] ki je EK predstavljala podlago za pripravo omenjenega predloga Uredbe o UI. Z vidika varstva pred diskriminacijo se tveganja za kršitev prepovedi diskriminacije pojavljajo na več ravneh. Delovanje sistemov UI temelji na obdelavi velikih količin (osebnih in neosebnih) podatkov, ki z uporabo algoritemskih modelov ustvarja določene rezultate, ki lahko predstavljajo odločitev o posameznikovih pravicah ali pa priporočilo odločevalcu za odločitev o teh pravicah. **Diskriminacija se v teh postopkih lahko pojavi iz različnih razlogov**: nepopolnih, nereprezentativnih in/ali netočnih učnih podatkih, na katerih temelji strojno učenje sistema UI; objektivno neutemeljeni uporabi algoritmov in modelov, ki temeljijo na obdelavi podatkov o osebnih okoliščinah posameznika kot relevantnih za ustvarjanje rezultatov in sprejemanje odločitev; uporabe približnih (*proxy*) podatkov za osebne okoliščine, ki vplivajo na avtomatizirano obdelavo; uporabe podatkov, ki temeljijo na pretekli diskriminaciji, ki se z avtomatizirano obdelavo zgolj reproducirajo (t.i. *feedback loop*) itd.[20] Strokovna skupina EU na visoki ravni za UI (HLEG AI) je v pripravljenih *Etičnih smernicah za zaupanja vredno umetno inteligenco* kot temeljno etično načelo v UI izpostavila **načelo pravičnosti**: »Vsebinska razsežnost pomeni zavezanost zagotavljanju enake in pravične porazdelitve koristi in stroškov ter preprečevanju nepoštene pristranskosti do posameznikov in skupin, njihove diskriminacije in stigmatizacije. Če je mogoče preprečiti nepošteno pristranskost, bi lahko sistemi umetne inteligence celo povečali družbeno pravičnost. Spodbujati bi bilo treba tudi enake možnosti v smislu dostopa do izobraževanja, blaga, storitev in tehnologije.«.[21]

[18] https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=COM:2021:206:FIN
[19] https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf
[20] Za podrobnejšo predstavitev tveganj za diskriminacijo v kontekstu UI glej FRA (2020) *Getting the Future Right – Artificial Intelligence and Human Rights*, str. 68-74.
[21] HLEG AI (2019) *Etične smernice za zaupanja vredno umetno inteligenco*, str. 15, dostopno na: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60438

Medtem, ko se protidiskriminacijsko pravo lahko nanaša tudi na delovanje sistemov UI, pa se dodatne težave med drugim pojavijo tudi pri **možnostih posameznika za uresničevanje njegove pravice do enakega obravnavanja** (t.i. *ex post* dimenzija regulacije UI, ki je predlog Uredbe o UI izrecno ne naslavlja). Pri tem sta pomembna zlasti dva vidika. Prvič, posamezniki velikokrat ne vedo, da se o njih sprejemajo odločitve, ki bodisi delno bodisi v celoti temeljijo na avtomatiziranem odločanju. To predstavlja **problem opazljivosti** (*observability*) **in transparentnosti** avtomatiziranega odločanja. V teh situacijah posamezniki torej niti ne vedo, da je njihov dostop do različnih pravic in ugodnosti podvržen avtomatiziranemu odločanju. Strokovnjaki opozarjajo, da pristop pridobitve izrecne privolitve posameznika k avtomatiziranemu odločanju v praksi (npr. preko sprejemanja »Pogojev o uporabi«) ne deluje in da takšen pristop predstavlja tveganje za izvotlitev varstva, ki ga sicer nudi koncept izrecne privolitve v GDPR.[22]

Drugič, problem transparentnosti se kaže tudi s **postopkovnega vidika**. Za ugotovitev obstoja zgoraj omenjenih razlogov, zaradi katerih lahko avtomatizirano odločanje v kontekstu umetne inteligence vodi v kršitev prepovedi diskriminacije, morajo biti prizadetemu posamezniku (in pristojnim organom, ki obravnavajo njegovo pritožbo) na voljo informacije, na kakšen način in na podlagi katerih podatkov je bila odločitev sprejeta. To torej pomeni, da bi morala ta odločitev v največji možni meri jasno razložljiva. HLEG AI je v omenjenih etičnih smernicah zato izpostavila, da »/p/ostopkovna razsežnost /načela/ pravičnosti vključuje zmožnost izpodbijanja odločitev, ki jih sprejmejo sistemi umetne inteligence in ljudje, ki jih upravljajo, ter zmožnost uveljavljanja učinkovitega pravnega sredstva proti njim. V ta namen mora biti mogoče identificirati subjekt, ki je odgovoren za odločitev, postopki odločanja pa bi morali biti razložljivi.«.[23] V zvezi s slednjim HLEG AI izrecno izpostavlja tudi potrebo po spoštovanju **načela razložljivosti**, ki pomeni, »da morajo biti postopki pregledni, da je treba odkrito sporočati zmogljivosti in namen sistemov umetne inteligence ter da mora biti mogoče odločitve – kolikor je mogoče – razložiti tistim, na katere neposredno in posredno vplivajo. Brez takšnih informacij odločitev ni mogoče ustrezno izpodbijati. /…/ Potrebna stopnja razložljivosti je zelo odvisna od okoliščin in resnosti posledic, če je navedeni rezultat napačen ali drugače netočen.«.[24] To načelo izpostavlja pomen odpiranja t.i. »črne škatle«, na kateri temelji delovanje UI.

*

Čeprav so tveganja za diskriminacijo pri avtomatiziranem odločanju relativno dobro poznana, pa je učinkovito uresničevanje varstva pred diskriminacijo pri avtomatiziranem odločanju v odsotnosti učinkovite in celovite regulacije UI postavljeno pod vprašaj. Časovnica sprejema navedenega predloga EK za Uredbo o UI je glede na obsežnost in kompleksnost predloga akta nepredvidljiva. To pomeni, da bi celovito regulacijo tega področja lahko stopila v veljavo šele po več letih, medtem ko je razvoj UI vse hitrejši, njena uporaba pa vse bolj razširjena. Strokovnjaki in mednarodne organizacije zato izpostavljajo in pozivajo, da je za regulacijo in nadzor nad avtomatiziranim odločanjem v kontekstu UI treba uporabiti pravna orodja in pristope, ki so že na voljo, ali pa jih ustrezno nadgraditi; **kot pomembno orodje se pri tem izpostavlja tudi pravo varstva osebnih podatkov**.[25] Iz člena 1(2) GDPR izhaja, da je namen uredbe varstvo osebnih podatkov posameznikov, a hkrati tudi drugih njihovih temeljnih pravic in svoboščin. Iz prakse Sodišča EU izhaja, da mora varstvo osebnih podatkov igrati instrumentalno vlogo zlasti pri varstvu pravice do nediskriminacije oziroma pravice enakega obravnavanja.[26]

Kot že omenjeno, GDPR že vključuje nekatere določbe, ki se nanašajo neposredno na vprašanje avtomatiziranega odločanja (in s tem neposredno tudi uporabo tehnologij, ki temeljijo na UI). Členi 13(2)(f), 14(2)(g) in 15(1)(h) tako med drugim določajo obveznost upravljavca in pravico posameznika, na katerega se obdelovani osebni podatki nanašajo, do **»smiselnih informacij«** o razlogih za avtomatizirano odločanje, vključno z oblikovanjem profilov, kot tudi pomen in predvidene posledice

[22] Fabienne Ufert (2020) AI Regulation Through the Lens of Fundamental Rights: How Well Does the GDPR Address the Challenges Posed by AI?. *European Papers* 5(2), str. 1092-1093.
[23] HLEG AI (2019), opomba 21 zgoraj, str. 15.
[24] *Ibid.*
[25] Glej npr. F. Zuiderveen Borgesius / Svet Evrope (2019) *Discrimination, artificial intelligence, and algorithmic decision-making*, dostopno na: https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73; Equinet (2020) *Regulating for an Equal AI: A New Role for Equality Bodies*, dostopno na: https://equineteurope.org/wpcontent/uploads/2020/06/ai_report_digital.pdf; F. Zuiderveen Borgesius (2020) *Strengthening legal protection against discrimination by algorithms and artificial intelligence*, The International Journal of Human Rights, 24:10, 1572-1593; Fabienne Ufert (2020) AI Regulation Through the Lens of Fundamental Rights: How Well Does the GDPR Address the Challenges Posed by AI?. *European Papers* 5(2), str. 1092-1093; Yordanka Ivanova (2020) *The Data Protection Impact Assessment as a Tool to Enforce Non-discriminatory AI*, SSNR Papers, dostopno na: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3584219.
[26] Glej npr. primer Sodišča EU C-524/06 Heinz Huber proti Zvezni republiki Nemčiji.

take obdelave za posameznika. Gre torej za določbe, ki načeloma naslavljajo poprej izpostavljeni **vidik transparentnosti in razložljivosti** delovanja sistemov UI.
Vendar pa strokovnjaki opozarjajo, da v praksi prihaja do restriktivnih interpretacij teh določb in da zaradi tega ni jasno, v kolikšni meri navedene določbe zagotavljajo, da bi se na podlagi »smiselnih informacij« lahko zagotovile dejanske informacije o načinu delovanja in podatki, na katerih temelji tehnologija za avtomatizirano odločanje.[27]

Avtomatizirano odločanje prav tako naslavlja **22. člen GDPR**, ki (upoštevajoč izjeme drugega odstavka tega člena) določa pravico posameznika, »da zanj ne velja **odločitev, ki temelji zgolj na avtomatizirani obdelavi, vključno z oblikovanjem profilov**, ki ima pravne učinke v zvezi z njim ali na podoben način nanj znatno vpliva«. Vendar v odsotnosti sodne prakse glede tega člena ni jasno, kaj pomenijo odločitve, ki temeljijo »zgolj« na avtomatizirani obdelavi. Strokovnjaki opozarjajo, da bi zaradi uporabe tehnologij UI v praksi **termin morali interpretirati tako, da zaobjame tudi odločitve, ki so sprejete z minimalno človeško intervencijo na podlagi sicer avtomatizirane obdelave**.[28] V praksi fizični odločevalci večinoma sledijo predlogom, ki izhajajo iz avtomatizirane obdelave, iz različnih razlogov, npr., ker te predloge dojemajo kot razumne ali nezmotljive ali ker želijo minimizirati lastno odgovornost (npr. kadar bančni uslužbenec stranki zavrne dostop do posojila, pri čemer odločitev temelji na rezultatu avtomatizirane obdelave z uporabo UI).[29] Prav tako izpostavljajo, da v praksi odločitve, ki imajo »pravne učinke« v zvezi s posameznikom ali nanj »na podoben način znatno vplivajo«, vključujejo tudi primere diskriminacije in izkoriščanja ranljivosti na različnih področjih (npr. pri trženju).[30]

V kontekstu varstva temeljnih pravic (zlasti varstva pred diskriminacijo) je posebej pomembna tudi določba 35. člena GDPR. Ta upravljavcem nalaga obveznost, da izvedejo **oceno učinka na varstvo osebnih podatkov**, zlasti, kadar bi obdelava podatkov z **uporabo novih tehnologij** lahko povzročila **veliko tveganje za pravice in svoboščine** posameznikov. Ta ocena mora minimalno obsegati tudi oceno tveganj za temeljne pravice posameznikov, na katere se podatki nanašajo, ter ukrepe za obvladovanje teh tveganj (člen 35(7)(c) in (d) GDPR. Dejstvo je, da sistemi UI sodijo med »nove tehnologije«, ki jih navaja predmetna določba GDPR. Hkrati je potrebno izpostaviti, da sledeč predlogu Uredbe o UI večina primerov, v katerih se sistemi UI uporabljajo za odločanje ali pomoč pri odločanju o pravicah, ugodnostih in interesih posameznikov, sodi v skupino t.i. visoko-tveganih AI sistemov. Poleg UI sistemov za biometrično identifikacijo in kategorizacijo oseb (naslovljena tudi v 78.-81. členu predloga ZVOP-2), v to skupino sodijo tudi sistemi na domala slehernem področju družbenega oziroma vsakdanjega življenja.[31] Velika večina držav članic EU sicer ne vodi javnega registra uporabljenih sistemov UI (bodisi v javnem bodisi zasebnem sektorju)- Vendar pa posebno poročilo Evropske mreže organov za enakost Equinet kaže, da je njihova uporaba že močno razširjena in se še povečuje.[32] Čeprav je sodna praksa in praksa organov za enakost v EU na tem področju še skopa, pa vseeno obstajajo pomembni primeri z različnih področij družbenega življenja, v katerih je že bila ugotovljena diskriminacija v kontekstu uporabe sistemov UI.[33]

Zaradi dokazanih visokih tveganj za diskriminacijo pri uporabi sistemov UI za namene avtomatizirane obdelave in avtomatiziranega odločanja, lahko ocena učinka na varstvo osebnih podatkov predstavlja pomemben instrument varstva pred diskriminacijo. Na to je Zagovornik opozoril tudi v svojem priporočilu k predlogu **Zakona o varstvu osebnih podatkov na področju obravnavanja kaznivih dejanj (ZVOPOKD)**.[34] V priporočilu je Zagovornik predlagal, da naj se iz že navedenih razlogov v okviru ocene učinka na varstvo osebnih podatkov ocena tveganj za človekove pravice izvaja **zlasti z vidika prepovedi diskriminacije**, kar je sicer določala že prva različica ZVOP-2 iz marca 2019. Zagovornikovo priporočilo k predlogu ZVOPOKD je bilo takrat sprejeto in je vključeno v veljavni zakon (49.(4)(2) člen).

[27] Glej npr. Zuiderveen Borgesius (2020), opomba 25 zgoraj, str. 1580.
[28] G. Malgieri and G. Comandé (2017), '*Why a Right to Legibility of Automated Decision-making Exists in the General Data Protection Regulation*', International Data Privacy Law 7(4), str. 243.
[29] Zuiderveen Borgesius (2020), opomba 25 zgoraj, str. 1573
[30] G. Malgieri and G. Comandé, opomba 28 zgoraj, *ibid*.
[31] V skladu s Prilogo 4 predloga Uredbe o UI so **kategorije visoko tveganih sistemov UI naslednje**: biometrična identifikacija in kategorizacija oseb; upravljanje kritične infrastrukture; izobraževanje in usposabljanje; zaposlovanje, upravljanje delavcev, samozaposlovanje; dostop do bistvenih zasebnih storitev in javnih storitev in ugodnosti, policijski nameni; migracije, azil in nadzor meja; pravosodni postopki, demokratični postopki.
[32] Equinet (2020), opomba 25 zgoraj, str. 81-96.
[33] *Prav tam*, str. 40-53, 106-110.
[34] http://www.zagovornik.si/wp-content/uploads/2020/06/Priporocila_Zagovornika_ZVOPPOKD_P.pdf

Potrebo po reguliranju ocene učinka sistemov UI na temeljne pravice – tudi s pomočjo uporabe GDPR – izpostavljajo tudi mednarodne organizacije in njihove agencije,[35] strokovnjaki pa so razvili tudi metodologije, po katerih bi se ocena učinka po 35. členu GDPR lahko uporabila za *ex ante* preprečevanje diskriminacije v kontekstu UI.[36]

*

Upoštevajoč navedeno pri Zagovorniku ocenjujemo, da predstavlja predlog novega ZVOP-2 priložnost, da se navedena tveganja za človekove pravice, zlasti glede prepovedi diskriminacije, naslovijo z zakonodajnimi ukrepi, ki bi tako z *ex ante* kot *ex post* vidika lahko izboljšali varstvo pred diskriminacijo v kontekstu avtomatizirane obdelave in avtomatiziranega odločanja v kontekstu uporabe sistemov UI. Zato predlagamo, da se za 81. členom (torej za členi, ki urejajo uporabo biometričnih ukrepov) predloga ZVOP-2 ali na drugo, po pripravljavčevem mnenju bolj ustreznem mestu, doda člen ki bi izrecno določil oziroma naslovil naslednje:

- obvezno oceno učinka na varstvo osebnih podatkov za vse avtomatizirane obdelave osebnih podatkov, ki temeljijo na uporabi UI (vidik »novih tehnologij«), pri čemer mora upravljalec oceno tveganja na temeljne pravice in svoboščine ter ukrepe za obvladovanje teh tveganj izvesti **zlasti z vidika prepovedi diskriminacije iz 3. člena predloga ZVOP-2**;
- pravico posameznika, da zanj ne veljajo odločitve, ki temeljijo **bodisi zgolj bodisi delno na avtomatizirani obdelavi**, vključno z oblikovanjem profilov, ki ima pravne učinke v zvezi z njim ali na podoben način nanj znatno vpliva (*v smislu razširjene interpretacije člena 22(1) GDPR, ki je skladna z uporabo sistemov UI za avtomatizirano odločanje*);
- pravico posameznika do **pritožbe zoper katerokoli odločitev**, ki temelji bodisi zgolj bodisi delno na avtomatizirani obdelavi, vključno z oblikovanjem profilov, ki ima pravne učinke v zvezi z njim ali na podoben način nanj znatno vpliva;
- interpretacijo pojma **»smiselne informacije«** iz členov 13(2)(f), 14(2)(g) in 15(1)(h) GDPR na način, ki bo upravljalcem določil zahtevo zagotoviti, posameznikom, na katere se osebni podatki nanašajo pa pravico dostopati do informacij o razlogih, načinu obdelave in podatkih, na podlagi katerih je bila odločitev sprejeta (*vidik zagotavljanja transparentnosti, razložljivosti in učinkovitega pravnega sredstva*).

[35] Glej npr. FRA (2020), opomba 25 zgoraj, str. 89 ter *Annex II: Examples of theoretical assessment of harm and significant impact of AI or automated decisions*.
[36] Glej npr. Yordanka Ivanova (2020) *The Data Protection Impact Assessment as a Tool to Enforce Non-discriminatory AI*, SSNR Papers, dostopno na: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3584219