

Ивана СТЕПАНОВИЋ
Институт за криминолошка
и социолошка истраживања
Београд, Србија

Прегледан рад
Примљено: 13.11.2020.
Прихваћено: 01.02.2021.

ОД ТРАДИЦИОНАЛНЕ БИРОКРАТИЈЕ ДО АЛГОРИТАМСКЕ ОБРАДЕ ПОДАТАКА: КАКО ИНФОРМАЦИОНЕ ТЕХНОЛОГИЈЕ ТРАНСФОРМИШУ КОНЦЕПТ НАДЗОРА?

Назор као производ модерног друштва радикално се трансформише путем савремених информационих технологија које у себи имају интегрисане алгоритме. Алгоритам је можда најзначајнији концепт савременог света јер мења начине рада, учествује у производним процесима, креира културне садржаје и доноси одлуке. Традиционална администрација током двадесет првог века постаје алгоритамска, што значи да сам медиј који се користи за складиштење података постаје жив, активан и контролишући јер он као вештачка интелигенција тумачи те податке и даље оперише са њима. Приватност и друга људска права и слободe не зависе више само од људског фактора и људских одлука, већ и од алгоритама, односно вештачких интелигенција. На алгоритме се све више ослањају не само интернет медији, друштвене мреже и различите платформе већ све чешће и све интензивније државне институције и приватне компаније. Ово је проблематично пре свега због тога што саме алгоритме карактерише нетранспарентност у погледу начина функционисања и сакупљања, па затим и обраде података. Недостатак транспарентности у погледу рада алгоритама, сама њихова дигитална природа, као и осамостаљеност од људске радне снаге доводе до етичких недоумица везано за коришћење алгоритамских програма који увек оперишу и као системи надзора, па самим тим угрожавају право на приватност. Циљ овог рада је да постави теоријско питање разлике између традиционалних и савремених система надзора, затим да укаже на потребу преиспитивања етичких принципа коришћења вештачких интелигенција с обзиром на заштиту људских права и слобода, као и да подигне свест о проблематич-

ности употребе дигиталних система надзора који уместо људске радне снаге користе вештачке интелигенције у државним органима и другим институцијама.

Кључне речи: алгоритми, надзор, људска права, приватност, технологија

Увод

Кључне промене које су утицале на трансформацију концепта надзора у двадесет првом веку везују се за интернет и то нарочито за интернет Веб 2.0 (Caviglione, Coccoli, 2011). Ове технологије омогућавају сакупљање, обраду и дељење великог броја информација, брзу комуникацију и такозвани *user generated content* (садржај који креирају корисници) на различитим интернет платформама. Подаци о личности, у које спадају не само бројеви личних карата, адресе становања и други подаци из званичних докумената већ и све оно што генеришу информационе технологије укључујући информације о кретању, историја претраживања на интернету, базе дигиталних фотографија, профили на друштвеним мрежама и подаци о оствареним куповинама путем кредитне или дебитне картице, стварају неку врсту виртуелних „двојника“ (Haggerty, Eriscon, 2000: 605) који су под константним надзором за који није задужена људска радна снага већ алгоритми (вештачке интелигенције) које на нетранспарентан начин прикупљају, похрањују и обрађују приватне податке, али и све интензивније доносе одлуке, регулишу понашање и пружају услуге, појављујући се на тај начин као нови субјекти друштва и нови субјекти моћи.

Алгоритми као нови механизми за надзор и контролу присутни су не само на друштвеним мрежама и онлајн платформама већ и у системима здравства или школства, а користе се и у раду полиције и других органа власти. Харари сматра да је алгоритам најважнији концепт савременог света јер у потпуности трансформише стварност друштва, те да га треба дефинисати као методички сет корака који служе томе да се направе прорачуни, реше проблеми и донесу одлуке (Harari, 2017: 97).

Алгоритамски надзор много је тешње повезан са контролом јер вештачке интелигенције саме могу да тумаче податке и доносе одлуке или предузимају одређене мере као што је, на пример, блокирање рачуна у банци, поништавање неког онлајн формулара или онемогућавање одређених радњи корисницима интернет платформи. Алгоритамски надзор, чини се, постаје нови вид класичног бирократског

надзора и све више улази у свакодневну употребу у свим сферама живота. Да би се боље разумела природа и сврха овог комплексног система надзора који почива на прикупљању али и интерпретацији, па чак и неком виду преобликовања приватних података у неке нове информације, важно је разумети шта му историјски претходи.

Концепт надзора се, као и концепт приватности, рађа у модерности, јер, као што показују Фукоове историјске анализе, управо тада тортура и сурово кажњавање бивају замењени једном другом технологијом управљања а то је стављање под надзор како би се појединци дисциплиновали уместо да се кажњавају (Foucault, 1995: 173). Мада надзор (*surveillance*) дословно значи бити под присмотром или бити (над)гледан, не ради се само о нечем строго визуелном, већ о систематском сакупљању података о појединцима, о њиховом идентитету, понашању, па чак и о наизглед неважним гестовима (Foucault, 1995: 77). И мада на први поглед може да изгледа као да је надзор проблем двадесет првог века и да је незамислив ван контекста савремених информационалних технологија, треба имати у виду да су праксе надзора кроз историју постојале много раније, те да су ове нове технологије омогућиле да се технике надзора које су већ раније осмишљене додатно усаврше.

Алгоритми су производ експанзије дигиталног надзора и њихова улога је да стотине хиљада типова приватних података рашчлањују, анализирају, сортирају и обликују у нове податке, али такође и да уместо људске радне снаге извршавају различите задатке (који су везани за обраду података) попут цензурисања говора мржње, пружања подршке корисницима разних платформи на интернету или излистивање персонализованих садржаја који се препоручују на основу личних података који откривају преференце и потребе појединаца. Алгоритми, односно вештачке интелигенције, дакле, врше надзор и све своје функције обављају захваљујући надзору. Они такође и спроводе контролу, учествују у креирању културних садржаја и обављају различите послове уместо људске радне снаге. Упркос покушајима да се поље приватности на интернету законски уреди регулативама попут Опште уредбе Европске уније о заштити приватних података (GDPR), све интрузивније технологије које се базирају на раду алгоритама и које су све присутније у физичким просторима прете да суштински угрозе људска права и слободе. Парадигматичан пример су апликације за праћење контаката направљене у циљу спречавања ширења вируса

KOVID-19 за које се сматра да могу да доведу до недемократских и дискриминаторских пракси (Sweeney, 2020: 303).

За разлику од традиционалних бирократија које су се фокусирале на сакупљање много базичнијих података о личности, као што су адресе становања, датуми рођења, пописи имовине и слично, савремени надзор има могућност прикупљања веома суптилних информација које задиру у срж приватности бића као што су, рецимо, подаци о покретима мишића на лицу који потенцијално могу открити мисли и осећања. Истовремено долази до минијатуризације надзора и његове експанзије, чиме се омогућава приступ много интимнијим подацима и далеко интензивнија контрола становништва. Управо због тога што алгоритамски надзор задира дубље у приватност и потискује људски фактор изван унутрашњости бирократских система, чинећи их све мање докучивим, теоријска истраживања о овом савременом концепту надзора неопходна су и требало би да претходе истраживањима која би служила као смернице за креирање јавних политика. Користећи методе анализе садржаја и критичке анализе дискурса, овај рад разматра концепте бирократије, надзора и алгоритама анализирајући како су они међусобно повезани и како управо разумевање ових појмова даје путоказ за критичко промишљање употребе вештачке интелигенције у различитим сегментима јавног и приватног живота.

1. Модерно друштво и настанак бирократског надзора

Развијена бирократија је свакако једна од најважнијих одлика модерне државе, а она повлачи значајне последице по концепт приватности. Као што кажу многи аутори (Dandeker, 1990; Giddens, 1985; Jacoby, 1984; Foucault, 1995; Herzfeld, 1992), бирократија се концептуализује као систем надзора који служи управљању великих група људи. А како је модерна држава велика, многољудна заједница са централизованом влашћу, управљање таквом државом захтева пописивање становништва, прављење статистика, стварање датотека и, уопште, надзирање становништва.

Међутим, да ли је бирократија као таква уопште изум који настаје у Европи у седамнаестом веку? Јакоби у својој књизи „Бирократизација свијета” даје кратак историјски приказ у коме показује како је бирократија постојала много пре постанка модерне државе, било да говоримо о седамнаестом или деветнаестом веку као историјском

периоду у коме се она инаугурише. Он каже: „бирократије је било свуда гдје су велике групе људи на великом простору стајале пред задацима које је требало централно рјешавати” (Jacoby, 1984: 15) и додаје да је „најтоталитарнија бирократија” у историји човечанства било писарство Египта и Вавилонa (Jacoby, 1984: 15).

Вебер такође наводи да велике бирократије постоје много пре стварања модерне државе, и то у Египту, у доба Новог Краљевства, у Риму у време Принципата и то у доба владавине Диоклецијана, у Кини од доба Ши Квангија, а велика бирократија је и сама римска католичка црква од тринаестог века наовамо (Weber, 1978: 964). Том списку треба додати и такозвану *Doomsday Book*, односно Књигу страшног суда, која је настала 1068. године у време Виљема Освајача у Енглеској и представља попис земље и становништва. Како Јакоби пише, „није било ниједне свиње, краве ни вола што нису били пописани”, а такође „није било ни комада обрађене земље” који нису били уписани у ову књигу (Jacoby, 1984: 89). То је био један од првих пописа ове врсте у историји и због тога је значајан када се говори о бирократији и уопште историји система надзора.

Ипак, бирократија модерне државе има своје специфичности. Она је посебна по томе што захвата „целокупну друштвену организацију” и постаје свеприсутна јер се шири и на сферу приватног (Jacoby, 1984: 79). Према његовој анализи, модерна држава без дилеме настаје непосредно после средњег века, то јест у седамнаестом веку. Тада се распадају „политичке творевине средњег века” и долази до централизације власти ка државном врху, а државни апарат затим „шири подручје своје моћи” (Jacoby, 1984: 28). Јакоби такође истиче да, иако је у седамнаестом веку модерна држава била обликована као апсолутна монархија, већ тада она бива „по први пут до краја домишљена”, а саму концепцију осмислио је Томас Хобс (Jacoby, 1984: 53). Већ он говори о томе како је монархија само један од могућих облика државе и сматра да је сваком друштву потребна централизована власт (Jacoby, 1984: 54).

Макс Вебер такође каже да, иако је бирократија постојала у различитим друштвима кроз историју, она добија свој прави облик тек у модерној држави (Weber, 1978: 956). Он такође сматра да нека одређења суштински одређују модерну бирократију или „бирократску агенцију” спрам свих њених претходних инкарнација, а то су редовне активности бирократски управљане структуре које се извршавају као званичне дужности, затим овлашћења за издавање наредби да се ове

дужности извршавају, која су регулисана правилима, и методичност која омогућава континуирано испуњавање ових дужности (Weber, 1978: 956). Вебер такође каже да модерне бирократске системе одликује хијерархија и да су за њено функционисање кључни „писани документи”, те да су они најпре осмишљени да одвајају приватно од јавног, а да се тек касније бирократија проширила тако да обухвата чак и сферу приватног живота (Weber, 1978: 957). За Вебера је новчана економија један од предуслова за модерну бирократију и један од њених кључних спецификаума. Заправо, он тврди да је „стабилни систем опорезивања” предуслов за перманентно постојање бирократске администрације и да само потпуно развијена новчана економија даје сигуран основ за такав систем опорезивања (Weber, 1978: 969).

Још једна врло важна особина модерне бирократије је да се она стално шири и усавршава у зависности од развоја технологије и продукције. Вебер каже да је разлог њеног напретка њена „техничка супериорност над свим осталим формама организације”, те да су кључни фактори „прецизност, брзина, недвосмисленост и знање о документима” (Weber, 1978: 976). Када се то има у виду, онда је лако објаснити како то да је бирократија напредовала од записа на папирусу у старом Египту до огромних дигиталних датотека које постоје данас. Као што каже Дандекер, ради се о томе да се капацитет надзора повећао, а не и његов основни принцип (Dandeker, 1990: 194).

Надзор није ништа друго него сакупљање информација у административне сврхе, као што каже Гиденс (Giddens, 1985: 46). Он такође каже да је надзор као политичка моћ феномен који је везан за модерну државу и није постојао раније (Giddens, 1985: 49). Савремена бирократија која се ослања на рачунаре и дигиталне датотеке само је развијенији облик администрације која је осмишљена још на самом почетку модерног доба. Према томе, када се говори о високоразвијеним бирократским системима двадесет првог века, треба имати у виду то да су основни принципи њиховог функционисања настали много пре него што су развијене технологије које су омогућиле велике датотеке (*big data*).

2. Дигитални надзор и делимична приватност

Надзор за који се чак може рећи да представља „централну димензију модерности” у двадесет првом веку постаје „флексибилан и мобилан”, па захвата и оне сфере приватног живота које раније није

додиривао (Bayman, Lyon, 2013: 3). Тај савремени дигитални надзор, како је већ указано, подразумева више метода прикупљања података помоћу различитих уређаја, од телефона и камера до сензора, скенера тела и биометрије, а типови података варирају од личних идентификационих бројева, банковних рачуна, приватне преписке, фотографија и аудио или видео снимака, отисака прстију и ДНК. Другим речима, свака информација и свака комуникација која је у дигиталном облику представља податак који може да се архивира, а такви подаци се данас сматрају „новом нафтом“ (Hirsch, 2014: 2).

Преломни догађај који је поставио изазов за право на приватност на глобалном нивоу био је велики терористички напад на САД септембра 2001. године, који је праћен низом мањих терористичких напада у другим земљама запада. Фокус се нагло помера са приватности као једне од кључних вредности класичног либерализма на безбедност и тај радикални обрт мења јавне политике, законске оквире и јавни дискурс. Доминантни дискурс о приватности и безбедности намеће идеју о томе да се мора направити компромис и жртвовати приватност зарад безбедности, као и идеју да појачан надзор треба да се нормализује. У то време долази до формирања једне потпуно „нове политике надзора“ која резултира читавим низом нових правних мера и технолошких изума намењених праћењу и надзору грађана као што су биометријски пасоши и личне карте (Levi, Wall, 2004: 203). Паралелно са тим, политика размене података о личности ради превенције тероризма заменила је политику приватности, односно дошла у колизију са њом, па тако аутори, попут Грегорија Волтерса, указују на проблем антагонизма приватност/безбедност који је садржан у самом тексту Конвенције 108. Наиме, он тврди да ова конвенција покушава да балансира између слободе да се процесуирају информације о појединцима и права на приватност, са друге стране (Walters, 2001: 119).

Проблем „великих података“ који „представљају нову парадигму у начину прикупљања, комбиновања и анализирања података“ али се „велики број односи на податке о личности и интеракцију међу људима“, па он поставља нове изазове пред заштиту приватности. Преломни тренутак у историји који ће одредити начин на који се данас промишља концепт приватности јесте откриће узбуњивача америчке Националне службе за безбедност Едварда Сноудена који је 2013. године медијима дао на увид тајна документа која доказују постојање пројеката масовног надзора различитих тајних служби о којима се до тада само спекулисало и који су нелегални и нелегитимни (Сноуден,

2020: 236). Тајна документа обелоданила су пројекат PRISM који је омогућио америчкој Националној служби за безбедност да добије било какве податке са интернета које прикупљају компаније са стотинама милиона корисника широм света који њихове производе (попут друштвене мреже *Facebook*, имејл сервиса *Gmail* или апликације за комуницирање *Skype*) користе као главна средства за комуникацију (Сноуден, 2020: 236). Овакви пројекти масовног надзора настају након терористичких напада у САД 2001. године када се доносе закони који дају више моћи америчкој Националној служби за безбедност, међутим, Сноуден је указао на то да је проблем у томе што су сами закони тајни баш као и пројекти надзора, а надзирани грађани уопште не морају да буду осумњичени (Сноуден, 2020: 243). Фајлови које је Сноуден предао редакцији листа *Гуардиан* пружају доказе о томе да је НСА „прикупљала, анализирала и чувала“ билионе телефонских позива и имејлова у САД, али такође дају доказе да исте такве праксе постоје и у Великој Британији и другим државама. С обзиром на то да је доказано да су мета надзора не само појединци осумњичени за тероризам, већ и обични грађани, подаци које објављује Сноуден илуструју како је сам интернет кроз све његове мејнстрим медије, од *Facebook*-а до *Google*-а и *Microsoft*-а, уређен тако да не омогућава приватност кореспонденције, те личну комуникацију чини потпуно транспарентном.

Сноуденови тајни фајлови показали су како се у САД, па и у остатку западног света не поштује право на приватност загарантовано пре свега међународним правом, то јест Општом декларацијом о људским правима, Међународним пактом о грађанским и политичким правима и Европском конвенцијом о људским правима јер државе преко тајних служби имају приступ тим подацима. Међутим, осим државних органа, приватне податке користе и други економски и привредни субјекти. Наиме, данас се велики подаци користе као „сирови материјал производње“ и „нови извор друштвених и економских вредности“ (Tene, Polonetsky, 2012). Они воде креирању „детаљних индивидуалних профила“ (Crawford, Schultz, 2014) и у другој деценији двадесет првог века експанзија интернета Веб 2.0, који се базира на садржајима које креирају сами корисници, доводи до кризе приватности због тога што подручје интернета остаје законски недовољно регулисано.

Општа уредба Европске уније о заштити података о личности представља први озбиљан покушај да се право на приватност података регулише на глобалном нивоу, или бар да се поставе некакви глобални стандарди заштите приватности (Safari, 2017). Паралелно са овим променама на нивоу закона, дешавају се и велике промене у пракси коришћења услуга на интернету. Многи сервиси, попут *WhatsApp*, уводе енкрипцију како би се сачувала тајност комуникације, а настају и потпуно нови сервиси, попут апликације *Signal*, који су креирани управо са идејом да обезбеде првенствено приватност комуникације (MacAskill, Hern, 2018).

Међутим, овакве регулативе могу да обезбеде једино делимичну заштиту података и ограничену, парцијалну приватност. Наиме, Општа уредба, па и сва друга законска решења заштите приватности на интернету полазе од претпоставке да подаци о личности нису и не могу бити апсолутно приватни јер су јавни самим тим што се налазе у простору интернета, те је могуће обезбедити једино делимичну контролу над тиме шта се са тим подацима дешава, а не и потпуну тајност тих података. Другим речима, приватни подаци на интернету немају ону врсту заштите на коју се може рачунати када су у питању физички простори или предмети као што је, рецимо, неповредивост стана или тајне писма. Дигитални подаци се готово по аутоматизму прикупљају, складиште и чувају захваљујући савременим информационом технологијама које су заправо технологије надзора.

3. Ауторитет алгоритама

Иако евидентно постоје промене које реafirмишу концепт приватности дигиталној ери, питање безбедности на интернету постаје све сложеније и све неухватљивије захваљујући томе што се надзор минијатуризује до нивоа метаподатака и регулише путем вештачких интелигенција. Ови подаци о подацима се екстраполирају из комуникација и активности на интернету и често се категоришу као анонимни и несензитивни. Ти подаци могу да се користе у разне сврхе као што је, на пример, маркетинг јер пружају информације попут: који тип муштерија купује одређени производ, који узраст прати одређену серију или која паста за зубе неког брeнда је најпродаванија. Ови подаци служе томе да се донесу одређени закључци који би поспешили бизнис неке компаније и није потребно да ти подаци буду везани за

појединачну особу јер они служе за статистичке прорачуне. Тако окарактерисан, надзор се чини као безазлен јер су подаци у процесу анализе деперсонализовани. Па ипак, нека истраживања показују како се ти подаци накнадно могу повезати са идентитетом појединца, па самим тим угрожавају право на приватност (Perez et al. 2018), а друга говоре о томе да је етичност пракси таргетирања корисника путем интернет платформи и друштвених мрежа упитна (White, Boatwright, 2020).

Интернет у стварима (*the internet of things*) пружа одређени комфор, али такође доводи до тога да се нехотично и неконтролисано разоткривају информације о приватном животу које могу да доведу до разних облика дискриминације (Wachter, 2018). Сваки уређај повезан на интернет прикупља одређене податке о корисницима, а они се онда могу користити или у виду деперсонализованих мета података у сврхе побољшања бизниса или за неку врсту шпијунаже. У оба случаја приватност се жртвује зарад неке друге користи, а уређаји се често креирају тако да унапред онемогућавају приватност. Карактеристичан пример уређаја који је осмишљен тако да побољша квалитет живота али истовремено угрожава приватност је Амазонов „паметни звучник” Echo који се, осим као асистент или помоћ у домаћинству, може користити и као прислушни уређај (MacAskill, Hern, 2013). Обрада великих података зависи од алгоритама, односно софтвера или вештачких интелигенција које се напајају управо приватним подацима. Данас се кроз алгоритме који управљају претраживачима, друштвеним мрежама и другим платформама на интернету испољава ауторитет и људске одлуке које утичу на целокупно друштво замењују се аутоматским одлукама софтвера (Pasquale, 2015).

Неки аутори чак сугеришу да алгоритми данас регулишу аспекте свакодневног живота (Beer, 2009: 985), а кључне критике усмерене су на чињеницу да су ти алгоритми тајни, што покреће питања транспарентности и одговорности (Pasquale, 2015; Bucher, 2018), а то се пре свега тиче компанија које су данас највећи ауторитети у јавном простору интернета попут Google-а или Facebook-а. Штавише, данас се може говорити о друштвеним мрежама и другим платформама као о „алгоритамским медијима” (Bucher, 2018: 1) који нису само преплетени са животом, већ се управо кроз њих живи (Степановић, 2020: 31). У том смислу, алгоритми не само да уређују медије одређујући и персонализујући садржај или цензуришући говор мржње, већ уређују и сам живот и то путем надзора.

Ширење технологије и надзора на све аспекте приватног живота и тенденција да се све људске активности претворе у податке који се онда похрањују у датотеке, деле, анализирају и користе за *machine learning* (машинско учење), односно за едуковање софтвера и производњу вештачких интелигенција. С обзиром на то да су приватни подаци нови капитал, сваки облик активности на интернету, било да се ради о некој пословној активности, учењу, новчаној трансакцији, приватној конверзацији или забави, представља процес производње, па су потрошачи истовремено произвођачи или просумерс (Fuchs, 2014). На тај начин се дигитални надзор, који је заправо алгоритамски, уплиће у процесе производње и потрошње и постаје саставни део ових процеса.

Хранећи се приватним подацима, алгоритми се појављују као нови субјекти моћи којима недостаје транспарентност, а врло често и објективност. Њихов утицај је присутан у свим сферама друштва јер се користе не само за друштвене мреже друге платформе већ и у безбедносним, финансијским, здравственим и другим институцијама (Bucher, 2018: 41). Они су проблематични управо због тога што нису нити објективни нити неутрални, већ су врло често пристрасни и склони дискриминаторским праксама (Browning, Arrigo, 2020; Borgesius, 2020). Међутим, кључни аргумент који оспорава етичност алгоритамске културе је тај да су алгоритми „тајни” механизми који на нетранспарентан начин тумаче и обликују податке, а затим на основу тих тумачења доносе одређене одлуке (Bucher, 2018: 41). Тајност рада алгоритама објашњава се, са једне стране, техничким особинама алгоритама који су заправо веома комплексни системи, а, са друге, тиме што је дискреција наопходна како би се компанија која их користи заштитила; на пример, компанија Facebook штити тајну функционисања алгоритама зато што би у супротном могло доћи до злоупотреба (Bucher, 2018: 41). Критике на рачун рада алгоритама усмерене су, дакле, на то што су алгоритми по природи потпуно непрозирне „црне кутије”, па је самим тим њихова моћ да доносе одлуке проблематична (Pasquale, 2015).

Надзор, дакле, са појавом ових нових информационих технологија и интернет медија постаје алгоритамски, непрозиран и тајан. Он је повезан са једним потпуно новим обликом контроле која више није везана за људски фактор већ за вештачке интелигенције које на нетранспарентан начин користе приватне податке. Покушаји да се алгоритамска обрада података ограничи тако да се заштите људска права

и слободе остају недовршени. Један од механизма за заштиту права на приватност у погледу алгоритамске обраде података представља Општа уредба Европске уније о заштити података о личности, међутим, он је проблематичан управо због тога што алгоритми имају особине црне кутије, па је самим тим технички превише захтевно да се уопште омогући принцип транспарентности дефинисан у овом правном документу (Crockett et al, 2021).

Закључак

Концепт бирократског надзора почива на идеји контролисања великих популација и своди се на креирање датотека. Кроз историју, те датотеке су се састојале од, условно речено, крупнијих података о појединцима који чине те популације, а данас алгоритми прикупљају веома суптилне податке попут боје гласа, гримаса лица или свакодневних радњи које разоткривају најприватнију унутрашњост личности. С обзиром на то да се људски живот све интензивније одвија не са технологијом већ дословце кроз њу, појединци остављају све више својих дигиталних трагова који остају трајно забележени. Ови трагови су често веома приватне информације о појединцима које се уз помоћ савремених технологија архивирају као и сви други подаци, а с обзиром на то да је реч о великим количинама информација, њихово складиштење и обрада могућа је једино путем вештачких интелигенција.

Савремени алгоритамски надзор интрузивнији је од свих претходних система надзора који су се користили кроз историју, а специфичан је по томе што сам медиј који се користи за похрањивање података такође има способност да их обрађује и тумачи, а затим на основу тих тумачења самостално доноси одлуке и обавља различите делатности замењујући људску радну снагу. Савремене информационе технологије захваљујући алгоритмима не служе само за складиштење података, већ оне представљају активне и, на неки начин, живе датотеке које саме сакупљају информације, интерпретирају их и затим их даље користе у различите сврхе, за обављање различитих активности и то на такав начин да појединац не само да је подвргнут анализи вештачких интелигенција већ може сносити последице алгоритамског тумачења података о њему.

Због свега овога, алгоритамске датотеке не могу се окарактерисати као пасивни медији већ као активни, интелигентни медији који

учествују у контроли и организацији друштва, производним процесима и креирању културних садржаја (Bucher, 2018: 150). Развој алгоритама који остају нетранспарентни и недокучиви појединцима а могу их надмашити у интелигенцији и одменити у обављању великог броја послова може довести до несагледивих последица, па чак и до тога да људски ресурси постану потпуно непотребни (Harari, 2017: 363–379).

Захваљујући алгоритмима, дигитални надзор улази дубоко у човека и, захваљујући сопственој интелигенцији, почиње да њиме управља и контролише све оне аспекте живота које традиционални надзор није додиривао. Чињеница да се различите компаније и институције, па и органи власти све више ослањају на алгоритме уместо на људску радну снагу доводи до тога да алгоритми ограничавају људска права и слободе јер се базирају на надзору, а такође им се препушта и доношење одлука. Због тога је неопходно стално критичко преиспитивање етичности принципа на којима се заснива рад алгоритама како би се овај до сада правно нерегулисани феномен расветлио и како би се могле креирати јавне политике које би пружиле оквир за етички прихватљиво употребавање вештачких интелигенција.

Литература

- Bauman, Z., Lyon, D. (2013). *Liquid Surveillance*. Cambridge: Polity Press.
- Beer, D. (2009). Power through the algorithm? Participatory web cultures and the technological unconscious. *New Media & Society*, 11(6), 985–1002.
- Borgesius, F. J. Z. (2020). "Strengthening legal protection against discrimination by algorithms and artificial intelligence". *The International Journal of Human Rights*, 24(10), 1572–1593.
- Browning, M., Arrigo, B. (2020). "Stop and Risk: Policing, Data, and the Digital Age of Discrimination". *American Journal of Criminal Justice*. DOI: 10.1007/s12103-020-09557-x
- Bucher, T. (2018). *If... Then: Algorithmic Power and Politics*. Oxford: Oxford University Press.
- Caviglione, L, Coccoli, M. (2011). "Privacy Problems with Web 2.0". *Computer Fraud & Security* (10), 16–19.
- Council of Europe, Savetodavni komitet konvencije o zaštiti lica u odnosu na automatsku obradu podataka o ličnosti (T-PD), „Smernice za

- zaštitu lica u odnosu na obradu podataka o ličnosti u svetu velikih podataka”. www.poverenik.rs (pristupljeno 02.01.2021).
- Crawford, K., Schultz, J. (2014). “Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms”. *Boston College Law Review*, 55 (93).
- Crockett et al (2021). “Reconciling Adapted Psychological Profiling with the new European Data Protection Legislation”. In Kurse, R. et al. *Computational Intelligence: A Methodological Introduction*; <https://www.springer.com/gp/book/9783030422264> (accessed 02.01.2021).
- Dandeker, C. (1990). *Surveillance, Power & Modernity*. Cambridge: Polity Press.
- Evropska konvencija o ljudskim pravima, čl. 8, ECHR; https://www.echr.coe.int/Documents/Convention_BOS.pdf (pristupljeno 02.01.2021).
- Foucault, M. (1995). *Discipline and Punish; The Birth of Prison*. New York: Vintage Books.
- Fuchs, C. (2014). *Social Media: A Critical Introduction*. London: SAGE.
- GDPR <https://gdpr-info.eu/> (pristupljeno 02.01.2021).
- Giddens, A. (1985). *Nation State and Violence*. Cambridge: Polity Press.
- Guardian The NSA Files; <https://www.theguardian.com/us-news/the-nsa-files> (accessed 02.01.2021).
- Haggerty, K. D., Ericson, R. V. (2000). “The Surveillant Assemblage”. *British Journal of Sociology* 51(4), 605–622.
- Harari, Y. N. (2017). *Homo Deus*. London: Vintage.
- Herzfeld, M. (1992). *The social production of indifference: Exploring the symbolic roots of Western bureaucracy*. New York: Berg.
- Hirsch, D. (2014). “The Glass House Effect: Big Data, the New Oil, and the Power of Analogy”. *Maine Law Review*. Available from: SSRN: <https://ssrn.com/abstract=2393792> (accessed: 02.01.2021).
- Jacoby, H. (1984). *Birokratizacija svijeta*. Zagreb: Globus.
- Levi, M. and Wall, D. S. (2004). “Technologies, Security and Privacy in the post 9/11”. *Journal of Law and Society*, 31(2), 194–220.
- MacAskill, E., Hern, A. (2018). “Edward Snowden: The people are still poweless, but now they’re aware”; <https://www.theguardian.com/us-news/2018/jun/04/edward-snowden-people-still-powerless-but-aware> (accessed 02.01.2021).
- Međunarodni pakt o građanskim i političkim pravima, čl. 17, BG CEN-TAR <http://www.bgcentar.org.rs> (pristupljeno 02.01.2021).

- Opšta deklaracija o ljudskim pravima, čl. 12, UNCHR; <http://www.unhcr.rs> (pristupljeno 02.01.2021).
- Pasquale, F. (2015). *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge Massachusetts: Harvard University Press.
- Perez, B. Et al. (2018). *You Are Your Metadata: Identification and Obfuscation of Social Media Users using Metadata Information*. arXiv <https://arxiv.org/abs/1803.10133> (accessed: 02.01.2021).
- Safari, B. (2017). "Intangible Privacy Rights: How Europe's GDPR Will Set a New Global Standard for Personal Data Protection". *Seton Hall Law Review* 47(3), Article 6.
- Snouden, E. (2020). *Trajno zabeleženo*. Beograd: Vuklan.
- Stepanović, I. (2020). *Život na internetu: pravo na privatnost i online komunikacija*. Beograd: Institut za kriminološka i sociološka istraživanja.
- Sweeney, Y. (2020). "Tracking the debate on COVID-19 surveillance tools". *Nat Mach Intell* 2, 301–304; <https://doi.org/10.1038/s42256-020-0194-1>
- Tene, O., Polonetsky, J. (2013). "Privacy in the Age of Big Data: A Time for Big Decisions". *11 Northwestern Journal of Technology & Intellectual Property*.
- Wachter, S. (2018). "The GDPR and the Internet of Things: A Three-Step Transparency Model". *Law, Innovation and Technology*, SSRN: <https://ssrn.com/abstract=3130392> (accessed 02.01.2021).
- Walters, G. J. (2001). *Human rights in an information age: A philosophical analysis*. Toronto: University of Toronto Press.
- Weber, M. (1978). *Economy and Society*. Berkeley, Los Angeles, London: University of California Press.
- White, C. L., Boatwright, B. (2020). "Social media ethics in the data economy: Issues of social responsibility for using Facebook for public relations". *Public Relations Review* 56(5).

FROM TRADITIONAL BUREAUCRACY TO ALGORITHMIC DATA PROCESSING: HOW DIGITAL TECHNOLOGY TRANSFORMS THE CONCEPT OF SURVEILLANCE?

By Ivana STEPANOVIĆ

ABSTRACT

Surveillance as a product of modern society has been radically transformed through algorithmic digital technologies. The algorithm is the key concept that changes the nature of surveillance because it alters the production process while interfering with labour, creating the culture and participating in decision making. Traditional administration is becoming algorithmic which implies that the medium which is used for storing data is no longer passive but active, alive and controlling because artificial intelligence interprets the data, produces new pieces of information based on them and takes further actions. Privacy and other human rights and liberties do not depend solely on decisions made by humans, but also by the ones created by algorithms which are being increasingly widespread not just throughout social media and other online platforms but by all institutions of the society. Algorithms are problematic because of their black-box nature or lack of transparency. The aim of this paper is to analyse the key differences between the traditional and contemporary surveillance systems and emphasise the need to examine and rethink ethical principles of utilising artificial intelligence with regards to the protection of human rights and liberties.

Keywords: algorithms, surveillance, human rights, privacy, technology.

Драгица БОГЕТИЋ, асистент
Факултет за специјалну едукацију
и рехабилитацију
Универзитета у Београду

Прегледан рад
Примљено: 10.08.2020.
Прихваћено: 14.12.2020.

Доц. др МИЛИЦА КОВАЧЕВИЋ, доцент
Факултет за специјалну едукацију и рехабилитацију
Универзитета у Београду

ПОВЕЗАНОСТ НЕГАТИВНИХ ИСКУСТАВА У ДЕТИЊСТВУ СА ЗЛОУПОТРЕБОМ АЛКОХОЛА И АЛКОХОЛИЗМОМ У ОДРАСЛОМ ДОБУ

Истраживања негативних дечјих искустава представљају водећа истраживања у области поређења здравља (и благостања) одраслих са искуствима у детињству која су се дешавала и деценијама раније. Негативна искуства у детињству обухватају низ трауматичних и стресних догађаја који могу утицати на емоционални, социјални и когнитивни развој деце. Ова искуства се односе на различите видове злостављања, занемаривања и одрастања у дисфункционалном породичном окружењу, присуство сценама породичног насиља, одрастање са чланом породице који је алкохоличар, наркоман, суицидалан или има менталне болести, родитељска неслога, криминалитет у породици и сл. (уобличени под појмом “Adverse Childhood Experiences – ACE”).

НИД су повезани, између осталог, и са повећаним ризиком од усвајања низа ризичних понашања. Преко иницијације и развијања ризичних понашања, НИД су повезана и са хроничним здравственим болестима и стањима, ниским животним потенцијалом и раном смртношћу (National Center for Injury Prevention and Control, 2019). Истраживања показују јасну рефлексију негативних искустава у детињству на злоупотребу алкохола и ризик од развоја алкохолизма у одраслој доби.

Стога, општи циљ рада јесте да се анализирају резултати савремених истраживања која су пратила повезаност негативних искустава у детињству и проблема са алкохолом у одраслој доби. Поред тога, специфични циљеви рада се односе на утврђивање појава/