*Др Драган Дакић,*
*доцент*

*УДК: 342.738:004.738.5*
*DOI: 10.46793/UPSSXI.245D*

# МАСОВНО ПРОФИЛИСАЊЕ НА ОСНОВУ ПОДАТАКА СА ДРУШТВЕНИХ МРЕЖА: ЗАШТО ДА НЕ?*

## *Резиме*

*Да ли правни стандарди Европске уније допуштају масовну обраду података које су њихови титулари учинили јавним а у циљу менталне подршке или превенције злочина? Наведено истраживачко питање је анализирано у оквиру хипотетичког става да овакво масовно профилисање не представља кршење права појединаца. Силогистички аксиоми ове хипотезе су 1. јавни органи проводе масовно профилисање на основу закона у складу са легитимним циљем, 2. масовно профилисање које се проводи на основу закона у складу са легитимним циљем не крши права појединаца. У методолошком смислу наведена хипотеза је испитана антитезом која заговара увођење права појединаца да буду заштићени од масовног профилисања као sui generis права заснивајући се управо на тврдњама да масовно профилисање крши право на приватност као и право на заштиту личних података. Доминатни научни методи који су коришћени у истраживању су метод дедукције и метод индукције као и студија случаја. Ови методи су примјењени у анализи обима и садржине права на приватност из чл. 8 Европске конвенције за заштиту људских права као и обима и садржине права на заштиту личних података из GDPR-а у односу на праксу масовног профилисања. Осим одговора на истраживачко питање, рад нуди основ за даље истраживање евентуалних позитивних обавеза државе у области заштите здравља и спрјечавања криминала и нереда. Такође, у раду је садржано појмовно дефинисање машинског учења и масовног профилисања које недостаје у правничкој литератури као и дистинкција између масовног профилисања и аутоматског одлучивања које је често, али погрешно, синонимизовано. Истраживање је ограничено на анализи масовног профилсиања које проводе државни органи на основу јавних овлашћења. Истраживање не обухвата масовно профилисање које проводе приватне компаније.*

* Рад је резултат истраживања на пројекту Правног факултета Универзитета у Крагујевцу: „*Усклађивање правног система Србије са стандардима Европске уније*”, који се финансира из средстава Факултета.

***Кључне ријечи:*** *масовно профилисање, право на приватност, право на заштиту личних података.*

## 1. Увод

У свом недавном чланку Плоуг описује начине на које анализа података добијених са друштвених мрежа помоћу модела вјештачке интелигенције (ВИ) носи значајан потенцијал за предвиђање психичко-психолошких здравствених стања[1] из чега не треба искључити ни потенцијал за превенцију злочина. Тако се наводи примјер анализитања фотографија објављених на друштвеној мрежи Инстаграм[2] односно Твитер[3], када су одређени модели машинског учења били у стању да идентификују депресивне кориснике са већом прецизношћу од љекара користећи се искључиво фотографијама које су корисници објављивали. Софтверска „дијагностика" је изведена из визуелних односно језичких карактеристика објава које су биле софтверски читљиве попут осврјетљења фотографија и њихових боја односно употребљених ријечи (позитивне-негативне) у објавама. Осим депресије, показало се да модели машинског учења могу да идентификују шири спектар менталних поремећаја, попут анксиозности, биполарног поремећаја, граничног поремећаја личности, шизофренију, аутизам,[4] ризик од самоубиства и анорексије.[5]

Оно што се може уочити као могућа правна препрека за упортебу поменутих модела машинског учења на описани начин тиче се заштите приватности односно употребе личних података која може бити проблематична због недостатка експлицитног пристанка њихових титулара. Аргументативна линија коју Плоуг развија у свом заговарању признања *sui generis* права појединца да буде заштићен од ових праски изграђена је на трипартиној конструкцији:[6] прво, да подаци и њихова употреба могу резултовати стигматизацијом титулара и довести до наглашене друштвене контроле; затим прфилисање помоћу ВИ је различито од осталих видова профилисања (тзв.

[1] Ploug, T., *The Right Not to Be Subjected to AI Profiling Based on Publicly Available Data—Privacy and the Exceptionalism of AI Profiling*, *Philos. Technol*, 36, 14 (2023). https://doi.org/10.1007/s13347-023-00616-9

[2] https://www.instagram.com/

[3] https://twitter.com/home

[4] Gkotsis, G., Oellrich, A., Velupillai, S., Liakata, M., Hubbard, T. J. P., Dobson, R. J. B., Dutta, R., *Characterisation of mental health conditions in social media using Informed Deep Learning*, Scientifc Reports, 7(1), Art. 1, 2017. Преузето од Ploug, T., *нав. чланак.*

[5] Amini, H., Mohammadi, E., Kosseim, L. *Quick and (maybe not so) easy detection of anorexia in social media: To explainability and beyond*, 141–158. In F. Crestani, D. E. Losada, & J. Parapar (Eds), *Early Detection of Mental Health Disorders by Social Media Monitoring: The First Five Years of the eRisk Project*, Springer International Publishing, 2022. Преузето од Ploug, T., *нав. чланак.*

[6] Ploug, T., *нав. чланак.*

аргумент ексепционалности или изузетности), као и то да је заштита *online* интерактивности посебно важна. Осим тога овај аутор наводи недостатности релавантних извора ЕУ права како би нагласио потребу за квалификовањем преложеног права као *sui generis* права.[7]

У овом раду ћемо посматрати предложене аргументе у контексту хпотетичког става да је масовно профилисање у циљу менталне подршке и превенције криминалитета дозвољено са аспекта важећих стандарда који се примјењују у Европској унији односно који се односе на заштиту личних података. Анализа ће се ослањати на доктринарне и формалне аспкете постављеног конфликта између права појединаца и праксе масовног профилисања. Што се тиче доктринарног аспекта он ће се односити на валоризацију предложених аргумената у односу на важеће стандарде заштите приватности и заштите личних података који су установљени кроз судску праксу и правну теорију. Формални аспект анализе посматраног конфликта ће се ослањати на лоцирање релевантних извора права који се примјењују у Европској унији те њихово језичко, онтолошко и системско тумачење.

У првом дијелу рада централно питање јесте „да ли се масовно профилисање данас користи, на који начин и у које сврхе?“, али како бисмо адекватно одговорили на постављено питање претходно је посвећена пажња појмовном дефинисању машинског учења и масовног профилисања. Машинско учење је представљено са аспекта његове дефиниције и са аспекта његове сврхе. Обе обе карактеристике су од правног значаја у поступку валоризације утицаја који овај поступак може да има на права појединаца. Због тога, представљене су алгоритамске шеме по којима се поступак машинског учења одвија те је идентификован правно најприхватљивији алгоритам. Масовно профилисање је појмовно дефинисано са правног и техничког аспекта. Анализа правног аспекта је обухватила теоретску концептуализацију масовног профилисања као и главне позитивно-правне оквире који се примјењују на ову праксу. Први дио рада се закључује одоговором на централно питање уз указивање на познате облике и алате масовног профилисања које је већим дијелом изостављено из овог истраживања.

Како бисмо провјерили аргументативну ваљаност која подржава увођење права на заштиту од масовног профилисања као *sui generis* права, у другом дијелу рада смо анализирали његове силогистичке аксиоме и то: масовно профилисање је супротно гаранцијама права на приватност; и масовно провилисање крши право на заштиту личних података. У том циљу анализираћемо поставке релевантних правних извора и то Европске конвенције која поставља стандарде заштите приватности и GDPR-а која је централни инструмент за заштиту личних података у правном систему Европске уније. Уз овај, централни инструмент анализа ће указати и на друге релевантне акте.

[7] *Исто.*

## 2. Масовно профилисање, тренутно стање ствари

*Уколико овај рад читате преко неког електронског уређаја,*
*већ сте подвргнути процесу профилисања*

Да бисмо боље разумјели контекст истраживања као и постављени хипотетички оквир неопходно је да испитамо да ли се масовно профилисање данас користи, на који начин и у које сврхе? Дакле, предмет истраживања у овом дијелу обухвата двије категорије и то машинско учење и масовно профилисање чије појмовно дефинисање је неопходно прије одговора на постављено питање.

Машинско учење је свеприсутна појава у свакодневним животима. Тако, свака употреба *Google* претраживача већ активира поступак машинског учења како на улазној тако и на излазној тачки обраде података. Сам појам машинског учења се може различито дефинисати у зависности од карактеристике коју ћемо узети за централну. У литератури је значајно заступљен став Артура Самјуела према којем је машинско учење дефинисано као област учења која рачунарима даје могућност да уче без експлицитног програмирања.[8] Према аутору Бата Махешу, сврха машинског учења је да учи из података, а када алгоритам научи шта да ради са подацима, може аутоматски да ради свој посао.[9] Како би ова сврха била успјешно испуњена машинско учење се ослања на различите алгоритме као што су учење под надзором, учење без надзора и учење уз помоћ. Надзирано учење је функција која пресликава улазне податке на излазним подацима на основу примјера парова улаз-излаз. Учење без надзора је функција за описивање скривене структуре из „неозначених" података. Учење уз помоћ је област машинског учења која се бави тиме како софтверски агенти треба да предузму акције у окружењу како би максимизирали појам кумулативног резултата. Раније сам указао на мањкавости система који се заснивају на надзираном учењу.[10] Свакако, они нису техничке природе већ произилазе из ненадзирног учешћа људског фактора. Слични се приговори могу ставити и на учење без надзора док се учење уз помоћ или учење под надзором чини најприхватљивијим алгоритмом. Разлог томе је у чињеници да учење под надзором карактеришу бројне особине

[8] Mahesh, B., *Machine learning algorithms-a review*, International Journal of Science and Research *(IJSR).[Internet]* 9.1 (2020), pp. 381-386.
[9] *Исто*.
[10] Dakić, D., *Reproductive Autonomy Conformity Assessment of Purposed AI System*. In *Serbian International Conference on Applied Artificial Intelligence*, Cham: Springer International Publishing, pp. 45-57.

као што су прилагодљивост, употребљивост, предвидљивост, унапредљивост,[11] чинећи га правно најпогоднијим за употребу приликом масовног профилисања.

Што се тиче појама профилисања, он садржи своју техничку и правну димензију. У техничком смислу масовно профилисање можемо посматрати као процес систематске анализе и категоризације података или информација, с циљем да се идентификују, оцјене и/или предвиде атрибути, карактеристике или обрасци понашања појединца или групе. Сам поступак укључује коришћење статистичких анализа, алгоритама, и других аналитичких алата.[12] Правна димензија по својој природи садржи теоретски аспект и позитивно-правни аспект.

Основне елементе теоретске концептуализације предмета нашег истраживања у овом дијелу рада можемо пронаћи код Хилдебрандт, М. (2008). у дјелу „Профилисање и идентитет европског грађанина“[13] у којем се примјеном доминантно критичког метода анализирају ефекти које профилисање има на лични идентитет али и социјалне норме. Забринутост овим праксама и технологијама артиклуисана је кроз анализу правних и филозофских основа на којима се темеље управо демократске вриједности попут људских права или поменутог идентитета. У доктрираном смислу овај извор слиједи линију типичног правничког приступа који се не одмиче даље од „избјегавање штете“ резона.[14] Сходно томе, предложена је чврста и свеобухватна регулатива како би се заштитиле посматране вриједности. Прагматичнији приступ можемо пронаћи код аутора Кастерс, Б. и Вергоу, С. (2015) у дјелу „Обећавајуће полицијске технологије: искуства, препреке и полицијске потребе у вези са технологијама за спровођење закона.“[15] Ови аутори не занемарују правне и етичке дилеме и изазове које прате пофилисање али правилно уочавају предности ове праксе које се прије свега односе на повећање ефикасности рада полиције и спровођење закона. Учљиво је да се овде ради о два приступа питању масовног профилисња који нису драстично удаљени један од другог. Наиме, уколико бисмо ставове изражене код Хилдебрандта могли сврстати у извјесном смислу као крајње поларизоване који посматраној пракси дају искључиво негативне конотације, утолико су ставови изражени код Кастерс, Б. и Вергоу ближи средњем курсу који уважава правне и етичке изазове али не занемарује корисности праксе профилисања.

---

[11] Burkart, N., Marco F. H., *A survey on the explainability of supervised machine learning*, Journal of Artificial Intelligence Research, 70 (2021), pp. 245-317.

[12] Mitchell, T. M., *Machine Learning*, McGraw-Hill Science/Engineering/Math, 1997.

[13] Hildebrandt, M., Gutwirth, S., *Profiling the European citizen*. Dordrecht Springer, 2008.

[14] Дакић, Д., *Аватари као пружаоци услуга: међународноправни аспекти*, Зборник радова: Правна регулатива услуга у националним законодавствима и праву Европске уније, Крагујевац, 2023.

[15] Custers, B., *Technology in Policing: Experiences, Obstacles and Police Needs*. In Custers B.H.M. (2012), Technology in Policing: Experiences, Obstacles and Police Needs, Computer law & security report (1), pp. 62-68, Available at SSRN: https://ssrn.com/abstract=3047124

Профилисање у контексту позитивног права Европске уније (ЕУ) повлачи неколико правних импликација. Општа уредба о заштити података (*GDPR*) је кључни правни оквир који регулише прикупљање и обраду личних података унутар ЕУ. Када је у питању профилисање, *GDPR* предвиђа посебне одредбе за заштиту права појединаца. Према слову овог извора можемо сматрати да се профилисање односи на било који облик аутоматизоване обраде личних података ради процене одређених личних аспеката, као што је анализа или предвиђање нечијег учинка на послу, економске ситуације, здравља, личних преференција, интересовања, понашања, локације или кретања. Због наведеног, поступак профилисања је у кореалтивној интеракцији са читавим спектром тангентних права као што су право на информисање које подразумјева право титулара података да буде упознат са поступком профилисања, његовој методологији и ефектима; затим право на приговор о којем свако лице мора бити благовремено поучено а које овлашћује титулара података да приговори на сам процес профилисања те доведе до његовог обустављања, затим право на увид и исправку које овлашћује титулара података да изврши увид у податке коришћене за профилисање те тражи и добије њихову корекцију; и минимализација података и безбједност које гарантују титулару прикупљање само нужних података потребних за испуњење сврхе у коју се прикупљају те њихово безбједно чување.

Не треба занемарити ни значај правног основа по којем се проводи профилисање. Наиме, да би профилисање било уопште могуће са правног аспекта, основ по којем се оно проводи мора да буде заснован на праву и укључује изричит пристанак појединца, неопходност извршења уговора, поштовање законске обавезе, заштиту виталних интереса, обављање задатка у јавном интересу или у вршењу службених овлашћења, као и други законом утврђени легитимни интереси.

Сада, што се тиче питања да ли се масовно профилисање данас користи, на који начин и у које сврхе, можемо рећи да је већ познато да се масовно профилисање користи у разним областима живота како од стране јавног сектора, у области безбједности, образовања, здравства, правосуђа тако и од стране приватног сектора у сфери маркетинга и е-трговине.[16] Посебно су занимљиви правни аспекти масовног профилисања у чију сврху приватне компаније користе осим паметних уређаја и друге најразличитије уређаје укључујући усисиваче повезане на интернет, веш машине, или аутомобиле[17] прикупљајући широк спектар података - од генетских до оних најприватнијих попут сексуалног живота власника. Ван сваке сумње је да прикупљени подаци нису усмјерени на побољшање функција самог уређаја као и то да поступак

[16] Wiedemann K., *Profiling and (automated) decision-making under the GDPR: A two-step approach*, Computer Law & Security Review, Vol. 45, 2022.

[17] https://www.jutarnji.hr/autoklub/aktualno/od-vaseg-seksualnog-zivota-do-toga-koliko-brzo-vozite-moderni-auti-svakodnevno-spijuniraju-vlasnike-15373502

прикупљања и обраде података пати од озбиљних правних недостатака, између осталих и недостатка експлицитног информисаног пристанка. Због обима самог рада, овде неће бити даље експланације напредних технологија за профилисање било индивидуално путем отворених програма попут *deepmood*[18] било масовно путем програма као што је *pixels*.[19]

## 3. Право на заштиту од масовног профилисања као *sui generis* право

Из уводног дијела овог рада евидентно је да се идеја о увођењу *sui generis* права појединца да буде заштићен од масовног профилисања може ослонити на двије врсте аргумената и то су правни и политички аргументи. Правни аргументи се односе на потребу заштите приватности у конфликту који настаје усљед масовног профилисања а који је појачан недостатком експлицитног информисаног пристанка титулара података. У оквиру аргумента о заштити приватности може се резоновати о тврдњи да масовно профилисање доводи до стигматизације. Из аргумента о заштити приватности логички деривира додатни аргуметн који се односи на заштиту личних података. Ипак, аргумент о заштити личних података не треба свести на дериват претходног аргумента управо због његовог нормативног утемељења као самосталног права у релевантним позитивно-правним изворима. Што се тиче политичких аргумената они се ослањају на тврдњу да предметна пракса може довести до повећања друштвене контроле, што само по себи не мора да представља (правну) недопуштеност; као и на тврдњу да је заштита *online* интерактивности посебно важна, којој са правног аспекта недостаје јасна заснованост на узрочно-посљедичној повезности посматране праксе и спутавања *online* интерактивности. Међутим, неправне аргументе није неопходно укрштати са правним јер се њихова валидација не врши на основу правне ваљаности.

Како бисмо провјерили аргументативну ваљаност која подржава увођење права на заштиту од масовног профилисања као *sui generis* права, неопходно је да размотримо њихове основне силогистичке аксиоме и то: масовно профилисање је супротно гаранцијама права на приватност; и масовно провилисање крши право на заштиту личних података. У том циљу анализираћемо поставке релевантних правних извора и то Европске конвенције која поставља стандарде заштите приватности и GDPR-а која је централни инструмент за заштиту личних података у правном систему Европске уније. Уз овај, централни инструмент анализа ће указати и на друге релевантне акте.

[18] https://deepmood.io/en_US/features
[19] https://www.digitalmarketer.com/blog/what-is-tracking-pixel/

### *3.1. Масовно профилисање и стандарди чл. 8 Европске конвенције*

Члан 8 Европске конвенције за заштиту људских права и основних слобода (Конвенција, Европска конвенција),[20] гласи:

1. Свако има право на поштовање свог приватног и породичног живота, дома и преписке.

2. Јавне власти се не смију мијешати у остваривање овог права осим ако то није у складу са законом и неопходно у демократском друштву у интересима националне безбједности, јавне безбједности или економске добробити земље, ради спречавања нереда или криминала, ради заштите здравља или морала, или ради заштите права и слобода других.

Европски суд за људска права (Суд) је већ имао прилике да разматра питање масовног профилисања, односно масовног праћења у јавном сектору што одговара предмету нашег интересовања. Из неколико следећих случајева моћи ћемо јасно да уочимо стандарде из чл. 8 Европске конвенције. У случају *Klass v Germany*,[21] подносиоци представке су тврдили да је неколико њемачких законских аката који дозвољавају тајни надзор поште, електронске поште и телекомуникација прекршило чл. 8 Европске конвенције о људским правима (ЕКЉП). Своју тврдњу су темељили на томе што дотична надзирана особа није била обавештена о мјери надзора и није постојала могућност судског одлучивања. Европски суд за људска права је сматрао да је мјешање у право на приватност подносиоца представке било оправдано јер релевантни национални закон пружа довољне гаранције против потенцијалне злоупотребе. Штавише, Суд је истакао да је оспорено законодавство обезбједило ефикасну контролу над правима појединца.

Следећи значајан случај је *Malone v United Kingdom*.[22] У овом предмету подносилац представке је тврдио да је полиција пресрела његову преписку, телефонске разговоре и телефонске линије. Суд је сматрао да постојање неког закона који даје овлашћења за пресретање комуникација како би се помогло полицији у њеној функцији спречавања криминала може бити неопходно у демократском друштву. Међутим, вршење таквих овлашћења мора бити предмет адекватних заштитних механизама од злоупотребе. У овом конкретном случају, оспорени закон није испунио стандард прецизности који служи као гаранција за спрјечавање злоупотреба. Наиме, одредбе о обиму дискреционих овлашћења као и о начину њиховог вршења су биле нејасне.

[20] "Convention for the Protection of Human Rights and Fundamental Freedoms." Council of Europe Treaty Series 005, Council of Europe, 1950. Bibliography: Council of Europe, 1950.
[21] *Klass v Germany* (App. 5029/71), 6 September 78.
[22] *Malone v the United Kingdom* (App. 8691/79) 2 August 1984.

Стога је Суд сматрао да мешање није било у складу са чл. 8(2) Европске конвенције о људским правима.[23]

У случају *S. and Marper v United Kingdom,*[24] подносиоци представке су били оптужени за кривична дјела, али је изостала пресуда којом би били оглашени кривима. Без обзира на то, полиција је чувала њихове отиске прстију, профиле ДНК и ћелијске узорке. Међутим, иако је овакво неограничено задржавање биометријских података било дозвољено законом када је лице осумњичено за кривично дјело, чак и ако је осумњичени касније буде ослобођен, Суд је ипак сматрао да мјешање у право подносилаца представке на поштовање приватног живота није било у складу са законом. Суд је извео овај закључакмиз чињенице да задржавање предметних биометријских података није било ограничено на сврху почетне истраге и није било засновано на објективним доказима о перманентној потреби. Суд је такође сматрао да је задржавање биометријских података појединаца који нису осуђени ни за једно кривично дјело било несразмерно и стога није неопходно у демократском друштву.[25]

У случају *Liberty v United Kingdom,*[26] подносиоци представке су тврдили да је Министарство одбране управљало електронским тестним постројењем (ЕТФ) за пресретање свих јавних телекомуникација, укључујући телефоне, факсимилне и е-маил комуникације, које се преносе микроталасном радиом везом. Ова веза је иначе преносила и велики део телекомуникационог саобраћаја Ирске. Подносиоци представке су тврдили да је обавеза државе да направи „аранжмане“ када је издат налог за пресретање представљала мешање у права из чл. 8(1) ЕКЉП и била је противна захтјеву предвидивости јер би потенцијално један налог могао да одобри пресретање сваке комуникације. Суд је сматрао да домаћи закон није довољно јасно указао на то да би се обезбедила адекватна заштита од злоупотребе овлашћења и јер су, опет, обим или начин вршења дискреционог права датог властима. Стога је Суд сматрао да мешање није оправдано према чл. 8(2) Европске конвенције о људским правима.

Дакле, узимајући у обзир судску праксу свако мјешање у право на поштовање приватног и породичног живота из чл. 8 Конвенције мора испуњавати три врсте услова и то како слиједи:

1. усклађеност са законом,
2. неопходност у демократском друштву те
3. пропорционалност са легитимним циљем којем се тежи.

Несумњиво је да масовно профилисање које се проводи у јавном сектору из безбједносних разлога задире у право на приватност грађана. Међутим, ово право није апсолутно, те мјешање само по себи не мора бити супротно захтјевима Конвенције. Суд би у сваком конкретном случају цијенио да ли је

[23] *Исто*, para 65
[24] *S. and Marper v the United Kingdom* (Apps. 30562/04 and 30566/04) 4 December 2008.
[25] *Исто*, para 119.
[26] *Liberty v the United Kingdom* (App. 58243/00) 1 July 2008.

мјешање легитимно или не. Евидентно, ова процјена ће у битној мјери зависити од „квалитета закона“ којма се уређује обим дискреционих овлашћења поступајућих органа као и прописани начин коришћења тих овлашћења.

## *3.2 Масовно профилисање и право ЕУ*

Што се тиче правних оквира установљених у Европској унији а тичу се заштите података, можемо идентификовати три главна извора и то: Директива о заштити података,[27] Општа уредба о заштити података (*GDPR*)[28] и Директива о полицији.[29] *GDPR* је замјенила Директиву о заштити података те јој припада централно мјесто по питању заштите личних података у правном систему Европске уније. Директива о полицији препознаје специфичну природу активности спровођења закона и представља *lex specialis* у односу на *GDPR*. Уопштено говорећи ни један од наведених извора не гарантују јасно, спроводиво и дјелотворно право када је у питању профилисање. Међутим, ови извори ипак јесу примјењиви на профилисање нарочито када је у питању аутоматско одлучивање које је у одређној мјери третирано на рестриктиван начин.

Овде наглашавамо потребу процесног и материјалног разликовања између масовног профилисања и аутоматског одлучивања. Наиме, како је претходно објашњено сврха масовног профилисања је да се предвиди понашање појединца и/или групе. Масовно профилисање само по себи не доводи ни до какве фактичке промјене стања ствари. У процесном смислу оно представља фазу прикупљања података, дакле не директно доказа, и може да пружи ослонац за било коју врсту мериторног одлучивања. Слично схватање налазимо и код Турбан, Е., Шарда, Р., и Дален, Д.[30] према којем "аутоматско одлучивање може се односити на системе који користе предефинисана правила, алгоритме и логичке операције да би обрадили велике количине информација и подржали

[27] European Parliament and Council Directive 95/46/EC of 24 October 1995 on the “protection of individuals with regard to the processing of personal data and on the free movement of such data [Official Journal L 281 of 23.11.1995]”.

[28] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the “protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)”.

[29] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the “protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA”

[30] Turban, E., Sharda, R., Delen, D., *Decision Support and Business Intelligence Systems* (9th ed.), Prentice Hall, 2010.

процес одлучивања."[31] Јасно је да и овакво прикупљање података мора да буде законом регулисано и усклађено са важећим стандардима који се свакако разликују у зависности од врсте података тј. да ли су они учињени јавним или су на неки начин означени и заштићени као приватни. За разлику од овог, аутоматско одлучивање „се односи на одлучивање које је у цјелости аутоматизовано, без неког значајног људског учешћа“ (*GDPR*, чл. 22). Дакле, аутоматско одлучивање карактеришу двије особине и то недостатак људског учешћа и мериторан исход поступка. Наведено је уочљиво и код Митчел, Т који аутоматско одлучивање дефинише као „процес коришћења алгоритама и модела машинског учења да се анализирају подаци и да се на основу тих анализа дође до одлука без директне људске интервенције."[32]

Претходно речено не треба схватити као да је аутоматско одлучивање забрањено. Радије, постоје гаранције којима је циљ заштита права појединаца путем права на приговор, на информисаност итд. Члан 22(2)(ц) и 22(3) захтјевају изричиту сагласност појединца за аутоматско доношење одлука, укључујући профилисање, у одређеним околностима. Иако у контексту *GDPR* можемо дискутовати о постојању забране аутоматског одлучивања у случајевима када таква одлука „значајно“ утиче на права појединца, сасвим је јасно да *GDPR* не садржи одредбе које забрањују масовно профилисање, нити садржи дјелотворне гаранције за заштиту појединаца од ове праксе.[33] Гаранције *GDPR*–а директно се односе на аутоматско одлучивање не на масовно профилисање.

Што се тиче Директиве о полицији[34] као што је већ речено она егзистира као посебан извор у области спровођења закона. Директива замјењује Оквирну одлуку о заштити података из 2008. године и признаје специфичну природу области безбедности, која заслужује посебан правни приступ. По узору на *GDPR*, Директива забрањује профилисање када резултати могу довести до дискриминације, што је рефлексија позитивне интенције у превенцији ризика који прате профилисање. Међутим, постоје разумне сумње о примјени овог члана у пракси.[35] Изјаве органа за спровођење закона често повезују криминалне активности са групама које се разликују по својој вјери, земљи порјекла, друштвеној класи, итд.[36] Чини се да се правни стандарди описани у Директиви ипак могу екстензирати до мјере несврсисходности.

[31] *Исто*.
[32] Mitchell, T. M., *нав. дјело*.
[33] Ghazarossian, G., Galič, M., *Under which circumstances does profiling carried out by public authorities upon their citizens for the purpose of prevention of crime and disorder, violate the fundamental right to privacy under the European Convention on Human Rights*?.
[34] Directive (EU) 2016/680 of the European Parliament …
[35] Ghazarossian, G., Galič, M., *нав. дјело.*
[36] *Исто*.

## 4. Закључак

Централно питање у првом дијелу рада било је „да ли се масовно профилисање данас користи, на који начин и у које сврхе?“. У циљу адекватног одговора машинско учење је дефинисано као област учења из података која рачунарима даје могућност да уче без експлицитног програмирања, а када алгоритам научи шта да ради са подацима, може аутоматски да ради задате радње. Даље, сам појам масовног профилисања је дефинисан са техничког и правног аспекта. У техничком смислу масовно профилисање је посматрано као процес систематске анализе и категоризације података или информација, с циљем да се идентификују, оцјене и/или предвиде атрибути, карактеристике или обрасци понашања појединца или групе.

У правном смислу анализа је показала нашто компликованију струкруту те смо идентификовали његову теоретску концептуализацију која се креће од негативног контекстуализовања односа посматране праксе и права појединаца до утулитаријанског резоновања које предлаже прагматичнији приступ овој пракси; као и нормативни дио који се односи на релевантне гаранције *GDPR*-а међу којима су идентификоване право на информисање које подразумјева право титулара података да буде упознат са поступком профилисања, његовој методологији и ефектима; затим право на приговор о којем свако лице мора бити благовремено поучено а које овлашћује титулара података да приговори на сам процес профилисања те доведе до његовог обустављања, затим право на увид и исправку које овлашћује титулара података да изврши увид у податке коришћене за профилисање те тражи и добије њихову корекцију; минимализација података и безбједност које гарантују титулару прикупљање само нужних података потребних за испуњење сврхе у коју се прикупљају те њихово безбједно чување и правни основ по којем се проводи профилисање.

Ипак, овај дио рада нам је показао да се масовно профилисање непрестано користи како од јавног тако и од приватног сектора који се истиче по обиму и алатима масовног профилисања и готово извјесне неусклађености са стандардима заштите права појединаца.

Други дио рада, након класификације аргумената на политичке и правне, фокусирао се на испитивање ваљаности правних аргумената на основу којих се тражи увођење права на заштиту појединаца од масовног профилисања као *sui generis* права. Силогистички аксиоми овог аргумента су:

1. да је масовно профилисање супротно гаранцијама права на приватност – што је тестирано у односу на гаранције из чл. 8 Европске конвенције, и

2. да масовно провилисање крши право на заштиту личних података - што је тестирано у односу на релевантне одредбе GDPR-а као централног инструмента за заштиту личних података у правном систему Европске уније као и у односу на други *lex specialis* извор.

Закључци до којих смо дошли анализирајући однос масовног профилисања и гаранција којима се штити право на приватност из обима чл. 8

Европске конвенције су да свако мјешање у право на поштовање приватног и породичног живота из чл. 8 Конвенције мора испуњавати три врсте услова и то како слиједи:

1. усклађеност са законом,
2. неопходност у демократском друштву те
3. пропорционалност са легитимним циљем којем се тежи.

Несумњиво је да масовно профилисање које се проводи у јавном сектору из безбједносних разлога задире у право на приватност грађана. Међутим, ово право није апсолутно, те мјешање само по себи не мора бити супротно захтјевима Конвенције. Суд би у сваком конкретном случају цијенио да ли је мјешање легитимно или не. Из досадашње судске праксе евиденто је да ће ова процјена у битној мјери зависити од „квалитета закона" којма се уређује обим дискреционих овлашћења поступајућих органа као и прописани начин коришћења тих овлашћења.

Закључци до којих смо дошли анализирајући правне оквире ЕУ примјењиве на масовно профилисање су следећи. Прво, правни извори се примарно баве питањима аутоматског одлучивања док је питање масовног профилисања акцесоарно постављено. Ради тога у раду је указано на процесну и материјалну различитост ова два поступка. Наиме, исход масовног профилисања не доводи ни до какве фактичке промјене стања ствари. У процесном смислу оно представља фазу прикупљања података, дакле не директно доказа, и може да пружи ослонац за било коју врсту мериторног одлучивања. За разлику од овог, аутоматско одлучивање карактеришу двије особине и то недостатак људског учешћа и мериторан исход поступка. Тако, у контексту *GDPR*–а можемо дискутовати о постојању забране аутоматског одлучивања у случајевима када таква одлука „значајно" тј мериторно утиче на права појединца. Суштина ове забране је у недопуштености декларативног одлучивања, јер аутоматско одлучивање је управо то, о мериторним стварима које по се по својој природи окончавају конститутивним одлукама.

С обзиром да се гаранције *GDPR*–а директно се односе на аутоматско одлучивање не на масовно профилисање закључујмео да *GDPR* не садржи одредбе које забрањују масовно профилисање, нити садржи дјелотворне гаранције за заштиту појединаца од ове праксе. По узору на *GDPR*, Директива забрањује профилисање када резултати могу довести до дискриминације, међутим, правни стандарди описани у њој могу се екстензирати до мјере несврсисходности тако да ни овај правни инструмент не мјења стање по питању забране масовног профилисања.

На основу свега претходно изнесеног одговор на истраживачко питање гласи да правни стандарди Европске уније допуштају јавним властима масовну обраду података које су њихови титулари учинили јавним а у циљу менталне подршке или превенције злочина који су препознати као легитимни циљеви у демократским друштвима.

*Dragan Dakić, Ph.D.,*
*Assistant Professor*

# MASS PROFILING BASED ON SOCIAL NETWORK DATA: WHY NOT?

## *Summary*

*Is it acceptable under EU legal standards for public bodies to conduct mass profiling of data that has been publicly shared for the purpose of mental support or crime prevention? This research question examines the hypothetical position that mass profiling does not violate individual rights. The hypothesis is based on two syllogistic axioms: 1) mass profiling is carried out by public bodies according to the law with a legitimate aim, and 2) mass profiling that is lawful and carried out for a legitimate aim does not infringe on individual rights. The hypothesis is tested methodologically through an antithesis that proposes introducing a right for individuals to be protected from mass profiling, based on the claims that mass profiling violates the right to privacy and the right to protection of personal data. The research used deductive and inductive methods, as well as case studies, to analyze the scope of Article 8 of the European Convention for the Protection of Human Rights regarding the right to privacy and the GDPR's right to protection of personal data in relation to mass profiling. The research provides a foundation for further exploration of the state's positive obligations in health protection and prevention of crime and disorder. Additionally, the paper offers a conceptual definition of machine learning and mass profiling, which is absent in legal literature, and distinguishes mass profiling from automatic decision-making, which is often mistakenly used synonymously. The study is limited to analysis of mass profiling conducted by state authorities on public authority and does not include mass profiling by private companies.*

***Key words:*** *mass profiling, right to privacy, right to protection of personal data.*

## Литература

Amini, H., Mohammadi, E., Kosseim, L. *Quick and (maybe not so) easy detection of anorexia in social media: To explainability and beyond*, 141–158. In F. Crestani, D. E. Losada, & J. Parapar (Eds), *Early Detection of Mental Health Disorders by Social Media Monitoring: The First Five Years of the eRisk Project*, Springer International Publishing, 2022.

Burkart, N., Marco F. H., *A survey on the explainability of supervised machine learning*, Journal of Artificial Intelligence Research, 70/2021.

Ghazarossian, G., Galič, M., *Under which circumstances does profiling carried out by public authorities upon their citizens for the purpose of prevention of crime and disorder, violate the fundamental right to privacy under the European Convention on Human Rights*?.

Gkotsis, G., Oellrich, A., Velupillai, S., Liakata, M., Hubbard, T. J. P., Dobson, R. J. B., Dutta, R. *Characterisation of mental health conditions in social media using Informed Deep Learning*, Scientifc Reports, 7(1), Art. 1, 2017.

Дакић, Д., *Аватари као пружаоци услуга: међународноправни аспекти*, Зборник радова: Правна регулатива услуга у националним законодавствима и праву Европске уније, Крагујевац, 2023.

Dakić, D., *Reproductive Autonomy Conformity Assessment of Purposed AI System*. In *Serbian International Conference on Applied Artificial Intelligence*, Cham: Springer International Publishing.

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the "protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA"

European Parliament and Council Directive 95/46/EC of 24 October 1995 on the "protection of individuals with regard to the processing of personal data and on the free movement of such data [Official Journal L 281 of 23.11.1995]"

*Klass v Germany* (App. 5029/71), 6 September 78

*Liberty v the United Kingdom* (App. 58243/00) 1 July 2008

Mahesh, B. *Machine learning algorithms-a review*, International Journal of Science and Research *(IJSR).[Internet]* 9.1, 2020.

*Malone v the United Kingdom* (App. 8691/79) 2 August 1984

Mitchell, T. M., *Machine Learning*, (1997) McGraw-Hill Science/Engineering/Math.

Ploug, T., *The Right Not to Be Subjected to AI Profiling Based on Publicly Available Data—Privacy and the Exceptionalism of AI Profiling*. *Philos. Technol.* **36**, 14 (2023). https://doi.org/10.1007/s13347-023-00616-9

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the "protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)"

*S. and Marper v the United Kingdom* (Apps. 30562/04 and 30566/04) 4 December 2008.

Turban, E., Sharda, R., Delen, D., *Decision Support and Business Intelligence Systems* (9th ed.). (2010). Prentice Hall

Hildebrandt, M., Gutwirth, S., *Profiling the European citizen*. Dordrecht, Springer, 2008.

"Convention for the Protection of Human Rights and Fundamental Freedoms." Council of Europe Treaty Series 005, Council of Europe, 1950. Bibliography: Council of Europe. (1950).

Custers, B., *Technology in Policing: Experiences, Obstacles and Police Needs*, In: Custers B.H.M. Technology in Policing: Experiences, Obstacles and Police Needs, Computer law & security report 1, 2012. Available at SSRN: https://ssrn.com/abstract=3047124

Wiedemann, K., *Profiling and (automated) decision-making under the GDPR: A two-step approach*, Computer Law & Security Review, Vol. 45, 2022.

https://deepmood.io/en_US/features
https://twitter.com/home
https://www.digitalmarketer.com/blog/what-is-tracking-pixel/
https://www.instagram.com/
https://www.jutarnji.hr/autoklub/aktualno/od-vaseg-seksualnog-zivota-do-toga-koliko-brzo-vozite-moderni-auti-svakodnevno-spijuniraju-vlasnike-15373502