

UDK 342.738:077

CERIF: S 123

DOI: 10.51204/Anali\_PFBU\_22106A

**Dr Dalibor PETROVIĆ\***

**Dr Dejan PAVLOVIĆ\*\***

## **PODRIVANJE ANONIMNOSTI U DOBA INTERNETA**

*Nakon rane faze razvoja interneta koja je počivala na anonimnoj komunikaciji u virtuelnim zajednicama, u poslednje dve decenije dešava se dramatičan preokret. Širenje upotrebe digitalnih platformi za umrežavanje, s jedne strane, i vrlo labave politike privatnosti na internetu, s druge strane, sve više sužavaju mogućnost anonimne upotrebe interneta.*

*Polazeći od takvih trendova, u radu se bavimo transformacijom uloge onlajn anonimnosti iz pravne i društvene perspektive sa ciljem da identifikujemo ključne faktore i aktere koji podstiču deanonimizaciju interneta.*

*U prvom delu rada pokazujemo da je anonimnost pratilac modernizacije savremenih društava, ali i da ona može nositi različite izazove po njihovu slobodu i bezbednost. U drugom delu rada analiziramo fenomen anonimnosti na internetu kroz različite pro et contra perspektive, obraćajući posebnu pažnju na identifikaciju ključnih aktera koji dovode do sveopšte deanonimizacije, kao jedne od suštinskih karakteristika organizacije i javnog i privatnog života u XXI veku.*

---

\* Vanredni profesor, Saobraćajni fakultet Univerziteta u Beogradu, Srbija, [d.petrovic@sf.bg.ac.rs](mailto:d.petrovic@sf.bg.ac.rs).

\*\* Docent, Fakultet političkih nauka Univerziteta u Beogradu, Srbija, [dejan.pavlovic@fpn.bg.ac.rs](mailto:dejan.pavlovic@fpn.bg.ac.rs).

**Ključne reči:** *Pravo na anonimnost. – Privatnost. – Digitalne platforme. – Regulacija. – Nadzor.*

## 1. UVOD

Danas će malo ko sporiti da je za prosečnog korisnika digitalnih tehnologija anonimnost na internetu praktično nedostižna. Svedoci smo brzog razvoja i množenja tehnologija usmerenih na identifikovanje korisnika interneta. Uvode se nove metode autentifikacije, verifikacije i nadzora, tako da se lica mogu digitalno i biometrijski identifikovati, označiti, pratiti i locirati u realnom vremenu. Pametni telefoni prepoznaju lica ili otisak prsta i sa njima povezuju brojne druge podatke koji su uskladišteni na personalnim uređajima ili na raznim serverima.

Uopšte uzev, nakon terorističkog napada 11. septembra 2001. godine u Njujorku, dakle upravo u vreme snažnog prodora interneta u sve sfere društvenog života, ideja ljudskih prava i sloboda neprekidno ustupa pred interesima nacionalne bezbednosti. Na delu je paradoks da sigurnosne mere koje su zamišljene da zaštite vrednosti liberalne demokratije značajno doprinose urušavanju istih tih vrednosti (Posner 2006, 1). Čini se da bezbednost kao vrednost trenutno uživa primat u odnosu na slobodu i autonomiju, zbog važnosti uloge države u zaštiti fizičke sigurnosti ljudi i imovine. U prilog tako pesimistične tvrdnje dovoljno je ukazati na brojne primere sekuritizacije različitih društvenih sfera nakon terorističkih napada u Sjedinjenim Američkim Državama, Francuskoj i Španiji, a sličan efekat je imala i migrantska kriza 2015. godine. Izvršna grana vlasti je u mnogim državama dobila šira ovlašćenja sa ciljem zaštite sigurnosti građana – od dužine trajanja pritvora, do presretanja komunikacije<sup>1</sup> i zamrzavanja imovine lica za koja se sumnja da pomažu terorističkim mrežama.<sup>2</sup> To stanje je izraz komunitarističke percepcije države i ideje društvenog ugovora (Chandler 2009, 126). Kada razmatramo traženje odgovarajuće ravnoteže između pojedinih ljudskih prava, uključujući privatnost i anonimnost, i interesa nacionalne bezbednosti, ovaploćene u raznorodnim invazivnim sigurnosnim merama, čini se da se da sve tri grane vlasti u mnogim državama olako daju prednost ovom drugom (Gross 2004, 30–36; Froomkin 2009, 441).

---

<sup>1</sup> Najpoznatiji primer je američki Zakon o patriotizmu iz 2001. godine (*Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism [USA Patriot] Act*).

<sup>2</sup> Videti rezolucije Ujedinjenih nacija 1267 (1999) i 1333 (2000) o osnivanju Komiteta za sankcije Saveta bezbednosti i sprovođenju postupka zamrzavanja imovine lica za koje se sumnja da finansiraju Al Kaidu.

Istovremeno, na vrednosnom nivou se takođe dešava transformacija percepcije anonimnosti. Iako je u periodu kada je internet tek nastajao doživljavana kao jedna od njegovih blagodeti, budući da se smatralo da anonimnost oslobađa pojedinca i podstiče konstruktivnu javnu debatu, ona je vremenom proterana u sferu ilegalnog. Posebno je zanimljivo to što se, s jedne strane, o privatnosti široko diskutuje, dok je, s druge strane, anonimnost, čini se, postala njena neželjena bliznakinja koje se roditelji, oličeni u državama i korporacijama, spremno odriču zarad koristi koje im njen izgon donosi. Tako prognana, anonimnost se sve više smešta u sferu tamnog, mračnog, tzv. dubokog interneta (eng. *deep internet*).<sup>3</sup> To praktično znači da je na delu jedna vrsta kriminalizacije anonimnosti, zbog čega svaki zahtev za anonimnom upotrebom interneta automatski izaziva podozrenje bezbednosnih službi, a sve češće i samih korisnika interneta.

Imajući takve trendove u vidu, u radu se bavimo transformacijom uloge anonimnosti u informacionom društvu iz pravno-sociološke perspektive sa ciljem da identifikujemo ključne faktore i aktore koji podstiču deanonimizaciju interneta. Jednostavnije rečeno, u analizi koja sledi pokušaćemo da odgovorimo na pitanje kome to i zbog čega smeta anonimni internet i koji su to makro i mikro faktori koji utiču na to da se anonimnost na internetu boji pretežno tamnim tonovima.

U radu zastupamo tri ključne teze. Prva, anonimnost je gradivni element koji je ugrađen u temelje modernih demokratskih društava. Druga, anonimnost kao takva nije inherentno ni dobra ni loša već zavisi od društvenog konteksta u kome se ispoljava i ciljeva koje sebi postavlja. Treća, ključni društveni akteri (*države, korporacije, mediji i korisnici interneta*) podstiču gušenje anonimnosti na internetu, a samim tim i u svakodnevnom životu.

U skladu sa tim, u radu najpre problematizujemo sam fenomen anonimnosti, baveći se njenom ulogom u razvoju modernih društava. S jedne strane, pokazaćemo da je anonimnost pratilac modernizacije savremenih

---

<sup>3</sup> Obično se kao *deep web* označavaju stranice koje traže prethodnu prijavu korisnika, čime se obezbeđuje dodatna anonimnost određenih sadržaja koji se na toj stranici nalaze. To znači da je pristup tim informacijama uslovno moguć, ali je bez prijave pristup ograničen na manju količinu informacija ili nema. Tipični primeri su *Facebook* i *JSTOR*. Sa druge strane, dark veb je specifičan po tome što je njegovim mrežama (kao što su *Tor* [*The Onion Router*], *I2P* [*Invisible Internet Project*] i *Freenet*) moguće pristupiti isključivo putem posebnih pretraživača. *Tor* je tehnologija čija je osnovna funkcija obezbeđivanje anonimnosti na internetu oslanjanjem na slanje podataka putem više servera i enkripciju na svakom od njih. Pokazalo se da je koristan za skrivanje identiteta opozicionih onlajn korisnika za vreme Arapskog proleća 2010. godine i Snoudenovih (*Edward Snowden*) akcija 2013. godine, ali ima i široku primenu za obavljanje čitavog spektra kriminalnih aktivnosti na crnim internet tržištima (Knorr 2020, 520; Bernal 2020, 32–35).

društava, ali da ona, isto tako, može nositi različite izazove po njihovu slobodu i bezbednost. U tom smislu ovaj članak ne pledira da ubedi čitaoca u bezuslovno pozitivne posledice anonimnog delanja već da ukaže na to da preterano insistiranje na njenim štetnim posledicama može biti pogubno po slobodu mišljenja i izražavanja u demokratskim društvima. Pažnju ćemo zatim posvetiti onlajn anonimnosti i aktuelnim raspravama o domašajima anonimnosti na internetu, ukazujući na njene specifičnosti u odnosu na tradicionalno shvaćenu anonimnost. U nastavku ispitujuemo njene društveno konstruktivne, odnosno pozitivne, a potom i negativne učinke. Poslednje poglavlje, pre nego što iznesemo naša zaključna razmatranja, posvećujemo analizi aktera i faktora koji dovode do proterivanja anonimnosti u sferu internet podzemlja (eng. *internet underground*), koje se najčešće naziva dubokim ili mračnim (eng. *dark*) internetom.

## 2. POJAM ANONIMNOSTI

Iako je pojam anonimnosti višeznačan te mu se može prići iz različitih naučnih perspektiva, njegovo određenje naizgled ne izaziva kontroverze. Moguće da zbog toga nema mnogo radova koji se iz pravne ili sociološke perspektive bave fenomenom anonimnosti, posebno domaćih autora.<sup>4</sup> Tek je širenjem upotrebe interneta aktuelizovano i pitanje anonimnosti, ali se autori ipak daleko manje interesuju za tu temu nego za temu privatnosti na internetu.

U dostupnoj literaturi anonimnost se najčešće deskriptivno definiše kao nemogućnost identifikacije u određenom stepenu ili kontekstu (Wallace 1999, 23). Tako Marks (Marx 1999, 100–101) ističe da je anonimnost jedan pol na veoma širokoj skali mogućnosti identifikacije koja se zasniva na sedam osnovnih dimenzija: 1. vlastito ime; 2. adresa; 3. pseudonimi koji mogu biti povezani sa nečijim imenom ili lokacijom (recimo, matični broj); 4. pseudonimi koji mogu biti povezani sa drugim vrstama identifikacije (na primer, identifikacioni broj u nekom sistemu); 5. prepoznavanje obrazaca ponašanja (recimo, životni stilovi); 6. društvena kategorizacija (pol, klasa, rasa, etnicitet itd.) i 7. simboli podobnosti ili nepodobnosti (posedovanje određenih znanja, artefakata ili veština kao izvora kategorizacije). Nekoliko godina kasnije isti autor (Marx 2004, 143–144) proširuje broj dimenzija

---

<sup>4</sup> Jedan od retkih tekstova objavljenih u Srbiji na ovu temu, pod naslovom „Internet i pravo na anonimnost“, nalazimo u zborniku *Sloboda izražavanja na internetu*, koji je uredila Jelena Surčulija (2010), ali i ovde je reč o stranom autoru Dirku Voorhovu (Voorhoof 2010).

na devet, ali ovoga puta ih predstavlja putem ključnih pitanja identifikacije – o kome je reč, koje karakteristike ima, gde se nalazi, kada je bio aktivan, ko je još povezan, šta koristi, šta se desilo, u šta veruje i koje su njegove karakteristike.

Slično tome, Vestin (Westin 1967, 39–40), jedan od utemeljivača prava na privatnost kao pravne discipline, zapaža da se anonimnost javlja kada je pojedinac u javnom prostoru ili čini dela u javnosti, ali izmiče identifikovanju i nadzoru. Zbog toga je za osećaj anonimnosti ključno da osoba smatra da neće biti identifikovana i obavezana da se ponaša u skladu sa važećim društvenim normama.

Supstancijalno, anonimnost se može odrediti kao nepovezivost nečijih osobenosti u bilo kom kontekstu, odnosno anonimnost je stanje u kojem drugi nisu u mogućnosti da uspostave vezu između nečije pojavnosti i njegovih drugih karakteristika (Wallace 1999, 24). Drugim rečima, za razumevanje anonimnosti je ključno da se ona odvija u određenom društvenom kontekstu, odnosno da podrazumeva određeni društveni odnos. Zbog toga anonimnost nije isto što i neimenovanost, nepoznatost ili izolovanost, jer je za anonimnost neophodno da postoje akteri koji neće biti u stanju da identifikuju osobu koja je u interakciji sa njima. Sličnog mišljenja je i Marks (Marx 1999, 2) koji zapaža da je, iako to može zvučati cinično, anonimnost zapravo krajnje društveni fenomen, budući da bez publike ona i ne postoji.

U određivanju pojma anonimnosti posebno je važno uspostaviti relaciju sa privatnošću. Iako su privatnost i anonimnost blisko povezani koncepti, ne može se govoriti o njihovom potpunom poklapanju. Anonimnost u određenoj meri i određenim slučajevima obezbeđuje privatnost, ali je svakako ne garantuje. Recimo, kada neko prisustvuje skupu anonimnih alkoholičara u procesu rehabilitacije, svakako ne uživa privatnost. Klasičan koncept privatnosti polazi od toga da svaki pojedinac ima pravo da bude ostavljen na miru, odnosno pravo da kontroliše pristup u svoju privatnu sferu, bilo da govorimo o njenoj fizičkoj ili simboličkoj demarkaciji. Međutim, pojavom digitalnih tehnologija i relativizacijom fizičkog prostora, privatnost je postala fluidna, a mogućnost njenog narušavanja sve suptilnija. Upravo su digitalne tehnologije i odgovorne za jednu vrstu zamućivanja razlike između anonimnosti i privatnosti, čineći ih izmešanim i pre svega poroznim usled intenziviranja upotrebe tehnologija nadzora. Zbog toga, Asenbaum (Asenbaum 2018, 461) zapaža da razumevanje anonimnosti treba da bude jasno odvojeno od koncepta privatnosti jer, u protivnom, neće biti moguće sagledati njene osobenosti, koje su ključne za svako demokratsko društvo. Na tom tragu, on smatra da je problem u tome što najveći broj definicija anonimnosti polazi od njene subjektivne strane. Naime, anonimnost se određuje u odnosu na to ko vrši identifikaciju subjekta. Na taj način se ona

shvata pasivno, kao puka negacija identiteta, odnosno stepen nemogućnosti da publika utvrdi identitet komunikatora, umesto da se ona shvata aktivno, kao akcija samih komunikatora. To je upravo posledica mešanja pasivnog koncepta privatnosti koja dolazi iz ljudskopravaške tradicije, kao odbrane prava na privatnost. Nasuprot tome, Asenbaum se zalaže za definisanje anonimnosti u tradiciji javnosferske teorije, poput one Jirgena Habermasa, smatrajući da je ona inherentno komunikativna. Anonimnost nije rezultat sakrivanja već, upravo suprotno, pokazivanja, razmene mišljenja i kreiranja identiteta. Kako ističe Asenbaum, inherentno oslobađajući efekat anonimnosti kao posledica nemogućnosti identifikacije takođe je konceptualizovan kao negativna sloboda, odnosno sloboda da se bude zaštićen od spoljne sankcije, što je isto posledica mešanja koncepta anonimnosti sa konceptom privatnosti. Međutim, prema njegovom mišljenju, anonimnost treba razumeti i kao pozitivnu slobodu, slobodu izražavanja i kreiranja identiteta, a ne kao suprotnost identitetu. Ona je preduslov za kreiranje identiteta, kao rezultat i negativnih i pozitivnih sloboda, odnosno „anonimnost predstavlja kontekstom uslovljeno ispoljavanje identiteta tako što se lična osećanja izražavaju u javnoj sferi, uz isključivanje pojedinih aspekata pravno utvrđene i fizički ukorenjene ličnosti“ (Asenbaum 2018, 462).

Osim u smislu mogućnosti identifikacije, anonimnost se može sagledavati i u odnosu na njenu svrhu, odnosno ciljeve. Tako Valas (Valas 1999, 29) ističe da se ona može grupisati u tri opšte kategorije:

1. anonimnost radi sprovođenja akcije anonimne osobe (akciona anonimnost);
2. anonimnost radi prevencije ili zaštite anonimne osobe od akcija drugih (uzvratna anonimnost) i
3. anonimnost radi sprovođenja procesa (procesna anonimnost).

Bilo koji slučaj anonimnosti može predstavljati svaki od tih tipova, bilo odvojeno, bilo zajedno, što znači da oni nisu međusobno isključivi već je samo neki dominantniji od druga dva. Takođe, ovde se anonimnost određuje vrednosno neutralno, što znači da se ne prejudicira da li će se ona koristiti u pozitivne ili negativne svrhe.

Uzimajući rečeno u obzir, za potrebe ovog rada anonimnost ćemo odrediti *interakciono* i *dualno*, kao anonimnost *od* i kao anonimnost *za*. Drugim rečima, smatramo da nema anonimnosti van interakcije, kao što anonimnost može podjednako da bude nemogućnost identifikacije *od* drugih subjekata i mogućnost uzimanja željenog identiteta *za*-rad ostvarivanja određenih individualnih ili društvenih ciljeva.

Stoga, anonimnost kao takva nije inherentno ni dobra ni loša već zavisi od društvenog konteksta u kome se ispoljava i ciljeva koje sebi postavlja. Recimo u kontekstu zatvorenog i represivnog društva anonimnost može imati važnu svrhu u formulisanju ideja čiji je cilj demokratizacija društva, ideja koje je zbog straha od sankcija moguće izneti jedino anonimno. S druge strane, u otvorenim i demokratskim društvima, gde se mišljenja uglavnom mogu nesputano iznositi, anonimnost nekada može da ude kontraproduktivna, recimo, može da podupire populističke ideje i demagoški diskurs u kojem onaj koji te ideje i diskurs promoviše za to ne preuzima odgovornost.<sup>5</sup> Međutim, kao što i, recimo, tehnologija, može biti upotrebljena i u destruktivne svrhe, ali to ne dovodi u pitanje njenu modernizacijsku ulogu, isto tako i anonimnost ne može na sebe preuzeti teret uzročnika društvene destrukcije. Drugim rečima, iako ona može biti oruđe koje se koristi za nanošenje štete drugima, njena upotreba sa tim ciljem nije proizvod njenih inherentnih osobenosti već najčešće simptom društvenih poremećaja koje uzorkuju neki širi procesi.

### 3. DEBATA O ANONIMNOSTI

#### 3.1. Anonimnost iz pravne i društvene perspektive

U prilog anonimnom izražavanju moguće je izneti brojne istorijske i uporednopravne argumente. O anonimnosti možemo govoriti u kontekstu slobode izražavanja, kao i prava na privatnost i autonomiju ličnosti. Sloboda izražavanja je neophodan alat građana koji žele aktivno da učestvuju u demokratskom društvu, da se informišu o javnim poslovima, sporovima i izborima. Dobro poznati argument milovske tradicije počiva na ideji da je sloboda izražavanja *conditio sine qua non* otkrivanja istine. Anonimni govor promoviše demokratsko samoupravljanje tako što uključuje u javnu debatu i one koji se, u suprotnom, ne bi čuli, naročito glasove i stavove onih koji imaju manju moć i uticaj, čineći tako javni diskurs, kao i sistem upravljanja, demokratskijim. Možemo očekivati i kreativnija rešenja društvenih problema ako se mogu čuti i nekonvencionalni predlozi. Specijalni izvestilac Ujedinjenih nacija za promociju i zaštitu prava na slobodu mišljenja i izražavanja (La Rue 2013, par. 49) veoma jasno ukazuje na vezu između anonimnosti i efektivne slobode izražavanja: „Ograničavanje anonimnosti ima odvratajuće dejstvo

---

<sup>5</sup> Recimo, lažne vesti koje kruže internetom često zapravo plasiraju anonimni ili pseudonimni izvori, posebno stvarajući konfuziju u vreme velikih društvenih kriza, poput pandemije Covid-19.

(eng. *chilling effect*), obeshrabruje slobodu izražavanja informacija i ideja. Ono, takođe, može izazvati isključivanje pojedinaca iz vitalnih društvenih sfera, podrivajući njihova prava na izražavanje i informaciju, povećavajući društvene nejednakosti. Pored toga, ograničavanje anonimnosti omogućava sakupljanje i skladištenje velike količine podataka od strane privatnog sektora, čime se značajno podiže nivo opterećenja i odgovornosti korporacija u pogledu zaštite privatnosti i bezbednosti takvih podataka.“

Anonimni govor doprinosi autonomiji i samoostvarenju ličnosti, tako što pruža mogućnost licu da istražuje nove ideje, načine izražavanja, pa čak i nove identitete (Lidsky, Cotter 2007, 1568–1569). Vestin (Westin 1967, 39–40) smatra da stanje anonimnosti osobi pruža mogućnost da se slobodnije izrazi jer zna da se stranac neće zadržavati u njegovom životu niti na njega može da vrši neki uticaj („fenomen stranca“). Nas, u stvari, zarad očuvanja brojnih ljudskih prava, zaista interesuju naša vidljivost i izloženost onima koji ne odobravaju kako se izražavamo i delujemo (Cohen 2008, 190). Mnogi ljudi ne bi izneli svoje stavove, ne bi se odlučili na uzbuđivanje, ne bi osporavali uvrežena mišljenja ili se konfrontirali predstavnicima vlasti ukoliko nisu u prilici da ostanu anonimni. Građani bi se teže priključivali kontraverznim organizacijama, kao što bi se ustručavali da diskutuju o osetljivim temama (Strossen 2001, 2106). Istorija obiluje primerima da su ljudi i organizacije koji su bili kritični prema državnim vlastima ili drugim moćnim licima i organizacijama doživljavali drakonske sankcije, bili lišavani života, slobode, imovine i slično. Odličan primer su brojna anonimna filozofska dela koja su tokom istorije osporavala religijske dogme. Anonimno pisanje ima dugu tradiciju i važnu ulogu u izražavanju ideja. U Engleskoj su anonimno pisali Defo (*Daniel Defoe*), Swift (Jonathan Swift), u Francuskoj Volter, dok su u Sjedinjenim Američkim Državama (SAD) čak i Federalistički spisi Hamiltona (*Alexander Hamilton*), Medisona (*James Madison*) i Džeja (*John Jay*) originalno bili objavljeni pod pseudonimom *Publius*, kao pisma uredniku. Čak je i predsednik Vrhovnog suda Maršal (*Chief Justice John Marshall*) pod pseudonimom *Prijatelj Republike* branio u javnosti pojedine odluke Vrhovnog suda SAD. Postoje dokazi da su mnogi američki predsednici i kongresmeni objavljivali svoje političke radove nepotpisani ili pod pseudonimom (Note 1961, 1085). Poseban i razumljiv motiv da budu anonimni imali su autori čija su dela osporavala politički *status quo*, ekonomske uslove rada, društvene norme i slično. Tomas Pejn (*Thomas Paine*) je 1776. godine objavio uticajni pamflet „Common Sense“ u prilog nezavisnosti od Velike Britanije pod pseudonimom *An Englishman* (Heins 2010, 66). Ta dela su imala neprocenjiv značaj za demokratizaciju i konstitucionalizaciju SAD, ali i šire.



Anonimnost je kasnije igrala značajnu ulogu u borbi za druge ciljeve, pre svega za građanska prava i prava žena, dok je danas važan štit za političke disidente. Kao što će se videti u raspravi koja sledi, mogućnost anonimnog delovanja na internetu posebno je danas važan segment političke borbe u mnogim autokratskim društvima.

Ipak, pravo na anonimnost nije kao takvo prihvaćeno u ustavima većine država sveta (Cobb 2007, Martin, Fargo 2015). Ne nalazimo takvu garanciju ni u Ustavu Republike Srbije. Neobično je što se u našem Ustavu ne navodi izričito ni pravo na poštovanje privatnosti, ali je pravo na poštovanje privatnog i porodičnog života garantovano u čl. 8 Evropske konvencije o ljudskim pravima i osnovnim slobodama, koja je sastavni deo pravnog poretka Republike Srbije. Osim toga, prema stavu Ustavnog suda RS, pravo na privatnost je sastavni deo ustavnog prava na dostojanstvo i slobodan razvoj ličnosti, garantovanih čl. 23 Ustava.<sup>6</sup>

U uporednom ustavnom pravu anonimnost uživa određen stepen zaštite kao element drugih prava i sloboda, pre svega slobode izražavanja i prava na privatnost, kao i slobode uopšte. Primetan je trend da se pravo na anonimnost sužava, s obzirom na to da interesi sigurnosti i nacionalne bezbednosti u konkretnim slučajevima odnose prevagu nad anonimnošću. Za to pitanje važna je i uloga kompanija koje pružaju usluge telekomunikacija. U ovoj sferi se poklapaju interesi državnog i privatnog sektora, pa su zakonska rešenja usmerena na obezbeđivanje uslova da se po potrebi može utvrditi identitet internet korisnika. Od internet provajdera se traži da sakupljaju i čuvaju podatke neophodne za identifikovanje korisnika, a u pojedinim državama vlasti imaju pravo da dobiju te podatke bez sudskog odobrenja ili nadzora (Ker.

U komparativnom pregledu značajni su nam normativni okviri i sudska praksa evropskih država i SAD. U Evropi je primetno traženje kompromisa između potrebe delotvorne primene zakona i poštovanja ljudskih prava garantovanih, *inter alia*, Evropskom konvencijom o zaštiti ljudskih prava i osnovnih sloboda (1950)<sup>7</sup> i Međunarodnim paktom o građanskim i političkim pravima (1966).<sup>8</sup> Državama potpisnicama je naloženo da je neophodno obezbediti pravo svakoga da na mišljenje, primanje i saopštavanje ideja bez mešanja javne vlasti i bez obzira na granice. Važno je, takođe, obezbediti i

---

<sup>6</sup> Ustavni sud Republike Srbije, Odluka o ustavnoj žalbi podnosioca X, UŽ-3238/2011, 8. mart 2012.

<sup>7</sup> *Službeni list SCG – Međunarodni ugovori* 9/2003, 5/2005, 7/2005 – ispr. i *Službeni glasnik RS – Međunarodni ugovori* 12/2010 i 10/2015.

<sup>8</sup> *Službeni glasnik SFRJ* 7/1971–73

pravo na privatnost. Ta prava i slobode, koji su povezani sa anonimnošću kao garantom efektivnosti, moraju biti primarni, a mogu biti ograničena kada za to postoje zakonska osnova, legitimni ciljevi i odgovarajuća mera proporcionalnosti između invazivnosti mera ograničenja i ciljeva kojima se teži.<sup>9</sup>

U Irskoj se trenutno vodi vrlo interesantan sudski postupak sa potencijalno veoma značajnim posledicama u oblasti zaštite prava na anonimnost na internetu. Jedna škola je od kompanije Fejsbuk zatražila da otkrije identitet korisnika Instagram naloga, a sudija Visokog suda Irske obratio se Sudu pravde Evropske unije tražeći odluku o prethodnom pitanju, u skladu sa čl. 267 Ugovora o funkcionisanju Evropske unije.<sup>10</sup> Od Suda se očekuje da odgovori na pitanje da li prava na privatnost, zaštitu podataka i slobodu izražavanja garantovanih Poveljom o ljudskim pravima Evropske unije (Evropska povelja) podrazumevaju i pravo da se na internet anonimno postavljaju sadržaji, pod uslovom da nisu protivni javnom poretku. Od Suda se zahteva i stav o uslovima pod kojima se, u skladu sa *GDPR* i Evropskom poveljom, kompanije koje vode platforme za društveno umrežavanje mogu prinuditi da razotkriju identitet inače anonimnih korisnika.<sup>11</sup>

U SAD postoji jasna linija precedenata kojima je utvrđeno da Prvi amandman<sup>12</sup> štiti pravo na anonimnost, uključujući i sferu interneta. Garantuje se pravo da se govori i piše anonimno, kao i da se anonimno učestvuje u grupnim aktivnostima. Vrhovni sud SAD je to pravo razvio kao derivat zaštite slobode govora, okupljanja, štampe, religije i peticije (Note 1961, 1084). Sasvim je logično da sudska tumačenja prava na privatnost ili anonimnost, koja nisu izričito garantovana Ustavom SAD, izazivaju više kontroverzi i protivljenja političkih grana vlasti i dela javnog mnjenja nego što je to slučaj sa u Ustavu izričito nabrojanim pravima, na primer slobodom štampe ili religije (Heins 2010, 56). U slučaju *NAACP v. Alabama* Vrhovni sud SAD je smatrao da bi obaveza otkrivanja članstva udruženja podrila

<sup>9</sup> Uporedi sa preambulom i čl. 15 Konvencije Saveta Evrope o visokotehnološkom kriminalu (tzv. Budimpeštanska konvencija o visokotehnološkom kriminalu), *Službeni glasnik RS* 19/2009, koja je stupila na snagu 1. jula 2004. godine.

<sup>10</sup> [Eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT), poslednji pristup 30. avgusta 2021.

<sup>11</sup> GDPRhub. The High Court – 2021 IEHC 287. 2021. [https://gdprhub.eu/index.php?title=The\\_High\\_Court\\_-\\_2021\\_IEHC\\_287](https://gdprhub.eu/index.php?title=The_High_Court_-_2021_IEHC_287), poslednji pristup 30. avgusta 2021. godine.

<sup>12</sup> „Kongres ne može da donosi nikakav zakon o ustanovljenju državne religije, kao ni zakon koji zabranjuje slobodno ispovedanje vere, a ni zakon koji ograničava slobodu govora ili štampe ili pravo naroda na mirne zborove i na upućivanje peticije vladi za ispravljanje nepravdi.“

to udruženje jer bi članovi bili podložni ekonomskoj odmazdi, otkazima, fizičkim pretnjama i drugim aktima netrpeljivosti i nasilja.<sup>13</sup> Vrhovni sud je dve godine kasnije proširio pravo na anonimno udruživanje oborivši lokalnu regulativu koja je dobrotvornim organizacijama nalagala da predaju spiskove svojih članova kao uslov za poreske olakšice.<sup>14</sup> Iste godine je Vrhovni sud bio suočen sa pitanjem da li Prvi amandman štiti i pravo da se govori anonimno. Naime, sud je oborio kalifornijski zakon koji je zabranjivao anonimne pamflete. U svom obrazloženju Sud je naveo da su anonimni pamfleti, brošure i knjige igrali važnu ulogu u progresu čovečanstva, tako što su progonjene grupe bile u mogućnosti da kritikuju opresivne prakse i zakone ili anonimno ili nikako.<sup>15</sup> U neposrednom kontekstu interneta američki sudovi takođe prepoznaju da sposobnost da se slobodno govori u velikoj meri zavisi od anonimnosti. Primera radi, Vrhovni sud Nju Džersija je smatrao da anonimni onlajn govornik uživa zaštitu Prvog amandmana da ostane neidentifikovan.<sup>16</sup>

Nasuprot izrečenom, iako je, dakle, jasan doprinos anonimnog izražavanja kvalitetu i kvantitetu ideja koje se nude u javnom prostoru, očigledno je i da se anonimnost može zloupotrebiti da se drugome nanese ozbiljna šteta. Lice može poželeti da se zaštiti anonimnošću ukoliko iznosi neistinu. Pod velom anonimnosti mogu se klevetati, vređati, uznemiravati ili povređivati nečija svojinska i autorska prava. Poseban problem je zloupotreba anonimnosti sa ciljem ugrožavanja pravnog poretka i nacionalne bezbednosti. Kao što sloboda izražavanja može biti ograničena „ako je to neophodno radi zaštite prava i ugleda drugih, čuvanja autoriteta i nepristrasnosti suda i zaštite javnog zdravlja, morala, demokratskog društva i nacionalne bezbednosti Republike Srbije“ (Ustav RS, čl. 46, st. 2), tako je racionalno očekivati da ni anonimnost ne može niti treba da uživa apsolutnu zaštitu. U tom smislu je ilustrativan primer slučaja u kome Vrhovni sud SAD 2010. godine nije zaštitio pravo da se potpiše referendumski inicijativa bez mogućnosti da potpisi inicijatora budu obnarodovani.<sup>17</sup> U državi Vašington dozvoljeno je osporiti zakon na referendumu ukoliko 4% glasača potpiše peticiju. Potpisnik mora da ostavi ime i adresu. Prema Zakonu o javnim ispravama, svako lice ima pravo na prepis ili kopiju tih podataka da bi moglo da utvrdi da li su potpisi validni. Potpisnici inicijative za referendumski opoziv zakona su protivnici istopolnih brakova i zbog svog potpisa su bili maltretirani, ali taj tretman nije

---

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

<sup>14</sup> *Bates v. Little Rock*, 361 U.S. 516 (1960)

<sup>15</sup> *Talley v. California*, 362 U.S. 60 (1960)

<sup>16</sup> *Dentrite International v. Doe No. 3*, 342 N.J. Super. 134 (App. Div. 2001). U ovoj presudi je kao precedent citirana *Talley v. California* u delu o značaju anonimnosti.

<sup>17</sup> *Doe v. Reed*, 561 U.S. 186 (2010).

bio dovoljno visokog intenziteta da bi ubedio sud da njihove identitete treba zaštititi od javnosti. Određene interesne grupe već decenijama zagovaraju ideju da bi američka vlada trebalo da nadzire aktivnost na internetu na način na koji to čini sa radio i televizijskim programom, ali FCC (*Federal Communications Commission*) ima vrlo usku nadležnost nad internetom. U literaturi se sreće i stav da iz perspektive publike anonimni govor ima manju vrednost jer adresant poruke nju ne može adekvatno da protumači ako ne zna ko je autor (Lidsky, Cotter 2007, 1539).

S druge strane, iz perspektive društvene teorije na fenomen anonimnosti među prvima su ukazali sociolozi koji su se bavili razvojem modernog načina života u urbanom okruženju. Iako neki od njih, poput Zimela, ne zauzimaju *a priori* negativan stav već anonimnosti prilaze kao neizbežnoj, pa čak i oslobađajućoj karakteristici urbanog nasuprot ruralnom životu (Simmel 2012), ipak kod mnogih klasičnih sociologa poput Tenisa ili Virta dominira negativna perspektiva anonimnosti (Vujović 1988, 32–37).

U nešto savremenijim sociološkim radovima daleko više se raspravlja o štetnim aspektima individualizma (Bauman, Gidens, Bek) nego što se fokus usmerava na samu anonimnost. Međutim, i u tom kontekstu, ponekad se otvara slično pitanje koje se otvara i u odnosu na posledice procesa individualizacije, odnosno u kojoj meri pojedinac treba da bude podređen zajednici. U tom smislu Tejlor (Taylor 1991, 9) prvu nelagodnost i razlog za brigu nalazi u individualizmu, kao fokusiranosti na sebe i izostanku brige za druge i društvo, gde se insistiranje na anonimnosti smatra pogrešnim jer se njime narušava odgovarajuća ravnoteža između interesa društva i anonimnosti i autonomije pojedinca. Takođe, postoje čak i tvrdnje da je privatnost prevaziđena, nepotrebna, pa čak i štetna, i da treba da prihvatimo potpunu otvorenost i izloženost jer „ako nisi ništa skrivio, nemaš se čega ni bojati“ (Brin 1998).

### **3.2. *Pro et contra* anonimnosti na internetu**

Ono što važi za anonimno izražavanje uopšte primenjivo je i na anonimnost na internetu. Perspektive su različite i suprotstavljene. Upravo zato taj fenomen i izaziva kontroverze i predstavlja podlogu za brojne zloupotrebe osnovnih ljudskih prava i sloboda. Kao dvosekli mač, anonimnost na internetu može pomoći uzbunjivačima da ostanu slobodni, posebno u autokratskim društvima, ali isto tako može pomoći delinkventima da izbegnu kaznu (Sarda *et al.* 2019, 561).

Najneposrednija korisnost anonimnosti na internetu vidi se u njenom doprinosu razvoju javnog diskursa podrškom slobodi govora i uopšte izražavanja (Akdeniz 2002, 224). Razvoj internet servisa i aplikacija koji korisniku pružaju slobodu stvaranja onlajn sadržaja revolucionisao je granice govora na način da svaki korisnik može brzo, lako i bez značajnih troškova da dopre do svojih adresata na globalnom nivou. To je fenomen koji Manuel Kastels (2014) naziva masovna samokomunikacija i definiše je kao novi obrazac masovne komunikacije koji se zasniva na visokoj autonomnosti budući da je ona samoprodukcija, samousmerena i samoodabrana.

Žardin (Jardine 2018) ističe da se, u kontekstu (ne)demokratičnosti političkih sistema, motivi za internet anonimnost mogu široko grupisati u dve kategorije: motivi koji su povezani sa mogućnostima koje anonimnost pruža i motivi koji se tiču neposrednih političkih potreba. Ovi prvi su najviše zastupljeni u veoma otvorenim i liberalnim političkim uređenjima, dok su motivi koji proističu iz političkih potreba najčešći u autoritarnim režimima. Drugim rečima, u otvorenim društvima su mogućnosti za anonimnu upotrebu interneta, recimo putem *Tor* pretraživača, široko dostupne, ali ne predstavljaju proizvod nužde već su ishod ličnih afiniteta pojedinaca. S druge strane, u autokratskim režimima su mogućnosti za onlajn anonimnost veoma sužene jer se države aktivno trude da suzbiju upotrebu tehnologija anonimnosti. Zbog toga, aktivisti koji koriste internet kao svoje polje govora sve češće bivaju progonjeni, hapšeni i osuđivani na stroge kazne zbog svojih aktivnosti, bilo da je reč o izborima u Zimbabveu ili Belorusiji, političkim prilikama u Tajvanu, Egiptu ili Hong Kongu.

O mahom pozitivnim efektima onlajn anonimnosti na političku participaciju govore različiti autori (Akdeniz 2002; Cooper 2020; Papacharissi 2004), kao što to pokazuju i neka istraživanja (Perbawani, Rahavu, Anshari 2018, 208). Politički aktivni građani često koriste anonimnost kao efikasno sredstvo za izbegavanje pravnih ili društvenih posledica za iznesene stavove, dok anonimnost na društvenim medijima može doprineti porastu političke participacije. Iako, naravno, kako ističe Papakarisi (Papacharissi 2004, 267), anonimnost može olakšati govor mržnje, ona je isto tako blagotvorna za slobodnu razmenu misli i komunikaciju oslobođenu ograničenja fizičkog sveta.

Upravo na tom tragu možemo pomenuti još jedan važan aspekt anonimne upotrebe interneta koji se tiče prevazilaženja strukturalnih ograničenja koja determinišu interakciju u realnom svetu. Polje dostupnih interakcija je na internetu daleko šire nego u realnom okruženju gde je komunikacije ograničena i mikrolokacijom pojedinaca i njegovom strukturalnom pozicijom u društvu (Petrović 2013, 170). Za razliku od komunikacije u svakodnevnom, fizičkom okruženju, komunikacija na internetu se odvija u daleko labavijim

strukturalnim okvirima gde je praktično jedina struktura koju je nemoguće neutralisati povezana sa kulturom, odnosno jezikom kojim se komunicira. Naravno, postoje i restrikcije koje nameću pre svega autoritarne države, a koje se odnose na tehničku (ne)mogućnost da se nekim prostorima na internetu uopšte pristupi, kao što je nemogućnost da iz Kine ili Rusije koristite Fejsbuk i neke druge digitalne platforme.

S druge strane, oni koji strahuju od anonimnosti na internetu ukazuju na štetu koja može proizaći iz situacija kada zlonamerna lica pod plaštom anonimnosti i bez straha od odgovornosti šire laži i druge štetne sadržaje ili masovno krše autorska prava. Nove informacione tehnologije su, poput Platonovog prstena moći,<sup>18</sup> u određenoj meri otežale pravnu zaštitu lica i imovine od prevaranata, klevetnika, nasilnika ili terorista. Recimo, anonimnost i enkripcija su jedan od osnovnih, ali i ključnih alata redovne komunikacije terorističkih organizacija (Lewis 2005, 112).

Anonimnost na internetu pruža mogućnost da se bez odgovornosti prema brojnoj publici odašilju sadržaji poput govora mržnje ili dezinformacija koje mogu imati veoma štetne posledice. Delovanje protivnika vakcinacije u doba pandemije kovida 19 možda je i ponajbolji primer za to. Šuler (Suler 2004, 321–322), koji je se bavio uzrocima nasilne komunikacije na internetu, tvrdi da je onlajn anonimnost jedan od ključnih faktora koji stvara tzv. efekat onlajn dezinhibiranosti. Taj efekat se, prema mišljenju tog autora, odnosi na stanje u kome ljudi, pod dejstvom različitih faktora u komunikaciji na internetu govore ili čine stvari koje inače, u regularnoj oflajn komunikaciji, ne bi govorili ili činili. Reč je o čitavom spektru ponašanja na internetu koji se kreće od benigne dezinhibiranosti, kad su ljudi otvoreniji i iskreniji nego u realnosti, do toksične dezinhibiranosti, kada se ljudi ponašaju neuporedivo lošije u odnosu na svoje svakodnevno ponašanje u realnosti.

---

<sup>18</sup> Platon u *Državi II* pripoveda o lidijskom pastiru Gigu koji pronalazi prsten moći koji nosioca može učiniti nevidljivim. Ovaj to koristi da se ubaci u dvorac i počini brojna nedela, a na kraju ubija kralja i preuzima kraljevstvo. „Nema čoveka koji bi se uzdržao da ne uzme tuđe, ako bi mogao neopažen da uzme nešto sa tržnice; ili bi išao po kućama i legao sa kim želi po svom nahodjenju; ubijao bi, ili oslobađao iz zatvora koga poželi, i u svakom pogledu bio poput boga među ljudima“ (Platon 1993, 359–360).

## 4. RAZUMEVANJE ANONIMNOSTI NA INTERNETU

### 4.1. Specifičnosti onlajn anonimnosti

Čini se da je pitanje anonimnosti dobilo značaj tek sa pojavom interneta. Mogućnost da se na mreži bude neko drugi već od njenih prvih dana inspirisalo je mnoge i na ozbiljne debate (Turkle 1995) i na šaljive opservacije na ovu temu.<sup>19</sup> Tehnooptimisti su bili uvereni da će javna sfera na internetu koja je oslobođena rasnih, verskih, etničkih, socioekonomski ili rodni obeležja identiteta dati ključni doprinos demokratizaciji društva (Akdeniz 2002; Papacharissi 2004), pa čak i da će pomoći da se ponovo uspostavi davno izgubljeni duh zajednice (Rheingold 2000).

Sve do pojave platformi za društveno umrežavanje, poput Fejsbuka, dakle negde do sredine dvehiljaditih, anonimna komunikacija na internetu je pre bila standard nego izuzetak, dok se iznošenje ličnih podataka na mrežu smatralo krajnje neobičnim, pa i nepoželjnim (Petrović 2008, 104–106). Ipak, pojavom platformi za društveno umrežavanje anonimnost sve više ustupa mesto javnom identifikovanju, bilo da je reč o dobrovoljnoj ili iznuđenoj identifikaciji korisnika interneta, da bismo danas došli u situaciju da je gotovo potpuno suzbijena mogućnost anonimne komunikacije na internetu.

Međutim, pre nego što dublje uđemo u debatu o konsekvencama onlajn anonimnosti, treba uspostaviti vezu između oflajn i onlajn anonimnosti. Naime, za razliku od anonimnosti u fizičkom okruženju, anonimnost na internetu se ne može poistovetiti sa nepostojanjem identiteta jer, kako zapaža Vorhov, povezivanje na internet, odnosno učestvovanje u komunikaciji putem interneta, neizbežno podrazumeva neku vrstu samoidentifikacije (Voorhoof 2010, 76). Zbog toga neki autori smatraju da bi, umesto anonimnosti, ispravnije bilo govoriti o pseudonimnosti, odnosno o onlajn identitetu koji nije neposredno povezan sa oflajn identitetom (Froomkin 1999, 114). Stvari dodatno komplikuje mogućnost postojanja višestrukih onlajn identiteta i istog onlajn identiteta koji deli više lica (recimo u onlajn društvenim pokretima). Osim toga, važno je napomenuti: da bismo uopšte mogli govoriti o anonimnosti na internetu, neophodno je da kumulativno budu ostvarena dva uslova: 1. da određenu onlajn anonimnu akciju nije moguće povezati sa

---

<sup>19</sup> Čuvena je karikatura Pitera Stajnera (*Peter Steiner*), koja se 1993. godine pojavila u magazinu *Njujorker* (*The New Yorker magazine*), na kojoj su prikazana dva psa od kojih je jedan za računarom i obraća se drugom psu rečima: „Na internetu niko ne zna da si pas.“

realnim identitetom aktera i 2. da dve anonimne akcije koje je učinio isti akter nije moguće povezati jednu sa drugom (Clark, Gauvain, Adams 2009, 400). Ukoliko je ispunjen samo prvi uslov, reč je o pseudonimnosti.

Dalje, važno je razlikovati jaku i slabu anonimnost na internetu. Slaba anonimnost je samo privid anonimnosti, dok jaka anonimnost znači da tragovi aktivnosti na internetu ne mogu ili vrlo teško mogu biti povezani sa osobom u realnom svetu. Recimo, jaka anonimnost je nužna uzbunjivačima ili disidentima koji se bore protiv represivnog režima, ali njoj pribegavaju i oni koji se bave polulegalnim ili ilegalnim aktivnostima na internetu. Prosečan korisnik interneta, koji je po pravilu na niskom nivou digitalne pismenosti, teško može odmaći dalje od slabe anonimnosti. Zanimljivo je to što se čini da većina njih i nema potrebu da sakrije svoj identitet na internetu niti misli da je to preterano važno (Electronic Frontier Foundation 2015, 3–6).

U onlajn prostoru važno je odrediti i šta se smatra identitetom aktera. Posredstvom „kolačića“ moguće je utvrditi IP adresu uređaja sa koga je poslata neka poruka, ali to ne znači automatski da pouzdano možemo znati ko je autor poruke, odnosno akter. Situacija postaje značajno komplikovanija ako se koriste mreže anonimnosti, u kojima se pomoću više proksi-servera sakriva izvorni pošiljalac poruke. Čak i ako bi postojale tehnološke pretpostavke da se identifikuju svi u lancu slanja poruke, sve do originalnog pošiljaoca, ostaje veliki politički problem da bi pravne norme i tehnologija mogli biti zloupotrebjeni u nedemokratske svrhe (Clark, Gauvain, Adams 2009, 402–405). Očigledno je da će uvek postojati pritisak istražnih organa da zarad efikasne i efektivne krivične istrage sužavaju prostor anonimnosti, što predstavlja svojevrstan oportunitetni trošak na strani zaštite anonimnosti uzbunjivača, disidenata i drugih lica kojima bi identifikacija ugrozila život, sigurnost ili neka druga prava.

## 4.2. Prilog razumevanju deanonimizacije interneta

Čini se da se u proteklih desetak godina osnažila jedna vrsta kampanje protiv anonimnosti na internetu. Stiče se utisak da je na delu jedan vid kriminalizacije anonimnosti koji praktično dovodi do toga da svaki zahtev za anonimnom upotrebom interneta automatski izaziva podozrenje ne samo bezbednosnih službi već sve češće i samih korisnika interneta. Planski ili ne, anonimnost se sve više gura u sferu mračnog interneta, čija je negativna slika pre svega proizvod onih koji kreiraju sliku javnog mnjenja. Jedno istraživanje koje je sprovedeno u Velikoj Britaniji pokazuje da se u više od 800 članaka o mračnom internetu, koji su u periodu 2001–2017. objavljeni u listovima *Daily Mail*, *Daily Mirror*, *Daily Telegraph*, *The Guardian*, *The Sun* i



*The Times*, on predstavlja u izrazito negativnom svetlu, pri čemu se ističe da je anonimnost jedna od njegovih glavnih karakteristika i da je ona povezana sa kriminalnim i antisocijalnim aktivnostima (Sarda *et al.* 2019, 562).

#### 4.2.1. Ključni akteri koji podstiču deanonimizaciju interneta

Osnovno pitanje na koje ovde želimo da odgovorimo jeste kome to smeta anonimni internet i zbog čega se on boji pretežno tamnim tonovima. Kao ključne aktere koji iz različitih motiva suzbijaju anonimnost na internetu za potrebe ove analize identifikujemo: države, korporacije, mejnstrim medije i same korisnike interneta. Ne treba izostaviti ni same *digitalne tehnologije* koje su osnovno sredstvo za deanonimizaciju njihovih korisnika. Iako se na ovom mestu nećemo detaljno baviti ulogom tehnologije kao jednog od aktera deanonimizacije interneta, u filozofskim studijama o tehnologiji otvoreno je pitanje da li tehnologije, osim funkcionalne, poseduju i inherentnu moralnu vrednost i da li takva vrednost može biti namerno usađena u tehničke sisteme (Feenberg, 1999). S jedne strane, postoje tvrdnje o vrednosnoj neutralnosti tehnologije koje ne isključuju mogućnost da ona ima značajan uticaj na društvene, moralne i političke aspekte života, ali negiraju da su negativne ili pozitivne posledice tog uticaja funkcija tog sistema. Naime, prema tom viđenju, tehnologija može biti samo instrument ljudske namere, a moralnost i politika su inherentni ljudima, a ne njihovim alatima. Tom stavu se suprotstavlja tvrdnja da su pojedine tehnologije u neposrednoj korelaciji sa konkretnim društvenim, etičkim i političkim vrednostima (Flanagan, Howe and Nissenbaum 2008, 347–348). U tom smislu, u većinu digitalnih proizvoda i usluga unapred je ugrađena mogućnost nadzora potrošača, dakle to postaje njihova primarna svrha (Zubof 2020), dok su, s druge strane, alati kao što su *Tor* i *Signal* dizajnirani upravo radi obezbeđivanja privatnosti i anonimnosti i pomažu da se te vrednosti usade i rasprostrane (Coleman 2019, 570).

Smatramo da je najplodnije viđenje Endrjua Finberga (Feenberg 2000, 228), koji tehnologiju vidi kao dvostrani fenomen – s jedne strane, ona je operator, dok je, s druge strane, ona objekt. Dakle, tehnologija nije samo efikasna sprava ili efikasan postupak već ona u sebi sadrži i različite društvene (ekonomske, političke, kulturne) kontekste koji su ukorenjeni u njenom dizajnu. U tom smislu digitalne tehnologije danas treba gledati kao poprište borbe različitih i suprotstavljenih interesa ključnih aktera. Neki od tih aktera, o kojima će biti reči u nastavku, imaju interes da se digitalne tehnologije razvijaju tako da sve više sužavaju mogućnost njihove anonimne upotrebe, dok su s druge strane akteri koji insistiraju na ugrađenim opcijama za anonimnost (poput različitih organizacija), ali i oni koji samostalno razvijaju alternativne tehnologije, poput pomenutog Tora ili Signala. *Države*

su, naravno, jedan od ključnih aktera od kojeg treba poći u analizi pritisaka koji vode deanonimizaciji interneta. U tom kontekstu ne može se na isti način govoriti o autoritarnim državama i onima koje imaju dugu demokratsku tradiciju. Međutim, bilo da govorimo o jednim ili drugima, izvesno je da je u korenu svake državne vlasti težnja da se kontrolišu dominantni diskursi u javnoj sferi. Na to su ukazivali mnogi autori, kao što su Gramši (2018), Fuko (1997), Kastels (2014). To koliko će se određeno društvo odupreti tim impulsima države zavisi od brojnih faktora poput demokratske tradicije, snage institucija, političke kulture i političkog sistema pojedinih država. Recimo, ako govorimo o SAD, tu je, kao što smo istakli u prethodnoj raspravi, pravo na anonimnost zagarantovano Prvim amandmanom njihovog Ustava, dok je Četvrtim amandmanom zagarantovano pravo da se nadzor vrši pod jasno definisanim okolnostima. Međutim, Snoudenova (*Edward Snowden*) otkrića pokazala su da, kada je reč o korisnicima interneta, državne agencije koje se bave nadzorom imaju sklonost da zaobiđu to ustavno pravo i da svakog, bilo da postoji pravni osnov ili ne, podvrgnu nadzoru (Coleman 2019, 569). U zemljama kao što je Kina taj nadzor je daleko direktniji i otvoreniji, a zakoni kojima se ta oblast uređuje retki su i lako ih je zaobići (Fry 2015, 499).

Prilično je jasno zašto *korporacijama* anonimnost na internetu nije u interesu. Bilo koja aktivnost koje se odvija onlajn, od kuće ili sa mobilnog uređaja, prati se, deponuje, kupuje i prodaje među tehnološkim džinovima kao što su Gugl (*Google*), Fejsbuk (Facebook) i Majkrosoft (*Microsoft*), a postoje i stotine manje poznatih trgovaca informacijama koji pomažu oglašivačima da izgrade zastrašujuće detaljne digitalne profile korisnika tako što prikupljaju podatke iz različitih izvora, uključujući i baze podataka raznih onlajn platformi (Moore 2010, 1). Možda je ponajbolje o tome pisala Zubof (2019, 261) obrazlažući kako, pre svega, internet kompanije, a zavaljujući trgovini sa njima i sve ostale kompanije, zarađuju ogroman novac upravo na osnovu mogućnosti identifikovanja osnovnih karakteristika, želja i potreba korisnika interneta. Imajući to u vidu, potpuno je razumljivo zbog čega Fejsbuk insistira na tzv. politici stvarnih imena (eng. *real name policy*) koju je ta kompanija uvela još 2015. godine (Haimson, Hoffmann 2016). U prilog tome govori i izjava koju je u to vreme dala sestra osnivača Fejsbuka Rendi Zakerberg (*Randi Zuckerberg*), direktor marketinga u kompaniji, koja se jasno založila za proterivanje anonimnosti sa mreža, obrazlažući to tvrdnjom da se ljudi ponašaju mnogo bolje kada koriste svoja stvarana imena (Witzleb *et al.* 2014, 296). Ipak, taj udar na anonimnost izazvao je revolt velikog broja korisnika, posebno u grupaciji seksualnih manjina (LGBTQIA), koji su to okarakterisali kao nepoštovanje osnovnih ljudskih prava (Haimson, Hoffmann 2016). Iako su u narednim godinama bili prisiljeni da odustanu

od krute politike stvarnih imena, Fejsbuk nijednog trenutka nije odustao od svoje namere da najveći broj svojih korisnika, na ovaj ili onaj način, identifikuje.

Tradicionalni mediji, kao treći akter deanonimizacije interneta, u njemu su, od njegovih samih početaka, videli rivala koga je valjalo zauzdati budući da je vrlo brzo postalo jasno da će internet ugroziti tradicionalne medije kao osnovno sredstvo informisanja. Dva su osnovna načina na koje tradicionalni mediji podrivaju anonimnost na internetu – direktno i indirektno. S jedne strane, oni insistiraju na svojoj kredibilnosti tako što ruše kredibilitet izvora na internetu koji su često upravo anonimni, odnosno neproverljivi. Posebno je u tom smislu izražena kampanja čiji je cilj fenomen tzv. lažnih vesti na internetu (*fake news*). Iako su mnoga istraživanja pokazala da je građansko novinarstvo sve važniji segment informisanja (Radojković 2015), tradicionalni mediji su uporni u tome da uruše verodostojnost interneta kao izvora informisanja, insistirajući na tome da je on izvor lažnih vesti, a kao jedan od ključnih uzroka njihovog plasiranja ističe se nepostojanje jasnog identiteta onih koji te vesti kreiraju i plasiraju (Wang, Pang, Pavlou 2018, 1; Radojković 2015, 309). S druge strane, indirektno podrivanje anonimnosti na internetu posledica je senzacionalističkog izveštavanja, u kojem se insistira na njegovim negativnim aspektima, što smo mogli videti na primeru izveštavanja britanskih medija o dark webu. Uopšte uzev, mediji su prezasićeni tekstovima u kojima se ukazuje na opasnosti koje vrebaju na internetu, a često se kao glavni protagonisti nelegalnih radnji ističu nepoznati ljudi na internetu koje korisnici neoprezno dodaju za prijatelje ili ulaze u nekakve privatne ili poslovne aranžmane sa njima.

I sami *korisnici* interneta svojim delovanjem često podstiču onlajn deanonimizaciju. Ako se još i može reći da Fejsbukova politika stvarnih imena na neki način prisiljava korisnike da se identifikuju, postavlja se pitanje zašto bi to korisnici radili na Tviteru, koji nema takvu politiku. Naime, jedno istraživanje o Tviteru (Peddinti, Ross, Cappos 2017, 84–87) pokazuje da većina korisnika, iako nije na to primorana, ima profile koje je lako povezati sa njihovim stvarnim identitetima (recimo, najveći broj koristi svoja prava imena i prezimena). Dakle, politike identifikacije korisnika digitalnih platformi nam ne mogu poslužiti kao jedino objašnjenje za široko rasprostranjenu praksu javnog ogoljavanja sopstvene intime na tim platformama. Prema našem sudu, potreba za neanonimizovanim, odnosno javnim delovanjem na internetu delom je posledica: 1. makrofaktora – odnosno težnje ljudi da unesu red u svoje okruženje u kontekstu života u rizičnom društvu i 2. mikrofaktora – odnosno potrebe da se kontekstualizuje interpersonalna interakcija na internetu.

#### *4.2.2. Mikro i makro faktori koji podstiču deanonimizaciju interneta*

Kada je reč o makrofaktorima, pritisci za deanonimizaciju koju sami korisnici interneta vrše jedni na druge deo su njihove implicitne strategije za kontrolisanje društvenih rizika sa kojima se susreću. Na ekspanziju rizičnog društva ukazao je još Urlih Bek (Bek, 2001) sredinom osamdesetih godina XX veka, tvrdeći da se savremeno društvo kreće ka stanju permanentnih rizika kojima su pojedinci sve izloženiji (od mogućnosti da izgube posao do mogućnosti da se razbole od zagađenja ili nastradaju u terorističkom napadu). Pojačavanje rizika posledica je radikalizacije modernizacije u drugoj polovini XX veka, odnosno individualizacijskih procesa zahvaljujući kojima se pojedinci iskorenjuju iz ukorenjujućih struktura industrijskoga društva, poput nacije, klase, vere, i bivaju sve više prepušteni sopstvenom menadžmentu kontrolisanja rizika koji ih okružuju. Međutim, prepuštenost samima sebi kod velikog broja pojedinaca izaziva stanje permanentne anksioznosti, koja ih nagoni da se vrate ukorenjujućim silama predmodernog društva, koje su često oličene i tribalističkim modelima zajedništva (Maffesoli 1996), gde se svi članovi plemena dobro poznaju i kao takvi svi su izloženi sudu javnosti. Te tribalističke tendencije se najbolje vide u eho komorama koje se obrazuju na internetu, odnosno grupacijama istomišljenika koji se sve više udaljavaju jedni od drugih (Flaxman, Sharad, Rao 2016). Svi ti procesi snažno utiču na pojedinca da se na mrežama deanonimizuje jer svako ko je anonimn može biti potencijalni uništitelj zajednice.

Na mikronivou, u kontekstu odvijanja interperosnalne interakcije, komunikatorima je važno da onoga sa kojim stupaju u interakciju mogu da smeste u neki sociokulturni i geografski kontekst, što je u onlajn komunikaciji često nemoguće (Cushman, Cahn 1985, 49–50). Zbog toga, a opet u kontekstu pomenutih rizika, rastu pritisci da se ljudi sa kojima se stupa u kontakt na internetu samoidentifikuju ne bi li se tako predupredili mogući neželjeni ishodi interakcije na internetu.

#### *4.2.3. Otpori deanonimizaciji interneta*

Nasuprot akterima koji vrše pritisak da se internet deanonimizuje stoje akteri koji imaju njima suprotstavljene interese. Kao ključne možemo da izdvojimo različita profesionalna i udruženja građana, nezavisna regulatorna tela i različite vladine i nevladine međunarodne organizacije koje aktivno rade na odbrani prava na anonimnu upotrebu digitalnih tehnologija. Posebno u akademskoj zajednici i među organizacijama civilnog društva danas postoji strah da regulatorni odgovor na realne ili zamišljene pretnje po javnu

bezbednost i nacionalnu sigurnost suštinski ugrožavaju našu posvećenost autonomiji ličnosti, privatnosti, jednakosti, slobodi izražavanja, kretanja ili udruživanja (Coleman 2019, 569).

Osim kolektivnih aktera, postoje i individualni akteri, poput nezavisnih novinara, aktivista, uzbunjivača ili hakera, koji u saradnji ili nezavisno tragaju za praktičnim rešenjima za problem nadzora, usput stvarajući i uslove za anonimno delovanje i osiguranje privatnosti.

Naročito su značajna nastojanja Saveta Evrope da se omogući zaštita ljudskih prava i poštovanje vladavine prava u informacionom društvu. Shodno preporukama te međunarodne organizacije, javne politike država članica moraju biti usmerene na očuvanje i proširenje zaštite, a naročito se mora voditi računa o pravu na privatnost života i korespondencije prilikom korišćenja interneta i drugih informaciono-komunikacionih tehnologija, uključujući i pravo korisnika da ne otkrivaju svoj identitet.<sup>20</sup> Takođe, Savet Evrope insistira na tome da je sloboda izražavanja i informisanja jednaka na internetu kao na ostalim forumima i podrazumeva da svako ima pravo da sebe izrazi i bude primalac informacija onlajn. U to spadaju, *inter alia*, politički govor, religijski pogledi, mišljenja i stavovi koji mogu da uvrede, šokiraju ili uznemire druge.<sup>21</sup> To, ipak, ne znači da se ne uzimaju u obzir reputacija i privatnost drugih, pa se tako može ograničiti izražavanje kojim se izazivaju diskriminacija, mržnja i nasilje. Ta ograničenja, prema rasprostranjenoj jurisprudenciji Evropskog suda za ljudska prava, moraju biti predviđena zakonom, usko skrojena i pod nadzorom sudova. Ne smeju biti arbitrerna, a moraju imati legitiman cilj, kao što su nacionalna bezbednost, teritorijalni integritet i javna bezbednost, sprečavanje nereda ili kriminala, zaštita zdravlja ili morala, ili zaštita prava i sloboda drugih.<sup>22</sup>

Korišćenje profila pod pseudonimom predstavlja i priliku i izazov za ljudska prava, pa Savet Evrope preporučuje da države članice sarađuju sa privatnim sektorom i građanskim društvom sa ciljem unapređenja prava na slobodu izražavanja korisnika na internetu. Jedan od važnih aspekata te inicijative jeste potreba da korisnici imaju punu informaciju o svojim izborima u pogledu onlajn identiteta. Taj stav je jasno iskazan u 7. principu

---

<sup>20</sup> 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.

<sup>21</sup> Vidi slučaj *Handyside v. The United Kingdom*, 5493/72, Svet Evrope, Evropski sud za ljudska prava, par. 49.

<sup>22</sup> Uporedi čl. 10, stav 2 Evropske konvencije za zaštitu ljudskih prava i osnovnih sloboda, kao i precedente *Lingens v. Austria*, par. 42–47, *Castells v. Spain*, par. 38–39, *Engel and Others v. the Netherlands*, par. 98.

Deklaracije o slobodi komunikacije na internetu: „U cilju obezbeđivanja zaštite od onlajn nadzora i jačanja slobode izražavanja informacija i ideja države članice treba da poštuju volju korisnika interneta da se ne objavi njihov identitet. To ne sprečava države članice da preduzimaju mere i saraduju da bi otkrile lica odgovorna za krivična dela...“<sup>23</sup> Pravo da se koristi pseudonim na internetu zaslužuje zaštitu, i iz ugla slobode izražavanja i prava da se primaju informacije i iz ugla prava na privatnost. Savet Evrope je svestan i potrebe za temeljnom zaštitom uzbunjivača. U novom medijskom ambijentu zaštita identiteta izvora informacija mora se proširiti i na korisnike onlajn platformi za društveno umrežavanje, naročito u situacijama kada bi otkrivanje identiteta moglo da izazove odmazdu, kao u slučajevima političkog i ljudskopravnog aktivizma.<sup>24</sup>

## 5. ZAKLJUČNA RAZMATRANJA

Širenje nadzora bez presedana gotovo da ne ostavlja nikakvu nadu da će stanje anonimnosti kakvo smo nekada poznavali biti makar približno ostvarljivo. Zbog toga će u godinama koje su pred nama pitanje prava na anonimnost verovatno postati jedno od centralnih pitanja povodom koga će koplja lomiti različiti zainteresovani akteri. Jedan moguć i po slobodu izražavanja opasan scenario je da u budućnosti internet bude detaljno i strogo regulisan, uz obavezu svakog korisnika da koristi isključivo svoj pravi identitet, tako da će sve što neko napiše ili izgovori na internetu biti deanonimizovano. Na drugoj strani spektra nalazio bi se scenario potpuno neregulisanog interneta, kakav je bio rani internet, koji je nekada, u globalnim okvirima gledano, koristila tek šačica entuzijasta, tehnogikova i hakera. Međutim, današnji internet nije ni nalik ranom internetu. On je integrisan u sve sfere savremenog života i ako bude ostavljen bez ikakve regulacije, to bi moglo, u krajnjem ishodištu, da ima nesagledive posledice, nalik povratku u Hobsovo prirodno stanje rata sviju protiv svih. Međutim, važno je naglasiti da onlajn anonimnost kao takva nije inherentno ni dobra ni loša već ona zavisi od društvenog konteksta u kome se ispoljava i ciljeva koje sebi postavlja. Zbog toga bi bilo koje regulatorno rešenje koje bi anonimnost kao takvu, *a priori*, proglasilo za nepoželjnu na internetu bilo veoma štetno,

---

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

<sup>24</sup> 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.

pa čak i opasno jer bi nas dovelo u situaciju ugrožavanja osnovnih ljudskih prava i sloboda. Rečju, ukidanje anonimnosti na internetu u praksi bi značilo ukidanje mogućnosti za anonimno delovanje generalno.

Neupitno je da će države i korporacije nastaviti da forsiraju transparentan internet u kome će malo šta moći da se sakrije. Mediji će, da bi sebe zaštitili od odgovornosti za stavove koji se iznose na njihovim portalima, nastaviti da zagovaraju individualizaciju odgovornosti za ono što je objavljeno, što će povratno otvarati vrata zakonodavcima da donose sve restriktivnije propise o anonimnoj komunikaciji na internetu. Osim toga, u potrazi za publikom, na tragu tabloidnog i senzacionalističkog izveštavanja, mediji će nastaviti da boje anonimni internet mračnim tonovima. Čak će i mnogi korisnici digitalnih tehnologija, koji su često skloni da izjave da ih digitalni nadzor ne zabrinjava jer nemaju ništa da kriju, davati dodatni impuls deanonimizaciji interneta. Povrh toga, rizici koji se oko nas nagomilavaju i opasnosti koje se nad nama nadvijaju stvaraće okvir u kome će se na anonimnost gledati sa podozrenjem jer se iza nje mogu kriti potencijalni teroristi, prevaranti ili pedofili.

U takvim okolnostima jedino još različita profesionalna i udruženja građana, retka nezavisna regulatorna tela i poneka međunarodna organizacija mogu predstavljati branu potpunoj deanonimizaciji ne samo interneta već generalno života u XXI veku. Međutim, ako zvanične institucije i organizacije civilnog društva ne uspeju da zaustave gušenje anonimnosti na internetu, a sve su manji izgledi za to, onda će poslednje nade biti položene u ruke tehnogikova, hakera i entuzijasta poput Edvarda Snoudena ili Žulijana Asanža (Julian Assange), koji će biti spremni da rizikuju sopstvene živote zarad odbrane univerzalnih vrednosti na kojima počivaju demokratska društva u kojima verujemo da zaslužujemo da živimo.

## LITERATURA

- [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] Bek, Urlih. 2001. *Rizično društvo*. Beograd: Filip Višnjić.
- [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 Reputiation 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>, poslednji pristup 23. jula 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] Fuko, Mišel. 1997. *Nadzirati i kažnjavati: nastanak zatvora*. Novi Sad: Izdavačka knjižarnica Zorana Stojanovića.
- [22] Gramši, Antonio. 2018. *Intelektualci, kultura, hegemonija*. Novi Sad: 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>, poslednji pristup 22. jula 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] Kastels, Manuel. 2014. *Moć komunikacija*. Beograd: 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] Platon. 1993. *Država*. Beograd: BIGZ.
- [42] Petrović, Dalibor. 2013. *Društvenost u doba interneta*. Novi Sad: Akademska knjiga.
- [43] Petrović, Dalibor. 2008. *U međumrežju*. Beograd: ISIFF i SF
- [44] Posner, Richard. 2006. *Not a Suicide Pact: The Constitution in a Time of National Emergency*. New York: Oxford University Press.
- [45] Radojković, Mirosljub. 2015. Da li će građansko novinarstvo zameniti profesionalno? 305–314. *Politički identitet Srbije u globalnom i regionalnom kontekstu*, ur. Vesna Knežević Predić. Beograd: Fakultet političkih nauka Univerziteta u Beogradu.
- [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. Internet i pravo na anonimnost. 73–83. *Sloboda izražavanja na internetu*, ur. Jelena Surčulija. Beograd: Centar za razvoj interneta.
- [54] Vujović, Sreten. 1988. *Sociologija grada*. Beograd: Zavod za udžbenike i nastavna sredstva.
- [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] Zubof, Šošana. 2021. *Doba nadzornog kapitalizma*. Beograd: 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.