

УДК 342.738:077

CERIF: S 123

DOI: 10.51204/Anali_PFBU_22106A

Др Далибор ПЕТРОВИЋ*

Др Дејан ПАВЛОВИЋ**

ПОДРИВАЊЕ АНОНИМНОСТИ У ДОБА ИНТЕРНЕТА

Након ране фазе развоја интернета која је почивала на анонимној комуникацији у виртуелним заједницама, у последње две деценије дешава се драматичан преокрет. Ширење употребе дигиталних платформи за умрежавање, с једне стране, и врло лабаве политике приватности на интернету, с друге стране, све више сужавају могућност анонимне употребе интернета.

Полазећи од таквих трендова, у раду се бавимо трансформацијом улоге онлајн анонимности из правне и друштвене перспективе са циљем да идентифујемо кључне факторе и актере који подстичу деанонимизацију интернета.

*У првом делу рада показујемо да је анонимност пратилац модернизације савремених друштава, али и да она може носити различите изазове по њихову слободу и безбедност. У другом делу рада анализирамо феномен анонимности на интернету кроз различите *pro et contra**

* Ванредни професор, Саобраћајни факултет Универзитета у Београду, Србија, d.petrovic@sf.bg.ac.rs.

** Доцент, Факултет политичких наука Универзитета у Београду, Србија, dejan.pavlovic@fpn.bg.ac.rs.

перспективе, обраћајући посебну пажњу на идентификацију кључних актера који доводе до свеопште деанонимизације, као једне од суштинских карактеристика организације и јавног и приватног живота у XXI веку.

Кључне речи: *Право на анонимност. – Приватност. – Дигиталне платформе. – Регулација. – Надзор.*

1. УВОД

Данас ће мало ко спорити да је за просечног корисника дигиталних технологија анонимност на интернету практично недостижна. Сведоци смо брзог развоја и множења технологија усмерених на идентификовање корисника интернета. Уводе се нове методе аутентификације, верификације и надзора, тако да се лица могу дигитално и биометријски идентификовати, означити, пратити и лоцирати у реалном времену. Паметни телефони препознају лица или отисак прста и са њима повезују бројне друге податке који су ускладиштени на персоналним уређајима или на разним серверима.

Уопште узев, након терористичког напада 11. септембра 2001. године у Њујорку, дакле управо у време снажног продора интернета у све сфере друштвеног живота, идеја људских права и слобода непрекидно уступа пред интересима националне безбедности. На делу је парадокс да сигурносне мере које су замишљене да заштите вредности либералне демократије значајно доприносе урушавању истих тих вредности (Posner 2006, 1). Чини се да безбедност као вредност тренутно ужива примат у односу на слободу и аутономију, због важности улоге државе у заштити физичке сигурности људи и имовине. У прилог тако песимистичне тврдње довољно је указати на бројне примере секуритизације различитих друштвених сфера након терористичких напада у Сједињеним Америчким Државама, Француској и Шпанији, а сличан ефекат је имала и мигрантска криза 2015. године. Извршна грана власти је у многим државама добила шири овлашћења са циљем заштите сигурности грађана – од дужине трајања притвора, до пресретања комуникације¹ и замрзавања имовине лица за која се сумња да помажу терористичким мрежама.² То стање је израз комуни-

¹ Најпознатији пример је амерички Закон о патриотизму из 2001. године (*Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism [USA Patriot] Act*).

² Видети резолуције Уједињених нација 1267 (1999) и 1333 (2000) о оснивању Комитета за санкције Савета безбедности и спровођењу поступка замрзавања имовине лица за које се сумња да финансирају Ал Каиду.

таристичке перцепције државе и идеје друштвеног уговора (Chandler 2009, 126). Када разматрамо тражење одговарајуће равнотеже између појединих људских права, укључујући приватност и анонимност, и интереса националне безбедности, оваплоћене у разнородним инвазивним сигурносним мерама, чини се да се да све три гране власти у многим државама олако дају предност овом другом (Gross 2004, 30–36; Froomkin 2009, 441).

Истовремено, на вредносном нивоу се такође дешава трансформација перцепције анонимности. Иако је у периоду када је интернет тек настајао доживљавана као једна од његових благодети, будући да се сматрало да анонимност ослобађа појединце и подстиче конструктивну јавну дебату, она је временом протерана у сферу илегалног. Посебно је занимљиво то што се, с једне стране, о приватности широко дискутује, док је, с друге стране, анонимност, чини се, постала њена нежељена близнакиња које се родитељи, оличени у државама и корпорацијама, спремно одричу зарад користи које им њен изгон доноси. Тако прогнана, анонимност се све више смешта у сферу тамног, мрачног, тзв. дубоког интернета (eng. *deep internet*).³ То практично значи да је на делу једна врста криминализације анонимности, због чега сваки захтев за анонимном употребом интернета аутоматски изазива подозрење безбедносних служби, а све чешће и самих корисника интернета.

Имајући такве трендове у виду, у раду се бавимо трансформацијом улоге анонимности у информационом друштву из правно-социолошке перспективе са циљем да идентификујемо кључне факторе и актере који подстичу деанонимизацију интернета. Једноставније речено, у анализи која следи покушаћемо да одговоримо на питање коме то и због чега смета анонимни интернет и који су то макро и микро фактори који утичу на то да се анонимност на интернету боји претежно тамним тоновима.

³ Обично се као *deep web* означавају странице које траже претходну пријаву корисника, чиме се обезбеђује додатна анонимност одређених садржаја који се на тој страници налазе. То значи да је приступ тим информацијама условно могућ, али је без пријаве приступ ограничен на мању количину информација или нема. Типични примери су *Facebook* и *JSTOR*. Са друге стране, дарк веб је специфичан по томе што је његовим мрежама (као што су *Tor* [*The Onion Router*], *I2P* [*Invisible Internet Project*] и *Freenet*) могуће приступити искључиво путем посебних претраживача. *Tor* је технологија чија је основна функција обезбеђивање анонимности на интернету ослањањем на слање података путем више сервера и енкрипцију на сваком од њих. Показало се да је користан за скривање идентитета опозиционих онлајн корисника за време Арапског пролећа 2010. године и Сноуденових (*Edward Snowden*) акција 2013. године, али има и широку примену за обављање читавог спектра криминалних активности на црним интернет тржиштима (Knorr 2020, 520; Bernal 2020, 32–35).

У раду заступамо три кључне тезе. Прва, анонимност је градивни елемент који је уграђен у темеље модерних демократских друштава. Друга, анонимност као таква није инхерентно ни добра ни лоша већ зависи од друштвеног контекста у коме се испољава и циљева које себи поставља. Трећа, кључни друштвени актери (*државе, корпорације, медији и корисници интернета*) подстичу гушење анонимности на интернету, а самим тим и у свакодневном животу.

У складу са тим, у раду најпре проблематизујемо сам феномен анонимности, бавећи се њеном улогом у развоју модерних друштава. С једне стране, показаћемо да је анонимност пратилац модернизације савремених друштава, али да она, исто тако, може носити различите изазове по њихову слободу и безбедност. У том смислу овај чланак не пледира да убеди читаоца у безусловно позитивне последице анонимног делања већ да укаже на то да претерано инсистирање на њеним штетним последицама може бити погубно по слободу мишљења и изражавања у демократским друштвима. Пажњу ћемо затим посветити онлајн анонимности и актуелним расправама о домашјима анонимности на интернету, указујући на њене специфичности у односу на традиционално схваћену анонимност. У наставку испитујемо њене друштвено конструктивне, односно позитивне, а потом и негативне учинке. Последње поглавље, пре него што изнесемо наша закључна разматрања, посвећујемо анализи актера и фактора који доводе до протеривања анонимности у сферу интернет подземља (eng. *internet underground*), које се најчешће назива дубоким или мрачним (eng. *dark*) интернетом.

2. ПОЈАМ АНОНИМНОСТИ

Иако је појам анонимности вишезначан те му се може прићи из различитих научних перспектива, његово одређење наизглед не изазива контроверзе. Могуће да због тога нема много радова који се из правне или социолошке перспективе баве феноменом анонимности, посебно домаћих аутора.⁴ Тек је ширењем употребе интернета актуелизовано и питање анонимности, али се аутори ипак далеко мање интересују за ту тему него за тему приватности на интернету.

⁴ Један од ретких текстова објављених у Србији на ову тему, под насловом „Интернет и право на анонимност“, налазимо у зборнику *Слобода изражавања на интернету*, који је уредила Јелена Сурчулија (2010), али и овде је реч о страном аутору Дирку Ворхову (Voorhoof 2010).

У доступној литератури анонимност се најчешће дескриптивно дефинише као немогућност идентификације у одређеном степену или контексту (Wallace 1999, 23). Тако Маркс (Marx 1999, 100–101) истиче да је анонимност један пол на веома широкој скали могућности идентификације која се заснива на седам основних димензија: 1. властито име; 2. адреса; 3. псеудоними који могу бити повезани са нечијим именом или локацијом (рецимо, матични број); 4. псеудоними који могу бити повезани са другим врстама идентификације (на пример, идентификациони број у неком систему); 5. препознавање образаца понашања (рецимо, животни стилови); 6. друштвена категоризација (пол, класа, раса, етницитет итд.) и 7. симболи подобности или неподобности (поседовање одређених знања, артефаката или вештина као извора категоризације). Неколико година касније исти аутор (Marx 2004, 143–144) проширује број димензија на девет, али овога пута их представља путем кључних питања идентификације – о коме је реч, које карактеристике има, где се налази, када је био активан, ко је још повезан, шта користи, шта се десило, у шта верује и које су његове карактеристике.

Слично томе, Вестин (Westin 1967, 39–40), један од утемељивача права на приватност као правне дисциплине, запажа да се анонимност јавља када је појединац у јавном простору или чини дела у јавности, али измиче идентификовању и надзору. Због тога је за осећај анонимности кључно да особа сматра да неће бити идентификована и обавезана да се понаша у складу са важећим друштвеним нормама.

Супстанцијално, анонимност се може одредити као неповезивост нечијих особености у било ком контексту, односно анонимност је стање у којем други нису у могућности да успоставе везу између нечије појавности и његових других карактеристика (Wallace 1999, 24). Другим речима, за разумевање анонимности је кључно да се она одвија у одређеном друштвеном контексту, односно да подразумева одређени друштвени однос. Због тога анонимност није исто што и неименованост, непознатост или изолованост, јер је за анонимност неопходно да постоје актери који неће бити у стању да идентификују особу која је у интеракцији са њима. Сличног мишљења је и Маркс (Marx 1999, 2) који запажа да је, иако то може звучати цинично, анонимност заправо крајње друштвени феномен, будући да без публике она и не постоји.

У одређивању појма анонимности посебно је важно успоставити релацију са приватношћу. Иако су приватност и анонимност блиско повезани концепти, не може се говорити о њиховом потпуном поклапању. Анонимност у одређеној мери и одређеним случајевима обезбеђује приватност, али је свакако не гарантује. Рецимо, када неко присуствује

скупу анонимних алкохоличара у процесу рехабилитације, свакако не ужива приватност. Класичан концепт приватности полази од тога да сваки појединац има право да буде остављен на миру, односно право да контролише приступ у своју приватну сферу, било да говоримо о њеној физичкој или симболичкој демаркацији. Међутим, појавом дигиталних технологија и релативизацијом физичког простора, приватност је постала флуидна, а могућност њеног нарушавања све суптилнија. Управо су дигиталне технологије и одговорне за једну врсту замућивања разлике између анонимности и приватности, чинећи их измешаним и пре свега порозним услед интензивирања употребе технологија надзора. Због тога, Асенбаум (Asenbaum 2018, 461) запажа да разумевање анонимности треба да буде јасно одвојено од концепта приватности јер, у противном, неће бити могуће сагледати њене особености, које су кључне за свако демократско друштво. На том трагу, он сматра да је проблем у томе што највећи број дефиниција анонимности полази од њене субјективне стране. Наиме, анонимност се одређује у односу на то ко врши идентификацију субјекта. На тај начин се она схвата пасивно, као пука негација идентитета, односно степен немогућности да публика утврди идентитет комуникатора, уместо да се она схвата активно, као акција самих комуникатора. То је управо последица мешања пасивног концепта приватности која долази из људскоправашке традиције, као одбране права на приватност. Насупрот томе, Асенбаум се залаже за дефинисање анонимности у традицији јавносферске теорије, попут оне Јиргена Хабермаса, сматрајући да је она инхерентно комуникативна. Анонимност није резултат сакривања већ, управо супротно, показивања, размене мишљења и креирања идентитета. Како истиче Асенбаум, инхерентно ослобађајући ефекат анонимности као последица немогућности идентификације такође је концептуализован као негативна слобода, односно слобода да се буде заштићен од спољне санкције, што је исто последица мешања концепта анонимности са концептом приватности. Међутим, према његовом мишљењу, анонимност треба разумети и као позитивну слободу, слободу изражавања и креирања идентитета, а не као супротност идентитету. Она је предуслов за креирање идентитета, као резултат и негативних и позитивних слобода, односно „анонимност представља контекстом условљено испољавање идентитета тако што се лична осећања изражавају у јавној сфери, уз искључивање појединих аспеката правно утврђене и физички укоренење личности“ (Asenbaum 2018, 462).

Осим у смислу могућности идентификације, анонимност се може сагледавати и у односу на њену сврху, односно циљеве. Тако Валас (Valas 1999, 29) истиче да се она може груписати у три опште категорије:

1. анонимност ради спровођења акције анонимне особе (акциона анонимност);
2. анонимност ради превенције или заштите анонимне особе од акција других (узвратна анонимност) и
3. анонимност ради спровођења процеса (процесна анонимност).

Било који случај анонимности може представљати сваки од тих типова, било одвојено, било заједно, што значи да они нису међусобно искључиви већ је само неки доминантнији од друга два. Такође, овде се анонимност одређује вредносно неутрално, што значи да се не прејудуцира да ли ће се она користити у позитивне или негативне сврхе.

Узимајући речено у обзир, за потребе овог рада анонимност ћемо одредити *интеракиционо* и *дуално*, као анонимност *од* и као анонимност *за*. Другим речима, сматрамо да нема анонимности ван интеракције, као што анонимност може подједнако да буде немогућност идентификације *од* других субјеката и могућност узимања жељеног идентитета *за*-рад остваривања одређених индивидуалних или друштвених циљева.

Стога, анонимност као таква није инхерентно ни добра ни лоша већ зависи од друштвеног контекста у коме се испољава и циљева које себи поставља. Рецимо у контексту затвореног и репресивног друштва анонимност може имати важну сврху у формулисању идеја чији је циљ демократизација друштва, идеја које је због страха од санкција могуће изнети једино анонимно. С друге стране, у отвореним и демократским друштвима, где се мишљења углавном могу неспутано износити, анонимност некада може да уде контрапродуктивна, рецимо, може да подупире популистичке идеје и демагошки дискурс у којем онај који те идеје и дискурс промовише за то не преузима одговорност.⁵ Међутим, као што и, рецимо, технологија, може бити употребљена и у деструктивне сврхе, али то не доводи у питање њену модернизацијску улогу, исто тако и анонимност не може на себе преузети терет узрочника друштвене деструкције. Другим речима, иако она може бити оруђе које се користи за доношење штете другима, њена употреба са тим циљем није производ њених инхерентних особености већ најчешће симптом друштвених поремећаја које узоркују неки шири процеси.

⁵ Рецимо, лажне вести које круже интернетом често заправо пласирају анонимни или псеудонимни извори, посебно стварајући конфузију у време великих друштвених криза, попут пандемије Covid-19.

3. ДЕБАТА О АНОНИМНОСТИ

3.1. Анонимност из правне и друштвене перспективе

У прилог анонимном изражавању могуће је изнети бројне историјске и упоредноправне аргументе. О анонимности можемо говорити у контексту слободe изражавања, као и права на приватност и аутономију личности. Слобода изражавања је неопходан алат грађана који желе активно да учествују у демократском друштву, да се информишу о јавним пословима, споровима и изборима. Добро познати аргумент миловске традиције почива на идеји да је слобода изражавања *conditio sine qua non* откривања истине. Анонимни говор промовише демократско самоуправљање тако што укључује у јавну дебату и оне који се, у супротном, не би чули, нарочито гласове и ставове оних који имају мању моћ и утицај, чинећи тако јавни дискурс, као и систем управљања, демократичнијим. Можемо очекивати и креативнија решења друштвених проблема ако се могу чути и неконвенционални предлози. Специјални извештај Уједињених нација за промоцију и заштиту права на слободу мишљења и изражавања (La Rue 2013, pag. 49) веома јасно указује на везу између анонимности и ефективне слободe изражавања: „Ограничавање анонимности има одвраћајуће дејство (eng. *chilling effect*), обесхрабрује слободу изражавања информација и идеја. Оно, такође, може изазвати искључивање појединаца из виталних друштвених сфера, подривајући њихова права на изражавање и информацију, повећавајући друштвене неједнакости. Поред тога, ограничавање анонимности омогућава сакупљање и складиштење велике количине података од стране приватног сектора, чиме се значајно подиже ниво оптерећења и одговорности корпорација у погледу заштите приватности и безбедности таквих података.“

Анонимни говор доприноси аутономији и самоостварењу личности, тако што пружа могућност лицу да истражује нове идеје, начине изражавања, па чак и нове идентитете (Lidsky, Cotter 2007, 1568–1569). Вестин (Westin 1967, 39–40) сматра да стање анонимности особи пружа могућност да се слободније изрази јер зна да се странац неће задржавати у његовом животу нити на њега може да врши неки утицај („феномен странца“). Нас, у ствари, зарад очувања бројних људских права, заиста интересују наша видљивост и изложеност онима који не одобравају како се изражавамо и делујемо (Cohen 2008, 190). Многи људи не би изнели своје ставове, не би се одлучили на узбуњивање, не би оспоравали уврежена мишљења или се конфронтирали представницима власти уколико нису у прилици да остану анонимни. Грађани би се теже прикључивали контраверзним организацијама, као што би

се устрчавали да дискутују о осетљивим темама (Strossen 2001, 2106). Историја обилује примерима да су људи и организације који су били критични према државним властима или другим моћним лицима и организацијама доживљавали драконске санкције, били лишавани живота, слободе, имовине и слично. Одличан пример су бројна анонимна филозофска дела која су током историје оспоравала религијске догме. Анонимно писање има дугу традицију и важну улогу у изражавању идеја. У Енглеској су анонимно писали Дефо (*Daniel Defoe*), Свифт (*Jonathan Swift*), у Француској Волтер, док су у Сједињеним Америчким Државама (САД) чак и Федералистички списи Хамилтона (*Alexander Hamilton*), Медисона (*James Madison*) и Џеја (*John Jay*) оригинално били објављени под псеудонимом *Publius*, као писма уреднику. Чак је и председник Врховног суда Маршал (*Chief Justice John Marshall*) под псеудонимом *Пријатељ Републике* бранио у јавности поједине одлуке Врховног суда САД. Постоје докази да су многи амерички председници и конгресмени објављивали своје политичке радове непотписани или под псеудонимом (Note 1961, 1085). Посебан и разумљив мотив да буду анонимни имали су аутори чија су дела оспоравала политички *status quo*, економске услове рада, друштвене норме и слично. Томас Пејн (*Thomas Paine*) је 1776. године објавио утицајни памфлет „*Common Sense*“ у прилог независности од Велике Британије под псеудонимом *An Englishman* (Heins 2010, 66). Та дела су имала непроцењив значај за демократизацију и конституционализацију САД, али и шире.

Анонимност је касније играла значајну улогу у борби за друге циљеве, пре свега за грађанска права и права жена, док је данас важан штит за политичке дисиденте. Као што ће се видети у расправи која следи, могућност анонимног деловања на интернету посебно је данас важан сегмент политичке борбе у многим аутократским друштвима.

Ипак, право на анонимност није као такво прихваћено у уставима већине држава света (Cobb 2007, Martin, Fargo 2015). Не налазимо такву гаранцију ни у Уставу Републике Србије. Необично је што се у нашем Уставу не наводи изричито ни право на поштовање приватности, али је право на поштовање приватног и породичног живота гарантовано у чл. 8 Европске конвенције о људским правима и основним слободама, која је саставни део правног поретка Републике Србије. Осим тога, према ставу Уставног суда РС, право на приватност је саставни део уставног права на достојанство и слободан развој личности, гарантованих чл. 23 Устава.⁶

⁶ Уставни суд Републике Србије, Одлука о уставној жалби подносиоца Х, Уж-3238/2011, 8. март 2012.

У упоредном уставном праву анонимност ужива одређен степен заштите као елемент других права и слобода, пре свега слободе изражавања и права на приватност, као и слободе уопште. Приметан је тренд да се право на анонимност сужава, с обзиром на то да интереси сигурности и националне безбедности у конкретним случајевима односе превагу над анонимношћу. За то питање важна је и улога компанија које пружају услуге телекомуникација. У овој сфери се поклапају интереси државног и приватног сектора, па су законска решења усмерена на обезбеђивање услова да се по потреби може утврдити идентитет интернет корисника. Од интернет провајдера се тражи да сакупљају и чувају податке неопходне за идентификовање корисника, а у појединим државама власти имају право да добију те податке без судског одобрења или надзора (Кер).

У компаративном прегледу значајни су нам нормативни оквири и судска пракса европских држава и САД. У Европи је приметно тражење компромиса између потребе делотворне примене закона и поштовања људских права гарантованих, *inter alia*, Европском конвенцијом о заштити људских права и основних слобода (1950)⁷ и Међународним пактом о грађанским и политичким правима (1966).⁸ Државама потписницама је наложено да је неопходно обезбедити право свакога да на мишљење, примање и саопштавање идеја без мешања јавне власти и без обзира на границе. Важно је, такође, обезбедити и право на приватност. Та права и слободе, који су повезани са анонимношћу као гарантом ефективности, морају бити примарни, а могу бити ограничена када за то постоје законска основа, легитимни циљеви и одговарајућа мера пропорционалности између инвазивности мера ограничења и циљева којима се тежи.⁹

У Ирској се тренутно води врло интересантан судски поступак са потенцијално веома значајним последицама у области заштите права на анонимност на интернету. Једна школа је од компаније Фејсбук затражила да открије идентитет корисника Инстаграм налога, а судија Високог суда Ирске обратио се Суду правде Европске уније тражећи одлуку о претходном питању, у складу са чл. 267

⁷ *Службени лист СЦГ – Међународни уговори* 9/2003, 5/2005, 7/2005 – испр. и *Службени гласник РС – Међународни уговори* 12/2010 и 10/2015.

⁸ *Службени гласник СФРЈ* 7/1971–73

⁹ Упореди са преамбулом и чл. 15 Конвенције Савета Европе о високотехнолошком криминалу (тзв. Будимпештанска конвенција о високотехнолошком криминалу), *Службени гласник РС* 19/2009, која је ступила на снагу 1. јула 2004. године.

Уговора о функционисању Европске уније.¹⁰ Од Суда се очекује да одговори на питање да ли права на приватност, заштиту података и слободу изражавања гарантованих Повељом о људским правима Европске уније (Европска повеља) подразумевају и право да се на интернет анонимно постављају садржаји, под условом да нису противни јавном поретку. Од Суда се захтева и став о условима под којима се, у складу са *GDPR* и Европском повељом, компаније које воде платформе за друштвено умрежавање могу принудити да разоткрију идентитет иначе анонимних корисника.¹¹

У САД постоји јасна линија прецедената којима је утврђено да Први амандман¹² штити право на анонимност, укључујући и сферу интернета. Гарантује се право да се говори и пише анонимно, као и да се анонимно учествује у групним активностима. Врховни суд САД је то право развио као дериват заштите слободе говора, окупљања, штампе, религије и петиције (Note 1961, 1084). Сасвим је логично да судска тумачења права на приватност или анонимност, која нису изричито гарантована Уставом САД, изазивају више контроверзи и противљења политичких грана власти и дела јавног мњења него што је то случај са у Уставу изричито набројаним правима, на пример слободом штампе или религије (Heins 2010, 56). У случају *NAACP v. Alabama* Врховни суд САД је сматрао да би обавеза откривања чланства удружења подрила то удружење јер би чланови били подложни економској одмазди, отказима, физичким претњама и другим актима нетрпељивости и насиља.¹³ Врховни суд је две године касније проширио право на анонимно удруживање оборивши локалну регулативу која је добротворним организацијама налагала да предају спискове својих чланова као услов за пореске олакшице.¹⁴ Исте године је Врховни суд био суочен са питањем да ли Први амандман штити и право да се говори анонимно. Наиме, суд је оборио калифорнијски закон који је забрањивао анонимне памфлете. У свом образложењу Суд је навео да су анонимни памфлети, брошуре и књиге

¹⁰ [Eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT](http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT), последњи приступ 30. августа 2021.

¹¹ GDPRhub. The High Court – 2021 IЕHC 287. 2021. https://gdprhub.eu/index.php?title=The_High_Court_-_2021_IЕHC_287, последњи приступ 30. августа 2021. године.

¹² „Конгрес не може да доноси никакав закон о установљењу државне религије, као ни закон који забрањује слободно исповедање вере, а ни закон који ограничава слободу говора или штампе или право народа на мирне зборове и на упућивање петиције влади за исправљање неправди.“

¹³ *NAACP v. Alabama*, 357 U.S. 449 (1958) at 463

¹⁴ *Bates v. Little Rock*, 361 U.S. 516 (1960)

играли важну улогу у прогресу човечанства, тако што су прогоњене групе биле у могућности да критикују опресивне праксе и законе или анонимно или никако.¹⁵ У непосредном контексту интернета амерички судови такође препознају да способност да се слободно говори у великој мери зависи од анонимности. Примера ради, Врховни суд Њу Џерсија је сматрао да анонимни онлајн говорник ужива заштиту Првог амандмана да остане неидентификован.¹⁶

Насупрот изреченом, иако је, дакле, јасан допринос анонимног изражавања квалитету и квантитету идеја које се нуде у јавном простору, очигледно је и да се анонимност може злоупотребити да се другоме нанесе озбиљна штета. Лице може пожелети да се заштити анонимношћу уколико износи неистину. Под велом анонимности могу се клеветати, вређати, узнемиравати или повређивати нечија својинска и ауторска права. Посебан проблем је злоупотреба анонимности са циљем угрожавања правног поретка и националне безбедности. Као што слобода изражавања може бити ограничена „ако је то неопходно ради заштите права и угледа других, чувања ауторитета и непристрасности суда и заштите јавног здравља, морала, демократског друштва и националне безбедности Републике Србије“ (Устав РС, чл. 46, ст. 2), тако је рационално очекивати да ни анонимност не може нити треба да ужива апсолутну заштиту. У том смислу је илустративан пример случаја у коме Врховни суд САД 2010. године није заштитио право да се потпише референдумска иницијатива без могућности да потписи иницијатора буду обнародовани.¹⁷ У држави Вашингтон дозвољено је оспорити закон на референдуму уколико 4% гласача потпише петицију. Потписник мора да остави име и адресу. Према Закону о јавним исправама, свако лице има право на препис или копију тих података да би могло да утврди да ли су потписи валидни. Потписници иницијативе за референдумски опозив закона су противници истополних бракова и због свог потписа су били малтретирани, али тај третман није био довољно високог интензитета да би убедио суд да њихове идентитете треба заштитити од јавности. Одређене интересне групе већ деценијама заговарају идеју да би америчка влада требало да надзире активност на интернету на начин на који то чини са радио и телевизијским програмом, али FCC (*Federal Communications Commission*)

¹⁵ *Talley v. California*, 362 U.S. 60 (1960)

¹⁶ *Dentrite International v. Doe No. 3*, 342 N.J. Super. 134 (App. Div. 2001). У овој пресуди је као прецедент цитирана *Talley v. California* у делу о значају анонимности.

¹⁷ *Doe v. Reed*, 561 U.S. 186 (2010).

има врло уску надлежност над интернетом. У литератури се среће и став да из перспективе публице анонимни говор има мању вредност јер адресант поруке њу не може адекватно да протумачи ако не зна ко је аутор (Lidsky, Cotter 2007, 1539).

С друге стране, из перспективе друштвене теорије на феномен анонимности међу првима су указали социолози који су се бавили развојем модерног начина живота у урбаном окружењу. Иако неки од њих, попут Зимела, не заузимају *a priori* негативан став већ анонимности прилазе као неизбежној, па чак и ослобађајућој карактеристици урбаног наспрот руралном животу (Simmel 2012), ипак код многих класичних социолога попут Тениса или Вирта доминира негативна перспектива анонимности (Вујовић 1988, 32–37).

У нешто савременијим социолошким радовима далеко више се расправља о штетним аспектима индивидуализма (Бауман, Гиденс, Бек) него што се фокус усмерава на саму анонимност. Међутим, и у том контексту, понекад се отвара слично питање које се отвара и у односу на последице процеса индивидуализације, односно у којој мери појединац треба да буде подређен заједници. У том смислу Тејлор (Taylor 1991, 9) прву nelaгодност и разлог за бригу налази у индивидуализму, као фокусираности на себе и изостанку бриге за друге и друштво, где се инсистирање на анонимности сматра погрешним јер се њиме нарушава одговарајућа равнотежа између интереса друштва и анонимности и аутономије појединца. Такође, постоје чак и тврдње да је приватност превазиђена, непотребна, па чак и штетна, и да треба да прихватимо потпуну отвореност и изложеност јер „ако ниси ништа скривио, немаш се чега ни бојати“ (Brin 1998).

3.2. *Pro et contra* анонимности на интернету

Оно што важи за анонимно изражавање уопште примењиво је и на анонимност на интернету. Перспективе су различите и супротстављене. Управо зато тај феномен и изазива контроверзе и представља подлогу за бројне злоупотребе основних људских права и слобода. Као двосекли мач, анонимност на интернету може помоћи узбуњивачима да остану слободни, посебно у аутократским друштвима, али исто тако може помоћи делинквентима да избегну казну (Sarda *et al.* 2019, 561).

Најнепосреднија корисност анонимности на интернету види се у њеном доприносу развоју јавног дискурса подршком слободи говора и уопште изражавања (Akdeniz 2002, 224). Развој интернет сервиса и

апликација који кориснику пружају слободу стварања онлајн садржаја револуционисао је границе говора на начин да сваки корисник може брзо, лако и без значајних трошкова да допре до својих адресата на глобалном нивоу. То је феномен који Мануел Кастелс (2014) назива масовна самокомуникација и дефинише је као нови образац масовне комуникације који се заснива на високој аутономности будући да је она самопроизведена, самоусмерена и самоодабрана.

Жардин (Jardine 2018) истиче да се, у контексту (не)демократичности политичких система, мотиви за интернет анонимност могу широко груписати у две категорије: мотиви који су повезани са могућностима које анонимност пружа и мотиви који се тичу непосредних политичких потреба. Ови први су највише заступљени у веома отвореним и либералним политичким уређењима, док су мотиви који проистичу из политичких потреба најчешћи у ауторитарним режимима. Другим речима, у отвореним друштвима су могућности за анонимну употребу интернета, рецимо путем *Tor* претраживача, широко доступне, али не представљају производ нужде већ су исход личних афинитета појединаца. С друге стране, у аутократским режимима су могућности за онлајн анонимност веома сужене јер се државе активно труде да сузбију употребу технологија анонимности. Због тога, активисти који користе интернет као своје поље говора све чешће бивају прогоњени, хапшени и осуђивани на строге казне због својих активности, било да је реч о изборима у Зимбабвеу или Белорусији, политичким приликама у Тајвану, Египту или Хонг Конгу.

О махом позитивним ефектима онлајн анонимности на политичку партиципацију говоре различити аутори (Akdeniz 2002; Cooper 2020; Papacharissi 2004), као што то показују и нека истраживања (Perbawani, Rahayu, Anshari 2018, 208). Политички активни грађани често користе анонимност као ефикасно средство за избегавање правних или друштвених последица за изнесене ставове, док анонимност на друштвеним медијима може допринети порасту политичке партиципације. Иако, наравно, како истиче Папакариси (Papacharissi 2004, 267), анонимност може олакшати говор мржње, она је исто тако благотворна за слободну размену мисли и комуникацију ослобођену ограничења физичког света.

Управо на том трагу можемо поменути још један важан аспект анонимне употребе интернета који се тиче превазилажења структуралних ограничења која детерминишу интеракцију у реалном свету. Поље доступних интеракција је на интернету далеко шире него у реалном окружењу где је комуникације ограничена и микролокацијом појединаца и његовом структуралном позицијом у друштву (Петровић

2013, 170). За разлику од комуникације у свакодневном, физичком окружењу, комуникација на интернету се одвија у далеко лабавијим структуралним оквирима где је практично једина структура коју је немогуће неутралисати повезана са културом, односно језиком којим се комуницира. Наравно, постоје и рестрикције које намећу пре свега ауторитарне државе, а које се односе на техничку (не)могућност да се неким просторима на интернету уопште приступи, као што је немогућност да из Кине или Русије користите Фејсбук и неке друге дигиталне платформе.

С друге стране, они који страхују од анонимности на интернету указују на штету која може произаћи из ситуација када злонамерна лица под плаштом анонимности и без страха од одговорности шире лажи и друге штетне садржаје или масовно крше ауторска права. Нове информационе технологије су, попут Платоновог прстена моћи,¹⁸ у одређеној мери отежале правну заштиту лица и имовине од превараната, клеветника, насилника или терориста. Рецимо, анонимност и енкрипција су један од основних, али и кључних алата редовне комуникације терористичких организација (Lewis 2005, 112).

Анонимност на интернету пружа могућност да се без одговорности према бројној публици одашиљу садржаји попут говора мржње или дезинформација које могу имати веома штетне последице. Деловање противника вакцинације у доба пандемије ковида 19 можда је и онајбољи пример за то. Шулер (Suler 2004, 321–322), који је се бавио узроцима насилне комуникације на интернету, тврди да је онлајн анонимност један од кључних фактора који ствара тзв. ефекат онлајн дезинхибираности. Тај ефекат се, према мишљењу тог аутора, односи на стање у коме људи, под дејством различитих фактора у комуникацији на интернету говоре или чине ствари које иначе, у регуларној офлајн комуникацији, не би говорили или чинили. Реч је о читавом спектру понашања на интернету који се креће од бенигне дезинхибираности, кад су људи отворенији и искренији него у реалности, до токсичне дезинхибираности, када се људи понашају неупоредиво лошије у односу на своје свакодневно понашање у реалности.

¹⁸ Платон у *Држави II* приповеда о лидијском пастиру Гигу који проналази прстен моћи који носиоца може учинити невидљивим. Овај то користи да се убаца у дворац и почини бројна недела, а на крају убија краља и преузима краљевство. „Нема човека који би се уздржао да не узме туђе, ако би могао неопажен да узме нешто са тржнице; или би ишао по кућама и легао са ким жели по свом нахођењу; убијао би, или ослобађао из затвора кога пожели, и у сваком погледу био попут бога међу људима“ (Платон 1993, 359–360).

4. РАЗУМЕВАЊЕ АНОНИМНОСТИ НА ИНТЕРНЕТУ

4.1. Специфичности онлајн анонимности

Чини се да је питање анонимности добило значај тек са појавом интернета. Могућност да се на мрежи буде неко други већ од њених првих дана инспирисало је многе и на озбиљне дебате (Turkle 1995) и на шаљиве опсервације на ову тему.¹⁹ Технооптимисти су били уверени да ће јавна сфера на интернету која је ослобођена расних, верских, етничких, социоекономски или родних обележја идентитета дати кључни допринос демократизацији друштва (Akdeniz 2002; Papacharissi 2004), па чак и да ће помоћи да се поново успостави давно изгубљени дух заједнице (Rheingold 2000).

Све до појаве платформи за друштвено умрежавање, попут Фејсбука, дакле негде до средине двехиљадитих, анонимна комуникација на интернету је пре била стандард него изузетак, док се изношење личних података на мрежу сматрало крајње необичним, па и непожељним (Петровић 2008, 104–106). Ипак, појавом платформи за друштвено умрежавање анонимност све више уступа место јавном идентификовању, било да је реч о добровољној или изнуђеној идентификацији корисника интернета, да бисмо данас дошли у ситуацију да је готово потпуно сузбијена могућност анонимне комуникације на интернету.

Међутим, пре него што дубље уђемо у дебату о консеквенцама онлајн анонимности, треба успоставити везу између офлајн и онлајн анонимности. Наиме, за разлику од анонимности у физичком окружењу, анонимност на интернету се не може поистоветити са непостојањем идентитета јер, како запажа Ворхов, повезивање на интернет, односно учествовање у комуникацији путем интернета, неизбежно подразумева неку врсту самоидентификације (Voorhoof 2010, 76). Због тога неки аутори сматрају да би, уместо анонимности, исправније било говорити о псеудонимности, односно о онлајн идентитету који није непосредно повезан са офлајн идентитетом (Froomkin 1999, 114). Ствари додатно компликује могућност постојања вишеструких онлајн идентитета и истог онлајн идентитета који дели више лица (рецимо у онлајн друштвеним покретима). Осим тога, важно је напоменути: да бисмо уопште могли говорити о анонимности на интернету, неопходно је да

¹⁹ Чувена је карикатура Питера Стајнера (*Peter Steiner*), која се 1993. године појавила у магазину *Њујоркер* (*The New Yorker magazine*), на којој су приказана два пса од којих је један за рачунаром и обраћа се другом псу речима: „На интернету нико не зна да си пас.“

кумулятивно буду остварена два услова: 1. да одређену онлајн анонимну акцију није могуће повезати са реалним идентитетом актера и 2. да две анонимне акције које је учинио исти актер није могуће повезати једну са другом (Clark, Gauvain, Adams 2009, 400). Уколико је испуњен само први услов, реч је о псеудонимности.

Даље, важно је разликовати јаку и слабу анонимност на интернету. Слаба анонимност је само привид анонимности, док јака анонимност значи да трагови активности на интернету не могу или врло тешко могу бити повезани са особом у реалном свету. Рецимо, јака анонимност је нужна узбуњивачима или дисидентима који се боре против репресивног режима, али њој прибегавају и они који се баве полулегалним или илегалним активностима на интернету. Просечан корисник интернета, који је по правилу на ниском нивоу дигиталне писмености, тешко може одмаћи даље од слабе анонимности. Занимљиво је то што се чини да већина њих и нема потребу да сакрије свој идентитет на интернету нити мисли да је то претерано важно (Electronic Frontier Foundation 2015, 3–6).

У онлајн простору важно је одредити и шта се сматра идентитетом актера. Посредством „колачића“ могуће је утврдити IP адресу уређаја са кога је послата нека порука, али то не значи аутоматски да поуздано можемо знати ко је аутор поруке, односно актер. Ситуација постаје значајно компликованија ако се користе мреже анонимности, у којима се помоћу више прокси-сервера сакрива изворни пошиљалац поруке. Чак и ако би постојале технолошке претпоставке да се идентификују сви у ланцу слања поруке, све до оригиналног пошиљалаца, остаје велики политички проблем да би правне норме и технологија могли бити злоупотребљени у недемократске сврхе (Clark, Gauvain, Adams 2009, 402–405). Очигледно је да ће увек постојати притисак истражних органа да зарад ефикасне и ефективне кривичне истраге сужавају простор анонимности, што представља својеврстан опортунитетни трошак на страни заштите анонимности узбуњивача, дисидената и других лица којима би идентификација угрозила живот, сигурност или нека друга права.

4.2. Прилог разумевању деанонимизације интернета

Чини се да се у протеклих десетак година оснажила једна врста кампање против анонимности на интернету. Стиче се утисак да је на делу један вид криминализације анонимности који практично доводи до тога да сваки захтев за анонимном употребом интернета аутоматски

изазива подозрење не само безбедносних служби већ све чешће и самих корисника интернета. Плански или не, анонимност се све више гура у сферу мрачног интернета, чија је негативна слика пре свега производ оних који креирају слику јавног мњења. Једно истраживање које је спроведено у Великој Британији показује да се у више од 800 чланака о мрачном интернету, који су у периоду 2001–2017. објављени у листовима *Daily Mail*, *Daily Mirror*, *Daily Telegraph*, *The Guardian*, *The Sun* и *The Times*, он представља у изразито негативном светлу, при чему се истиче да је анонимност једна од његових главних карактеристика и да је она повезана са криминалним и антисоцијалним активностима (Sarda et al. 2019, 562).

4.2.1. Кључни актери који подстичу деанонимизацију интернета

Основно питање на које овде желимо да одговоримо јесте коме то смета анонимни интернет и због чега се он боји претежно тамним тоновима. Као кључне актере који из различитих мотива сузбијају анонимност на интернету за потребе ове анализе идентификујемо: државе, корпорације, мејнстрим медије и саме кориснике интернета. Не треба изоставити ни саме *дигиталне технологије* које су основно средство за деанонимизацију њихових корисника. Иако се на овом месту нећемо детаљно бавити улогом технологије као једног од актера деанонимизације интернета, у филозофским студијама о технологији отворено је питање да ли технологије, осим функционалне, поседују и инхерентну моралну вредност и да ли таква вредност може бити намерно усађена у техничке системе (Feenberg, 1999). С једне стране, постоје тврдње о вредносној неутралности технологије које не искључују могућност да она има значајан утицај на друштвене, моралне и политичке аспекте живота, али негирају да су негативне или позитивне последице тог утицаја функција тог система. Наиме, према том виђењу, технологија може бити само инструмент људске намере, а моралност и политика су инхерентни људима, а не њиховим алатима. Том ставу се супротставља тврдња да су поједине технологије у непосредној корелацији са конкретним друштвеним, етичким и политичким вредностима (Flanagan, Howe and Nissenbaum 2008, 347–348). У том смислу, у већину дигиталних производа и услуга унапред је уграђена могућност надзора потрошача, дакле то постаје њихова примарна сврха (Зубоф 2020), док су, с друге стране, алати као што су *Tor* и *Signal* дизајнирани управо ради обезбеђивања приватности и анонимности и помажу да се те вредности усаде и распрострање (Coleman 2019, 570).

Сматрамо да је најплодније виђење Ендрјуа Финберга (Feenberg 2000, 228), који технологију види као двострани феномен – с једне стране, она је оператор, док је, с друге стране, она објект. Дакле, технологија није само ефикасна справа или ефикасан поступак већ она у себи садржи и различите друштвене (економске, политичке, културне) контексте који су укорењени у њеном дизајну. У том смислу дигиталне технологије данас треба гледати као поприште борбе различитих и супротстављених интереса кључних актера. Неки од тих актера, о којима ће бити речи у наставку, имају интерес да се дигиталне технологије развијају тако да све више сужавају могућност њихове анонимне употребе, док су с друге стране актери који инсистирају на уграђеним опцијама за анонимност (попут различитих организација), али и они који самостално развијају алтернативне технологије, попут поменутог Тора или Сигнала. *Државе су*, наравно, један од кључних актера од којег треба поћи у анализи притисака који воде деанонимизацији интернета. У том контексту не може се на исти начин говорити о ауторитарним државама и онима које имају дугу демократску традицију. Међутим, било да говоримо о једнима или другима, извесно је да је у корену сваке државне власти тежња да се контролишу доминантни дискурси у јавној сфери. На то су указивали многи аутори, као што су Грамши (2018), Фуко (1997), Кастелс (2014). То колико ће се одређено друштво одупрети тим импулсима државе зависи од бројних фактора попут демократске традиције, снаге институција, политичке културе и политичког система појединих држава. Рецимо, ако говоримо о САД, ту је, као што смо истакли у претходној расправи, право на анонимност загарантовано Првим амандманом њиховог Устава, док је Четвртим амандманом загарантовано право да се надзор врши под јасно дефинисаним околностима. Међутим, Сноуденова (*Edward Snowden*) открића показала су да, када је реч о корисницима интернета, државне агенције које се баве надзором имају склоност да заобиђу то уставно право и да сваког, било да постоји правни основ или не, подвргну надзору (Coleman 2019, 569). У земљама као што је Кина тај надзор је далеко директнији и отворенији, а закони којима се та област уређује ретки су и лако их је заобићи (Fry 2015, 499).

Прилично је јасно зашто *корпорацијама* анонимност на интернету није у интересу. Било која активност које се одвија онлајн, од куће или са мобилног уређаја, прати се, депонује, купује и продаје међу технолошким џиновима као што су Гугл (*Google*), Фејсбук (*Facebook*) и Мајкрософт (*Microsoft*), а постоје и стотине мање познатих трговаца информацијама који помажу оглашивачима да изграде застрашујуће детаљне дигиталне профиле корисника тако што прикупљају податке из различитих извора, укључујући и базе података разних онлајн плат-

форми (Moore 2010, 1). Можда је понајбоље о томе писала Зубоф (2019, 261) образлажући како, пре свега, интернет компаније, а заваљујући трговини са њима и све остале компаније, зарађују огроман новац управо на основу могућности идентификовања основних карактеристика, жеља и потреба корисника интернета. Имајући то у виду, потпуно је разумљиво због чега Фејсбук инсистира на тзв. политици стварних имена (енг. *real name policy*) коју је та компанија увела још 2015. године (Haimson, Hoffmann 2016). У прилог томе говори и изјава коју је у то време дала сестра оснивача Фејсбука Ренди Закерберг (*Randi Zuckerberg*), директор маркетинга у компанији, која се јасно сложила за протеривање анонимности са мрежа, образлажући то тврдњом да се људи понашају много боље када користе своја стварна имена (Witzleb *et al.* 2014, 296). Ипак, тај удар на анонимност изазвао је револт великог броја корисника, посебно у групацији сексуалних мањина (LGBTQIA), који су то окарактерисали као непоштовање основних људских права (Haimson, Hoffmann 2016). Иако су у наредним годинама били присиљени да одустану од круте политике стварних имена, Фејсбук ниједног тренутка није одустао од своје намере да највећи број својих корисника, на овај или онај начин, идентификује.

Традиционални медији, као трећи актер деанонимизације интернета, у њему су, од његових самих почетака, видели ривала кога је ваљало зауздати будући да је врло брзо постало јасно да ће интернет угрозити традиционалне медије као основно средство информисања. Два су основна начина на које традиционални медији подривају анонимност на интернету – директно и индиректно. С једне стране, они инсистирају на својој кредибилности тако што руше кредибилитет извора на интернету који су често управо анонимни, односно непроверљиви. Посебно је у том смислу изражена кампања чији је циљ феномен тзв. лажних вести на интернету (*fake news*). Иако су многа истраживања показала да је грађанско новинарство све важнији сегмент информисања (Радојковић 2015), традиционални медији су упорни у томе да уруше веродостојност интернета као извора информисања, инсистирајући на томе да је он извор лажних вести, а као један од кључних узрока њиховог пласирања истиче се непостојање јасног идентитета оних који те вести креирају и пласирају (Wang, Pang, Pavlou 2018, 1; Радојковић 2015, 309). С друге стране, индиректно подривање анонимности на интернету последица је сензационалистичког извештавања, у којем се инсистира на његовим негативним аспектима, што смо могли видети на примеру извештавања британских медија о дарк вебу. Уопште узев, медији су презасићени текстовима у којима се указује на опасности које вребају на интернету, а често се као главни протагонисти нелегалних

радњи истичу непознати људи на интернету које корисници неопрезно додају за пријатеље или улазе у некакве приватне или пословне аранжмане са њима.

И сами *корисници* интернета својим деловањем често подстичу онлајн деанонимизацију. Ако се још и може рећи да Фејсбукова политика стварних имена на неки начин присиљава кориснике да се идентификују, поставља се питање зашто би то корисници радили на Твитеру, који нема такву политику. Наиме, једно истраживање о Твитеру (Peddinti, Ross, Capros 2017, 84–87) показује да већина корисника, иако није на то приморана, има профиле које је лако повезати са њиховим стварним идентитетима (рецимо, највећи број користи своја права имена и презимена). Дакле, политике идентификације корисника дигиталних платформи нам не могу послужити као једино објашњење за широко распрострањену праксу јавног огољавања сопствене интиме на тим платформама. Према нашем суду, потреба за неанонимизованим, односно јавним деловањем на интернету делом је последица: 1. макрофактора – односно тежње људи да унесу ред у своје окружење у контексту живота у ризичном друштву и 2. микрофактора – односно потребе да се контекстуализује интерперсонална интеракција на интернету.

4.2.2. Микро и макро фактори који подстичу деанонимизацију интернета

Када је реч о макрофакторима, притисци за деанонимизацију коју сами корисници интернета врше једни на друге део су њихове имплицитне стратегије за контролisaње друштвених ризика са којима се сусрећу. На експанзију ризичног друштва указао је још Урлих Бек (Бек, 2001) средином осамдесетих година XX века, тврдећи да се савремено друштво креће ка стању перманентних ризика којима су појединци све изложенији (од могућности да изгубе посао до могућности да се разболе од загађења или настрадају у терористичком нападу). Појачавање ризика последица је радикализације модернизације у другој половини XX века, односно индивидуализацијских процеса захваљујући којима се појединци искорењују из укоренењујућих структура индустријског друштва, попут нације, класе, вере, и бивају све више препуштени сопственом менаџменту контролisaња ризика који их окружују. Међутим, препуштеност самима себи код великог броја појединаца изазива стање перманентне анксиозности, која их нагони да се врате укоренењујућим силама предмодерног друштва, које су често оличене и трибалистичким моделима заједништва (Maffesoli 1996), где се сви чланови племена добро познају и као такви сви су изложени суду јавности. Те

трибалистичке тенденције се најбоље виде у ехо коморама које се образују на интернету, односно групацијама истомишљеника који се све више удаљавају једни од других (Flaxman, Sharad, Rao 2016). Сви ти процеси снажно утичу на појединца да се на мрежама деанонимизује јер свако ко је анониман може бити потенцијални уништитељ заједнице.

На микронивоу, у контексту одвијања интерперосналне интеракције, комуникаторима је важно да онога са којим ступају у интеракцију могу да сместе у неки социокултурни и географски контекст, што је у онлајн комуникацији често немогуће (Cushman, Sahn 1985, 49–50). Због тога, а опет у контексту поменутих ризика, расту притисци да се људи са којима се ступа у контакт на интернету самоидентификују не би ли се тако предупредили могући нежељени исходи интеракције на интернету.

4.2.3. Отпори деанонимизацији интернета

Насупрот актерима који врше притисак да се интернет деанонимизује стоје актери који имају њима супротстављење интересе. Као кључне можемо да издвојимо различита професионална и удружења грађана, независна регулаторна тела и различите владине и невладине међународне организације које активно раде на одбрани права на анонимну употребу дигиталних технологија. Посебно у академској заједници и међу организацијама цивилног друштва данас постоји страх да регулаторни одговор на реалне или замишљене претње по јавну безбедност и националну сигурност суштински угрожавају нашу посвећеност аутономији личности, приватности, једнакости, слободи изражавања, кретања или удруживања (Coleman 2019, 569).

Осим колективних актера, постоје и индивидуални актери, попут независних новинара, активиста, узбуњивача или хакера, који у сарадњи или независно трагају за практичним решењима за проблем надзора, испут стварајући и услове за анонимно деловање и осигурање приватности.

Нарочито су значајна настојања Савета Европе да се омогући заштита људских права и поштовање владавине права у информационом друштву. Сходно препорукама те међународне организације, јавне политике држава чланица морају бити усмерене на очување и проширење заштите, а нарочито се мора водити рачуна о праву на приватност живота и кореспонденције приликом коришћења интернета и других информационо-комуникационих технологија, укључујући и право корисника да

не откривају свој идентитет.²⁰ Такође, Савет Европе инсистира на томе да је слобода изражавања и информисања једнака на интернету као на осталим форумима и подразумева да свако има право да себе изрази и буде прималац информација онлајн. У то спадају, *inter alia*, политички говор, религијски погледи, мишљења и ставови који могу да увреде, шокирају или узнемире друге.²¹ То, ипак, не значи да се не узимају у обзир репутација и приватност других, па се тако може ограничити изражавање којим се изазивају дискриминација, мржња и насиље. Та ограничења, према распрострањеној јуриспруденцији Европског суда за људска права, морају бити предвиђена законом, уско скројена и под надзором судова. Не смеју бити арбитрерна, а морају имати легитиман циљ, као што су национална безбедност, територијални интегритет и јавна безбедност, спречавање нереда или криминала, заштита здравља или морала, или заштита права и слобода других.²²

Коришћење профила под псеудонимом представља и прилику и изазов за људска права, па Савет Европе препоручује да државе чланице сарађују са приватним сектором и грађанским друштвом са циљем унапређења права на слободу изражавања корисника на интернету. Један од важних аспеката те иницијативе јесте потреба да корисници имају пуну информацију о својим изборима у погледу онлајн идентитета. Тај став је јасно исказан у 7. принципу Декларације о слободи комуникације на интернету: „У циљу обезбеђивања заштите од онлајн надзора и јачања слободе изражавања информација и идеја државе чланице треба да поштују вољу корисника интернета да се не објави њихов идентитет. То не спречава државе чланице да предузимају мере и сарађују да би откриле лица одговорна за кривична дела...“²³ Право да се користи псеудоним на интернету заслужује заштиту, и из угла слободе изражавања и права да се примају информације и из угла права на приватност. Савет Европе је свестан и потребе за темељном заштитом узбуњивача. У новом медијском амбијенту заштита идентитета извора информација мора се проширити и на кориснике онлајн платформи

²⁰ Council of Europe, Recommendation CM/Rec (2007)16 of the Committee of Ministers to member states on measures to promote the public service value of the Internet, Strasbourg 2016.

²¹ Види случај *Handyside v. The United Kingdom*, 5493/72, Свет Европе, Европски суд за људска права, пар. 49.

²² Упореди чл. 10, став 2 Европске конвенције за заштиту људских права и основних слобода, као и прецеденте *Lingens v. Austria*, пар. 42–47, *Castells v. Spain*, пар. 38–39, *Engel and Others v. the Netherlands*, пар. 98.

²³ Council of Europe, Declaration on freedom of communication on the Internet, adopted by the Committee of Ministers on 28 May 2003.

за друштвено умрежавање, нарочито у ситуацијама када би откривање идентитета могло да изазове одмазду, као у случајевима политичког и људскоправног активизма.²⁴

5. ЗАКЉУЧНА РАЗМАТРАЊА

Ширење надзора без преседана готово да не оставља никакву наду да ће стање анонимности какво смо некада познавали бити макар приближно остварљиво. Због тога ће у годинама које су пред нама питање права на анонимност вероватно постати једно од централних питања поводом кога ће копља ломити различити заинтересовани актери. Један могућ и по слободу изражавања опасан сценарио је да у будућности интернет буде детаљно и строго регулисан, уз обавезу сваког корисника да користи искључиво свој прави идентитет, тако да ће све што неко напише или изговори на интернету бити деанонимизовано. На другој страни спектра налазио би се сценарио потпуно нерегулисаног интернета, какав је био рани интернет, који је некада, у глобалним оквирина гледано, користила тек шачица ентузијаста, техногикова и хакера. Међутим, данашњи интернет није ни налик раном интернету. Он је интегрисан у све сфере савременог живота и ако буде остављен без икакве регулације, то би могло, у крајњем исходишту, да има несагледиве последице, налик повратку у Хобсово природно стање рата свију против свих. Међутим, важно је нагласити да онлајн анонимност као таква није инхерентно ни добра ни лоша већ она зависи од друштвеног контекста у коме се испољава и циљева које себи поставља. Због тога би било које регулаторно решење које би анонимност као такву, *a priori*, прогласило за непожељну на интернету било веома штетно, па чак и опасно јер би нас довело у ситуацију угрожавања основних људских права и слобода. Речју, укидање анонимности на интернету у пракси би значило укидање могућности за анонимно деловање генерално.

Неупитно је да ће државе и корпорације наставити да форсирају транспарентан интернет у коме ће мало шта моћи да се сакрије. Медији ће, да би себе заштитили од одговорности за ставове који се износе на њиховим порталима, наставити да заговарају индивидуализацију одговорности за оно што је објављено, што ће повратно отварати врата законодавцима да доносе све рестриктивније прописе о анонимној комуникацији на интернету. Осим тога, у потрази за публиком, на трагу

²⁴ Council of Europe, Recommendation CM/Rec (2011)7 of the Committee of Ministers to member states on a new notion of media, Strasbourg, 21. 9. 2011, par. 73.

таблоидног и сензационалистичког извештавања, медији ће наставити да боје анонимни интернет мрачним тоновима. Чак ће и многи корисници дигиталних технологија, који су често склони да изјаве да их дигитални надзор не забрињава јер немају ништа да крију, давати додатни импулс деанонимизацији интернета. Поврх тога, ризици који се око нас нагомилавају и опасности које се над нама надвијају ствараће оквир у коме ће се на анонимност гледати са подозрењем јер се иза ње могу критички потенцијални терористи, преваранти или педофили.

У таквим околностима једино још различита професионална и удружења грађана, ретка независна регулаторна тела и понека међународна организација могу представљати брану потпуној деанонимизацији не само интернета већ генерално живота у XXI веку. Међутим, ако званичне институције и организације цивилног друштва не успеју да зауставе гушење анонимности на интернету, а све су мањи изгледи за то, онда ће последње наде бити положене у руке техногикова, хакера и ентузијаста попут Едварда Сноудена или Жулијана Асанжа (Julian Assange), који ће бити спремни да ризикују сопствене животе зарад одбране универзалних вредности на којима почивају демократска друштва у којима верујемо да заслужујемо да живимо.

ЛИТЕРАТУРА

- [1] Akdeniz, Yaman. 1/2002. Anonymity, Democracy, and Cyberspace. *Social Research: An International Quarterly* 69: 223–237.
- [2] Asenbaum, Hans. 3/2018. Anonymity and Democracy: Absence as Presence in the Public Sphere. *American Political Science Review* 112: 459–472.
- [3] Бек, Урлик. 2001. *Ризично друштво*. Београд: Филип Вишњић.
- [4] Bernal, Paul. 2020. *What do we now and what should we do about Internet privacy*. London: SAGE.
- [5] Brin, David. 1999. *Transparent Society*. Basic Books.
- [6] Chandler, Jennifer. 2009. Privacy versus National Security. 121–138. *Lessons from the Identity Trail*, eds. Ian Kerr, Valerie Steevens, Carole Luckock. Oxford: Oxford University Press.
- [7] Clark, Jeremy, Philippe Gauvin, Carlisle Adams. 2009. Exit Node Reputation for Anonymity Networks. 399–416. *Lessons from the Identity Trail*, eds. Ian Kerr, Valerie Steevens, Carole Luckock. Oxford: Oxford University Press.

- [8] Cobb, Neil. 3/2007. Governance through Publicity: Anti-Social Behaviour Orders, Young People, and the Problematization of the Right to Anonymity. *Journal of Law and Society* 34: 342–373.
- [9] Cohen, Julie E. 2008. Privacy, Visibility, Transparency, and Exposure, *U. Chi. L. Rev.* 75: 181–201.
- [10] Coleman, Gabriella. 7/2019. How has the fight for anonymity and privacy advanced since Snowden’s whistle-blowing? *Media, Culture & Society* 41: 565–571.
- [11] Cooper, Christopher A. 3/2020. Public servants, anonymity, and political activity online: bureaucratic neutrality in peril? *International Review of Administrative Sciences* 86: 496–512.
- [12] Cushman, Donald P., Dudley D. Cahn. 1985. *Communication in interpersonal relationships*. Albany, NY: SUNY Press.
- [13] Electronic Frontier Foundation. 2015. Anonymity and Encryption – Comments submitted to the United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression. <https://www.ohchr.org/Documents/Issues/Opinion/Communications/EFF.pdf>, последњи приступ 23. јула 2021.
- [14] Feenberg, Andrew. 1999. *Questioning Technology*. New York: Routledge.
- [15] Feenberg, Andrew. 2/2000. Constructivism and Technology Critique: Replies to Critics. *Inquiry* 43: 225–237.
- [16] Flanagan, Mary, Daniel Howe, Helen Nissenbaum. 2008. Embodying Values in Technology: Theory and Practice. 322–353. *Information Technology and Moral Philosophy*, eds. Jeroen van den Hoven, John Weckert. Cambridge: Cambridge University Press.
- [17] Flaxman, Seth, Sharad Goel, Justin M. Rao. 2016. Filter Bubbles, Echo Chambers, and Online News Consumption. *Public opinion quarterly* 80: 298–320.
- [18] Froomkin, Michael. 2/1999. Legal Issues in Anonymity and Pseudo-anonymity. *The Information Society: An International Journal* 15: 113–127.
- [19] Froomkin, Michael. 2009. Anonymity and the Law in the United States. 441–464. *Lessons from the Identity Trail*, eds. Ian Kerr, Valerie Steevens, Carole Luckock. Oxford: Oxford University Press.
- [20] Fry, James. D. 2015. Privacy, Predictability and Internet Surveillance in the US and China: Better the Devil You Know. *University of Pennsylvania Journal of International Law* 37: 419–501.

- [21] Фуко, Мишел. 1997. *Надзирати и кажњавати: настанак затвора*. Нови Сад: Издавачка књижарница Зорана Стојановића.
- [22] Грамши, Антонио. 2018. *Интелектуалци, култура, хегемонија*. Нови Сад: Mediterran Publishing.
- [23] Gross, Emanuel. 1/2004. The Struggle of a Democracy against Terrorism – Protection of Human Rights: The Right to Privacy versus the National Interest – the Proper Balance. *Cornell Int. Law Journal* 37: 27–93.
- [24] Haimson, Oliver L, Anna Lauren Hoffmann. 6/2016. Constructing and Enforcing. „Authentic“ Identity Online: Facebook, Real Names, and Non-Normative Identities. *First Monday* 21(6), <https://journals.uic.edu/ojs/index.php/fm/article/view/6791/5521>, последњи приступ 22. јула 2021.
- [25] Heins, Marjorie. 2010. The Right to be let Alone: Privacy and Anonymity at the U.S. Supreme Court. *Revue française d études américaines* 123: 54–72.
- [26] Jardine, Eric. 2/2018. Tor, what is it good for? Political repression and the use of online anonymity-granting technologies. *New media & society* 20: 435–452.
- [27] Кастелс, Мануел. 2014. *Моћ комуникација*. Београд: Clio.
- [28] Knorr, Lidija. 2/2020. www: kritički potencijali anonimnog dijela interneta. *Jahr–European Journal of Bioethics* 11: 517–529.
- [29] La Rue, Frank. 2013. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue to the U.N. Human Rights Council [A/HRC/14/23]. Geneva: United Nations.
- [30] Lidsky, Lyrissa Barnett, Thomas Cotter,. 2007. Authorship, Audiences, and Anonymous Speech. *Notre Dame Law Review* 82: 1537–1604.
- [31] Lewis, James A. 2005. The Internet and Terrorism.. *Proceedings of the ASIL Annual Meeting* 99: 112–115.
- [32] Maffesoli, Michel. 1996. *The Time of the Tribes: The Decline of Individualism in Mass Society*. London: SAGE Publications.
- [33] Martin, Jason A, Anthony L. Fargo. 2/2015. Anonymity as a Legal Right: Where and Why It Matters. *North Carolina Journal of Law and Technology* 16: 311–376.
- [34] Marx, Gary T. 2/1999. What's in a Name? Some Reflections on the Sociology of Anonymity. *The information society* 15: 99–112.

- [35] Marx, Gary T. 1/2004. Internet Anonymity as a Reflection of Broader Issues Involving Technology and Society. *Asia-Pacific Review* 11: 142–166.
- [36] Moore, Adam D. 2010. *Privacy Rights – Moral and Legal Foundations*. Pennsylvania State University Press.
- [37] Note. 1961. The Constitutional Right to Anonymity: Free Speech, Disclosure and the Devil. *Yale Law Journal* 70: 1084–1128.
- [38] Papacharissi, Zizi. 2/2004. Democracy Online: Civility, Politeness, and the democratic Potential of Online Political Discussion Groups. *New media & Society* 6: 259–283.
- [39] Peddinti, Sai Tea, Keith W. Ross, Justin Cappos. 3/2017. User Anonymity on Twitter. *IEEE Security & Privacy* 15: 84–87.
- [40] Perbawani, Pulung S., Rahayu Rahayu, Irham Nur Anshari. 2/2018. Online Political Participation and Netizen Anonymity in Indonesia's Digital Democracy. *PCD Journal* 6: 185–212.
- [41] Платон. 1993. *Држава*. Београд: БИГЗ.
- [42] Петровић, Далибор. 2013. *Друштвеност у доба интернета*. Нови Сад: Академска књига.
- [43] Петровић, Далибор. 2008. *У међумрежју*. Београд: ИСИФФ и СФ
- [44] Posner, Richard. 2006. *Not a Suicide Pact: The Constitution in a Time of National Emergency*. New York: Oxford University Press.
- [45] Радојковић, Миролуб. 2015. Да ли ће грађанско новинарство заменити професионално? 305–314. *Политички идентитет Србије у глобалном и регионалном контексту*, ур. Весна Кнежевић Предић. Београд: Факултет политичких наука Универзитета у Београду.
- [46] Rheingold, Howard. 2000. *The Virtual Community, revised edition: Homesteading on the Electronic Frontier*. MIT press.
- [47] Sardá, Thais, Simone Natale, Nikos Sotirakopoulos, Mark Monaghan. 4/2019. Understanding online anonymity. *Media, Culture & Society* 41: 557–564.
- [48] Simmel, Georg. 2012. The Metropolis and Mental Life. 37–45. London: Routledge.
- [49] Strossen, Nadine. 2001. Protecting Privacy and Free Speech in Cyberspace Symposium: The Unwanted Gaze, by Jeffrey Rosen. *Georgia Law Journal* 89: 2103–2115.

- [50] Suler, John. 3/2004. The Online Disinhibition Effect. *Cyberpsychology & behavior* 7: 321–326.
- [51] Taylor, Charles. 1991. *The Malaise of Modernity*. Toronto: House of Anansi Press.
- [52] Turkle, Sherry. 1995. *Life on the Screen: Identity in the age of Internet*. New York: Simon & Schuster.
- [53] Voorhoof, Dirk. 2010. Интернет и право на анонимност. 73–83. *Слобода изражавања на интернету*, ур. Јелена Сурчулија. Београд: Центар за развој интернета.
- [54] Вујовић, Сретен. 1988. *Социологија града*. Београд: Завод за уџбенике и наставна средства.
- [55] Wallace, Kathleen A. 1999. Anonymity. *Ethics and Information technology* 1: 21–31.
- [56] Wang, S. A., M. S. Pang, P. A. Pavlou. 2018. 'Cure or Poison?' Identity Verification and the Spread of Fake News on Social Media. *Identity Verification and the Spread of Fake News on Social Media (September 14, 2018)*. *Fox School of Business Research Paper* (18–040).
- [57] Westin, Alan. 1967. *Privacy and Freedom*. New York: Ig Publishing.
- [58] Witzleb, Normann, David Lindsay, Moira Paterson, Sharon Rodrick. 2014. *Emerging Challenges in Privacy Law: Comparative Perspectives*. Cambridge: Cambridge University Press.
- [59] Зубоф, Шошана. 2021. *Доба надзорног капитализма*. Београд: Clio.

Dalibor PETROVIĆ, PhD

Associate Professor, University of Belgrade Faculty of Transport and Traffic Engineering, Serbia

Dejan PAVLOVIĆ, PhD

Assistant Professor, University of Belgrade Faculty of Political Sciences, Serbia

ANONYMITY IN THE AGE OF THE INTERNET

Summary

While in its early phases the Internet had been based on anonymous communication within virtual communities, the past two decades have brought about a reversal. The proliferation of digital networking platforms, on one hand, and loose internet privacy policies, on another, have been narrowing the space for anonymous use of the Internet.

Based on these trends the paper deals with the transformation of the role of online anonymity in the socio-legal perspective. In the first part we demonstrate that anonymity accompanies the modernization of contemporary societies, but there are also various freedom and security challenges. In the second part of the paper, we analyze internet anonymity as a phenomenon, assessing both arguments in favor and against it. We are particularly interested in identification of the stakeholders who advocate overall deanonymization, as one of the crucial characteristics of public and private life in contemporary society.

Key words: *Right to anonymity. – Privacy. – Digital platforms. – Regulations. – Surveillance.*

Article history:

Received: 30. 8. 2021.

Accepted: 2. 12. 2021.