

SISTEM U RIZIKU: NAPREDNE TEHNOLOGIJE U SRBIJI

Akteri, svrhe i pravni okvir primene u
javnom sektoru



SHARE
FONDACIJA

IMPRESUM

IZVRŠNI UREDNICI: Andrej Petrovski i Danilo Krivokapić

AUTORKE: Andrijana Ristić i Snežana Bajčeta

LEKTURA: Milica Jovanović

DIZAJN I PRELOM: Olivia Solis Villaverde

**SHARE Fondacija,
Oktobar 2025**

Sadržaj

Sažetak	4
Kontekst	4
Životni ciklus podataka	6
Metodologija	7
Prikupljanje podataka	9
Analiza podataka i automatizovano odlučivanje	21
Kritična infrastruktura i skladištenje podataka	28
Otvorena pitanja	34
Beleške	35

Sažetak

Studija predstavlja presek aktuelnih prilika u oblasti upotrebe naprednih tehnologija u Srbiji, kroz mapiranje aktera, tehnologija, nivoa i ciljeva primene. Nastojeći da uspostavi analitički okvir za dalje praćenje napretka u pogledu transparentnosti, zakonitosti i odgovornosti u primeni naprednih tehnologija, istraživanje donosi sistematizovan prikaz ključnih korisnika naprednih alata u javnom sektoru u Srbiji, te institucionalnih i pravnih okvira upotrebe tehnologije, uz identifikaciju postojećih rizika i izazova.

Period obuhvaćen istraživanjem obeležen je ubrzanom digitalnom transformacijom, centralizacijom podataka i sve češćim spajanjem bezbednosnih i administrativnih funkcija kroz tehnološke sisteme. Analiza obuhvata tri međusobno povezane dimenzije: pravni i institucionalni okvir, koji ukazuje na ograničenja u regulativi i nadzoru nad primenom tehnologija; upotrebu i obrasce implementacije naprednih tehnoloških sistema u različitim fazama životnog ciklusa podataka; i, konačno, uticaj na ljudska prava i šire društvene implikacije, sa posebnim osvrtom na rizike po privatnost, odgovornost i transparentnost javnih institucija.

Kontekst

Ubrzani tehnološki napredak posledično menja tradicionalne modele funkcionisanja države i društva. Sa ciljem unapređenja efikasnosti i dostupnosti usluga, tehnološke inovacije postale su sastavni deo operativnog okvira ne samo javnog, već i privatnog sektora. Međutim, često ishitrena i nedovoljno regulisana primena novih tehnologija i masovna obrada podataka, iako može podsticati inovacije i razvoj, istovremeno značajno utiče na porast rizika od kršenja ljudskih prava. Usled sve veće rasprostranjenosti veštačke inteligencije, ovaj trend postaje još izraženiji. U takvom kontekstu raste pritisak na relevantne aktere da što pre pristupe optimizaciji operativnih procesa, pri čemu se često zanemaruju temeljna istraživanja i sveobuhvatne procene rizika. Iako je veštačka inteligencija trenutno u fokusu digitalnih inovacija, ona čini samo deo šire kategorije naprednih tehnologija koje se razvijaju i primenjuju u različitim društvenim i institucionalnim oblastima u Srbiji.

Evropska komisija definiše napredne tehnologije kao „savremene ili buduće tehnologije za koje se očekuje da će u značajnoj meri uticati na transformaciju poslovnog i društvenog okruženja“, dok u tu kategoriju svrstava napredne materijale, naprednu proizvodnju, veštačku inteligenciju, proširenu i virtuelnu realnost, obradu velikih skupova podataka (Big Data), blokčejn tehnologiju, Cloud tehnologije, industrijsku biotehnologiju, internet stvari (IoT), mikro- i nanoelektroniku, mobilnost, nanotehnologiju, fotoniku, robotiku i bezbednosne tehnologije.¹

U skladu sa svetskim trendovima, Srbija je prethodnih godina počela intenzivnije da ulaže

u razvoj i distribuciju naprednih tehnologija, pogotovo veštačku inteligenciju. *Prva Strategija razvoja veštačke inteligencije u Srbiji* usvojena je 2019. godine čime su postavljeni temelji novog institucionalnog okvira u ovoj oblasti.² U skladu sa Strategijom, Vlada Srbije je 2021. osnovala *Institut za veštačku inteligenciju* sa ciljem istraživanja savremenih tehnologija veštačke inteligencije i stvaranja inovativnih rešenja.³ Zatim, po uzoru na slične preporuke UNESCO-a i Evropske unije, Srbija je 2023. godine usvojila *Etičke smernice za razvoj, primenu i upotrebu pouzdane i odgovorne veštačke inteligencije*.⁴ O intenzitetu fokusa na napredne tehnologije u Srbiji govori i činjenica da je nova Strategija razvoja veštačke inteligencije pripremljena i usvojena pre isteka stare. Nova strategija, između ostalog, za cilj ima „povećanje primene veštačke inteligencije u prioritetnim segmentima društva i privrede“.⁵

Pored zvaničnih dokumenata, brojne izjave državnih funkcionera potvrdile su novi pravac Vlade Srbije – da se država pozicionira kao regionalni lider u primeni veštačke inteligencije,⁶ čemu ide u prilog i odluka da Srbija predseđava Globalnim partnerstvom za veštačku inteligenciju (GPAI) u periodu od 2025. do 2027. godine.⁷ Imajući u vidu visoko postavljene ciljeve, koji u najvećoj meri prevazilaze postojeće kapacitete, primena naprednih tehnologija u različitim sektorima u Srbiji odvija se velikom brzinom, uglavnom bez značajnog osvrta na ljudska prava i slobode.

S obzirom na ovakvo strateško opredeljenje Srbije, neophodno je ponuditi uvid u razvoj i upotrebu naprednih tehnologija i staviti poseban naglasak na ključni element funkcionisanja ovih sistema – podatke građana koji se masovno prikupljaju, analiziraju, skladište i upotrebljavaju u javnom sektoru. Kroz mapiranje relevantnih primera, cilj ove studije je da analizira i pokaže 'životni ciklus' podataka građana i uloge različitih naprednih tehnologija u ovom sistemu, da istakne probleme povezane

sa različitim delovima tog ciklusa i na taj način doprinese prevenciji ili ispravljanju posledica takozvane nespretno digitalizacije.

Nespretna digitalizacija odnosi se na nepromišljene i loše izvedene digitalne transformacije u okviru društva. Ovakve transformacije često su rezultat nedovoljne tehnološke pismenosti, nedostatka adekvatnog ekspertskeg znanja ili zakonskog okvira od strane onih koji promene sprovode, zbog kojih dolazi do nepotpunih procesa koji mogu naneti više štete nego koristiti. U mnogo slučajeva se zanemaruje zaštita podataka zarad efikasnosti i lakše optimizacije određenih sistema, što dugoročno nosi ozbiljne posledice po privatnost građana za koje se ti sistemi uspostavljaju. Često su u pitanju javna preduzeća i drugi sistemi za čije funkcionisanje je zaslužna država odnosno lokalne samouprave i drugi organi vlasti.

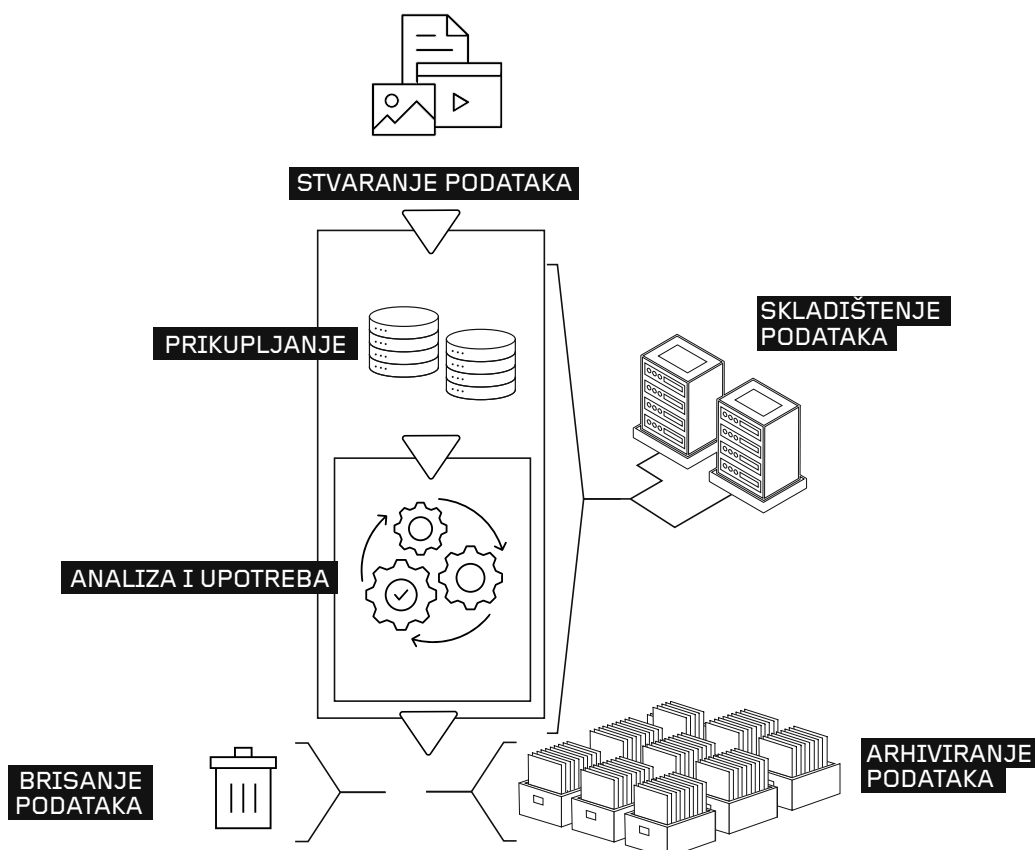
Životni ciklus podataka

Podaci kao takvi, postali su jedna od najznačajnijih moneta 21. veka. Podaci su neophodni za funkcionisanje gotovo svega u digitalnom svetu – svake usluge, proizvoda, sajta i mreže. Među ekspertskim krugovima se već godina ma o podacima priča kao o novoj nafti,⁸ jednom od najvrednijih svetskih resursa koji je od presudnog značaja za svetsku ekonomiju i funkcionisanje. Ipak, kao i sirova nafta, sirovi podaci u takvom obliku često imaju ograničenu upotrebn u svrhu. I baš kao što nafta podleže rafinisanju, tako i podaci moraju da prođu proces analize kako bi se iz njih izvukla maksimalna korist. Imajući to u vidu, proizvođači i kompanije shvatili su vrednost ličnih podataka kao pogonskog goriva za svoje poslove.

Kada su u pitanju države, pretpostavka je da bi situacija trebalo da bude malo drugačija. Prema društvenom ugovoru, građani su spremni da

prihvate određene obaveze i deo svojih ličnih sloboda žrtvuju zarad pravilnog funkcionisanja građanskog društva. Ovakav ugovor u savremenom društvu zahteva sledeći kompromis – građani ustupaju svoje lične podatke državi, a država im za uzvrat jemči da će njihove podatke koristiti kako bi im olakšala administrativne procedure i korišćenje javnih usluga. Ipak, u praksi izgleda da je situacija malo drugačija. Umesto optimizacije i olakšanog delanja, procesi digitalizacije javnih usluga ispunjeni su netransparentnošću, komplikacijama i napadima na kritičnu infrastrukturu.

Životni ciklus podataka u javnom sektoru obuhvata više uzastopnih faza. Proces započinje stvaranjem podataka, nakon čega se oni prikupljaju i postaju deo državne informacione infrastrukture. Pošto sami sirovi podaci imaju ograničenu vrednost, oni zatim prolaze kroz proces pripreme i analize, čime se pretvaraju u informacije koje se mogu koristiti za različite svrhe, uključujući analize, izveštavanje i automatizovano odlučivanje, sa ili bez podrške veštačke inteligencije. U završnoj fazi, poda-



ci se arhiviraju ili brišu iz sistema, u skladu sa propisima o čuvanju i zaštiti podataka. Paralelno sa svim fazama odvija se i skladištenje podataka, pri čemu se podaci čuvaju u različitim oblicima i bazama, zavisno od njihove namene i nivoa obrade.

Prvenstveni cilj ove studije je da bolje objasni tehnološke odlike mapiranih tehnologija i specifičnosti njihove upotrebe. Zatim, studija se trudi da problematizuje društvene izazove primene ovih tehnologija i ukazuje na rizike ugrožavanja ljudskih prava posredstvom istih. Poseban akcenat stavljen je na značaj ličnih podataka na kojima se većina ovih sistema zasniva i koji iste pokreću. Podaci kao pogonska snaga ovih procesa služe kao merilo kvaliteta funkcionisanja sistema. Drugim rečima, služe da prikažu na koje sve načine podaci mogu biti kompromitovani, zloupotrebljeni i preusmereni zarad ubrzanog unapređivanja ovih tehnologija. Na osnovu dobijenih uvida, nalaza i istraživačkih rezultata, u okviru studije su formulisane i preporuke relevantnim akterima, a u cilju prevencije i smanjenja rizika usled primene naprednih tehnologija u javnom sektoru.

Metodologija

U okviru ove studije, mapiranje naprednih tehnologija u Srbiji sprovedeno je sveobuhvatnom analizom primarnih i sekundarnih izvora, poput pravnih akata, strateških dokumenata Vlade Srbije, izveštaja institucija, javnih nabavki, novinskih članaka, izveštaja domaćih i međunarodnih organizacija civilnog društva i zvaničnih veb stranica državnih institucija, privatnih kompanija i drugih relevantnih aktera.

Identifikovano je 129 naprednih tehnologija, na osnovu nekoliko kriterijuma:

- Prvi kriterijum jeste da tehnologije **pripadaju kategoriji naprednih tehnologija** u skladu sa gorenavedenom definicijom Evropske komisije;
- Drugi kriterijum odnosi se na **potencijalni rizik po ljudska prava** i slobode usled primene tih tehnologija, gde se kao ključni indikator rizika razmatra tehnološki vođeno korišćenje podataka o ličnosti;
- Treći kriterijum podrazumeva **raznolikost oblasti upotrebe** naprednih tehnologija, odnosno nastojanje da zahvat slučajeva mapiranih tehnologija bude što raznovrsniji.

Takođe, priroda izvora informacija za ovo mapiranje istovremeno je značajno oblikovala istraživački domet, ali je istovremeno i važan istraživački nalaz sama po sebi. **Javno dostupne informacije o upotrebi naprednih tehnologija u javnom sektoru su vrlo oskudne, što ukazuje na nizak stepen transparentnosti.** Najzad, u studiju nisu uvrštene napredne tehnologije za koje nije bilo jasnih indicija da su u upotrebi u javnom sektoru u Srbiji, iako brojni izvori ukazuju na to da je broj naprednih tehnologija u ovim sektorima znatno veći.⁹

Srbija sve više ulaže u razvijanje rešenja baziranih na naprednim tehnologijama kroz finansiranje projekata u saradnji sa akademskom

zajednicom ili privatnim kompanijama. Ovim istraživanjem su obuhvaćeni i projekti koji ispunjavaju kriterijume naprednih tehnologija i potencijalnog uticaja na ljudska prava i slobode, a koji se finansiraju iz različitih fondova uključujući *Fond za investicionu delatnost*, *Fond za nauku Republike*, *Fond Instituta za veštačku inteligenciju* i *Fond AI4SME Serbia*, koji za cilj ima osnaživanje malih i srednjih preduzeća u primeni veštačke inteligencije, osnovan na inicijativu Vlade Srbije.

U skladu sa navedenim kriterijumima i istraživačkim izazovima, ova polazna studija dominantno je fokusirana na upotrebu naprednih tehnologija u javnom sektoru. Identifikovane su 54 napredne tehnologije koje primenjuju javni akteri, kao i 75 tehnologija u procesu razvoja kroz projekte koje finansira ili podržava Vlada Srbije ili druge državne institucije na kojima učestvuje akademska zajednica ili privatne kompanije.

Analitički pregled pokazuje da su napredne tehnologije najzastupljenije u oblasti bezbednosti (20), zatim manje u oblasti pravosuđa (5), trgovine (5), e-uprave (5), zdravstva (4), obrazovanja (4), i socijalnih prava (4), dok se u oblastima energetike (2), telekomunikacija (1), komunalnih delatnosti (1) i zaštite životne sredine (1) i drugim oblastima (2) napredne tehnologije ili ređe koriste ili su informacije o njihovoj primeni javno dostupne u manjoj meri.

Mapirane napredne tehnologije u ovoj studiji predstavljene su prema kriterijumu primarne funkcije koju imaju u okviru životnog ciklusa podataka u javnom sektoru – od faze prikupljanja podataka, u kojoj dominiraju tehnologije za

nadzor i praćenje, preko faze analize i automatizacije procesa odlučivanja koje sve češće obavljaju napredni tehnički sistemi zasnovani na algoritamskim rešenjima i veštačkoj inteligenciji, do razmatranja pitanja skladištenja i potencijalnih pravaca buduće upotrebe podataka i razvoja digitalizacije javne uprave. Posebna pažnja biće posvećena pitanju transparentnosti, odgovornosti i zakonitosti njihove primene, imajući u vidu ograničenu dostupnost informacija o konkretnim tehnologijama i praksama koje se koriste u Srbiji.

Iako su napredne tehnologije u studiji prikazane kroz pojedinačne faze životnog ciklusa podataka, od prikupljanja, preko analize i automatizovanog odlučivanja, do skladištenja, važno je napomenuti da njihova upotreba nije ograničena isključivo na jednu fazu. Mnoge napredne tehnologije deluju istovremeno u više faza ciklusa, preplićući funkcije prikupljanja, analize, razmene i donošenja odluka. Ipak, u ovoj studiji svaka tehnologija je predstavljena u onom segmentu koji najbolje osvetljava njenu dominantnu funkciju i uticaj u okviru određene faze. Takav pristup omogućava jasniju analitičku strukturu i bolju vidljivost sistemskih obrazaca u načinu na koji država koristi napredne tehnologije u radu sa podacima.

Najzad, imajući u vidu metodološka ograničenja ovog istraživanja, kao i nalaze koji ukazuju na postojeće izazove u pogledu institucionalnih kapaciteta, zaštite prava građana i javnog nadzora nad primenom naprednih tehnologija, poslednje poglavlje biće usmereno na identifikaciju otvorenih pitanja i istraživačkih praznina. Ona se odnose, pre svega, na potrebu za daljim empirijskim istraživanjima, razvojem regulatornih i etičkih okvira, te uspostavljanjem mehanizama koji bi osigurali veću transparentnost i odgovorno korišćenje podataka u javnom sektoru.

Prikupljanje podataka

Živimo u dobu u kojem su podaci postali jedno od ključnih razvojnih resursa savremenog društva. Svakog dana u svetu nastaje više od 400 miliona terabajta informacija,¹⁰ što svedoči o razmerama digitalne transformacije koja oblikuje gotovo sve sfere ljudske aktivnosti. Iako pojedinačni podaci u svom izvornom obliku često nemaju veliku analitičku vrednost, njihova ukupna količina, povezanost i mogućnost analize čine ih resursom od izuzetnog značaja. Potencijal podataka kao ekonomske i strateške vrednosti najpre su prepoznali privatni akteri, koji su na toj osnovi izgradili nove modele poslovanja i ostvarili značajan profit.

Sledeći taj primer, države širom sveta sve intenzivnije razvijaju politike i infrastrukture i napredne tehnologije za prikupljanje i upravljanje podacima svojih građana, sa ciljem unapređenja javnih usluga, efikasnije razmene informacija i automatizacije administrativnih procesa.¹¹ Međutim, prikupljanje podataka, pogotovo podataka o ličnosti, u javnom sektoru neretko se povezuje i sa širim funkcijama nadzora, kontrole i bezbednosti, što otvara važna pitanja o balansu između javnog interesa, zaštite prava građana i legitimne upotrebe tehnologija.¹²

U Srbiji, najznačajniji pomak u procesu digitalizacije u cilju unapređenja javnih usluga nastao je stvaranjem portala eUprava koji održava posebna služba Vlade Srbije – Kancelarija za IT i eUpravu. Portal predstavlja „centralno mesto elektronskih usluga javne uprave za sve građane, privredu i zaposlene u državnoj upravi i lokalnoj samoupravi”,¹³ a do sada eUprava beleži preko dva i po miliona korisnika (eGrađana).¹⁴ Veliki broj državnih institucija, uključujući ministarstva, gradove, opštine i zdravstvene ustanove, pružaju građanima eUsluge, što pretpostavlja razmenu podataka između građana i institucija. Portal eUprave je samo jedan primer masovnog prikupljanja po-

dataka građana. Međutim, veliki broj državnih institucija koristi napredne tehnologije kako bi prikupljali podatke građana radi dalje obrade i analize.

U skladu sa načelima nespretne digitalizacije, kao čest primer za isprobavanje ovih sistema uzimaju se ranjive grupe i njihovi osetljivi podaci.

JEDINSTVENI INFORMACIONI SISTEM PROSVETE (JISP)

Za potrebe tadašnjeg Ministarstva prosvete, nauke i tehnološkog razvoja, 2017. godine razvijen je i pušten u rad Jedinostveni Informacioni Sistem Prosvete (JISP) koji predstavlja najobimniju digitalizovanu bazu podataka o građanima, jer na jednom mestu objedinjuje sve informacije o ustanovama, zaposlenima, učenicima i studentima unutar obrazovnog sistema u Srbiji. Uspostavljen Zakonom o osnovama sistema obrazovanja i vaspitanja,¹⁵ ovaj sistem su državni zvaničnici okarakterisali kao najbolju i najvažniju reformu u obrazovanju. Sistem funkcioniše tako što se svakom učeniku dodeljuje Jedinostveni obrazovni broj (JOB) koji je isti kroz čitav obrazovni proces i predstavlja „ključ za povezivanje svih podataka” o tom licu u JISP-u.¹⁶ Sistem je takođe povezan i sa Centralnim registrom obaveznog socijalnog osiguranja, čime se u vezu dovode prosveta i privreda.¹⁷

S obzirom na to da se u JISP-u centralizuju sve informacije o obrazovnom sistemu u Srbiji, neophodno je da se iste konstantno prikupljaju, zbog čega su osmišljena brojna rešenja. Među prvim takvim rešenjima razvijen je i uveden sistem esDnevnika, ili sistem elektronskog dnevnika,

ka, u školskoj 2017/2018. godini koji je zamenio tradicionalne papirne dnevnike za upis ocena, evidenciju prisustva, praćenje uspeha i ponašanja učenika, sada u realnom vremenu. Sistem funkcioniše tako što nastavno osoblje unosi podatke u centralnu bazu, a roditelji imaju pristup podacima putem internet portala, koristeći posebne kredencijale.¹⁸ Međutim, sredinom 2020. godine, nastala je velika zabuna usled pojave novog sistema eŠkola, koji je razvila kompanija Tesla software d.o.o, promovisanog na portalu esDnevnika. Na eŠkolu je bilo moguće registrovati se koristeći iste kredencijale kao i na esDnevniku i sadržala je identične informacije o učenicima kao i na esDnevniku. Pristup podacima je bio zasnovan na „paketima usluga“ koji su se naplaćivali. Ministarstvo je prvobitno tvrdilo da taj sistem nije u njihovoj nadležnosti, što je izazvalo još veću zabrinutost kod roditelja i javnosti, nakon čega je saopšteno da sistem eŠkole nije namenjen za državne obrazovne ustanove, već za privatne.¹⁹ Ceo sistem se ističe velikim stepenom netransparentnosti i stvara anksioznost kod roditelja i zaposlenih, pogotovo nakon što su osetljivi podaci došli u posed privatne kompanije koja je na osnovu njih stvorila profitabilno rešenje za privatne obrazovne institucije.

Kao proizvod Strategije razvoja obrazovanja i vaspitanja u Republici Srbiji do 2030. godine,²⁰ sistem Zdravitas predstavlja još jedno tehničko rešenje koje bi trebalo da hrani JISP sistem podacima. Ovaj sistem je takođe privukao veliku pažnju javnosti, nakon što je najavljena njegova primena u školama bez konsultacija ili obaveštenja roditelja i učenika. Projekat je razvilo Ministarstvo prosvete

u saradnji sa Fakultetom organizacionih nauka i Fakultetom sporta i fizičkog vaspitanja. U suštini, Zdravitas predstavlja informacioni sistem namenjen praćenju fizičkog razvoja i motoričkih sposobnosti učenika.²¹ U okviru portala obrađuju se podaci i to, između ostalog, ime, prezime, ime jednog roditelja (zakonskog zastupnika), JMBG, JOB, datum, mesto i opština rođenja, pol, visina, težina, indeks telesne mase, kao i rezultati različitih testova fizičke spremnosti.²² Usled velikog nezadovoljstva učitelja, učenika i roditelja, Ministarstvo prosvete odložilo je primenu portala Zdravitas, uz najavu da će se dodatno poraditi na zaštiti podataka o ličnosti i argumentaciji u prilog digitalizaciji u ovoj oblasti.²³

INFORMACIONI SISTEM COVID-19

Nakon početka pandemije virusa covid-19, vlasti širom sveta našle su se u trci sa vremenom da istovremeno zaštite građane, obezbede koliko je moguće funkcionisanje svakodnevice i vode adekvatnu evidenciju o širenju virusa, i da za sve to vreme pružaju pravovremene i transparentne informacije. U Srbiji je u aprilu 2020. godine Zaključkom Vlade Republike Srbije ustanovljen Informacioni sistem COVID-19 (IS COVID-19) pod pokroviteljstvom Instituta za javno zdravlje „Dr Milan Jovanović Batut”.²⁴ IS COVID-19 predstavljao je centralizovani sistem čiji je cilj bio evidentiranje i praćenje pacijenata obolelih od koronavirusa zarad kontrole i dalje prevencije širenja pandemije. Samo nekoliko dana nakon puštanja sistema u rad došlo je do kompromitacije same baze. Naime, na stranici Doma zdravlja Rakovica našli su se javno

dostupni kredencijali za pristupanje bazi u kojoj su se nalazile velike količine ličnih podataka osoba obolelih od koronavirusa, uključujući i podatke osoba koje su potencijalni nosioci virusa zbog kontakta sa obolelima.²⁵ Samo mesec dana nakon što je Svetska zdravstvena organizacija proglasila globalnu pandemiju, ovakav proput u informacionoj bezbednosti relevantnih institucija čija je obaveza između ostalog bila da zaštite privatnost svojih pacijenata, doprinela je do povećanja brige među građanima kao i sumnje u sposobnost i želju države da se odgovorno i ozbiljno bavi zaštitom populacije.

U korišćenju naprednih tehnologija za prikupljanje podataka građana ipak prednjače bezbednosne državne strukture kao što su Ministarstvo unutrašnjih poslova (MUP), Bezbednosno-informativna agencija (BIA) i druge službe bezbednosti. U ovom smislu, podaci se najviše prikupljaju za potrebe nadzora i kontrole, a same napredne tehnologije razlikuju se po tome da li služe za masovni kao što je video nadzor ili targetirani nadzor koji, između ostalog, obuhvata i spajver.

Napredne tehnologije za masovni nadzor

Masovni nadzor, prema definiciji Saveća Evrope, predstavlja arbitraran oblik nadzora čiji je cilj sprečavanje teških krivičnih dela, a ne ublažavanje njihovih posledica, a koji je manje selektivan od „ciljanog“ nadzora kao što su prisluškivanje telefona, praćenje i slično, za šta je u načelu potrebna neka vrsta ovlašćenja poput sudskog naloga.²⁶ To praktično podrazumeva upotrebu tehnologija za aktivno praćenje

stanovništva, umesto za identifikaciju konkretne osobe od interesa koja predstavlja jasnu i neposrednu pretnju po imovinu, život ili javnu bezbednost.

U pogledu masovnog nadzora prednjači MUP, tačnije sektori policije, obezbeđenja grada Beograda i komunalne milicije.

Sistem video nadzora u Srbiji sastoji se u najvećoj meri od biometrijskih i naprednih kamera kineskih proizvođača Huawei i Dahua. U Beogradu je postavljeno preko hiljadu Huawei kamera sa mogućnostima prepoznavanja lica, dok je preko četrdeset gradova i opština u Srbiji opremljeno Dahua kamerama koje imaju napredne mogućnosti kao što je prepoznavanje lica, predmeta, vozila i objekata. Dahua kamere su postavljene širom Srbije na osnovu netransparentnih procesa javnih nabavki na kojima je samo jednoj beogradskoj bezbednosnoj firmi, Macchina Security, bio dodeljen posao.²⁷

PROJEKAT „SIGURNO DRUŠTVO“

U kontekstu prikupljanja podataka u javnom sektoru, jedan od najznačajnijih primera u Srbiji predstavlja projekat „Sigurno društvo“ koji je planiran kao deo šire saradnje između MUP-a i kineske kompanije Huawei. Projekat je predviđao postavljanje preko hiljadu kamera na više od 800 lokacija širom Beograda, sa mogućnošću biometrijske analize i prepoznavanja lica. Ova inicijativa, predstavljena javnosti 2019. godine, pokrenula je brojne polemike u vezi sa legitimnošću, proporcionalnošću i transparentnošću prikupljanja i obrade podataka građana u javnom prostoru.

Poverenik je ocenio da sistem predviđen za masovni biometrijski nadzor ne može biti opravdan, jer nije jasno

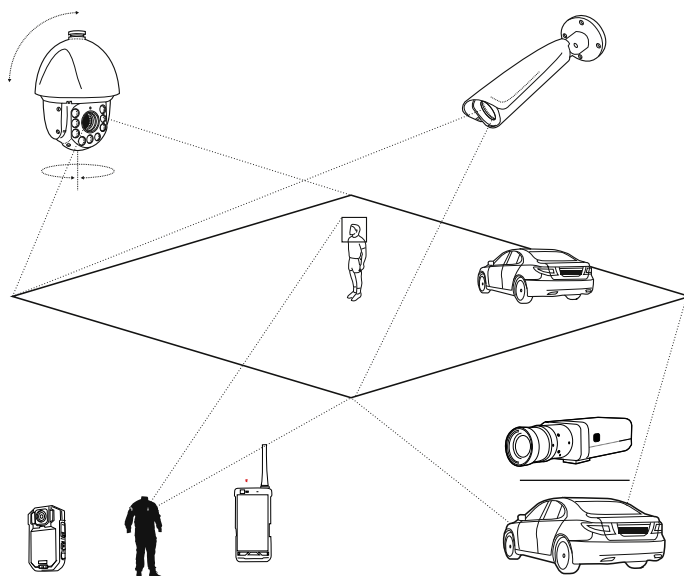
definisana njegova svrha niti je dokazana neophodnost i proporcionalnost takve mere u demokratskom društvu. Na osnovu toga, sprovođenje projekta je privremeno obustavljeno.

Uprkos tome, kamere sa mogućnošću biometrijske identifikacije počele su da se postavljaju tokom 2019. i 2020. godine, što se vremenski poklopilo sa uvođenjem vanrednog stanja usled pandemije COVID-19. Ubrzo nakon, SHARE Fondacija pokrenula je inicijativu „hiljade kamera“ sa ciljem mapiranja lokacija biometrijskih kamera i podizanja svesti o rizicima od masovnog nadzora na javnom prostoru.²⁸ Ova građanska akcija ukazala je na nedostatak transparentnosti od strane vlasti u vezi sa implementacijom naprednih tehnologija koje direktno utiču na pravo građana na privatnost i slobodu kretanja.²⁹

Tokom 2021. godine Ministarstvo unutrašnjih poslova predstavilo je nacrt novog Zakona o unutrašnjim poslovima, kojim je bilo predviđeno uvođenje pravnog okvira za korišćenje masovnog biometrijskog nadzora na javnim prostorima. Nakon snažnih reakcija civilnog društva, nacrt zakona je povučen iz procedure. Međutim, slični predlozi ponovo su se pojavili krajem 2022. godine, zajedno sa novim verzijama propisa o obradi podataka i internim evidencijama u okviru MUP-a. Iako su nacrti i tada povučeni nakon javne rasprave i snažnog negodovanja eksperata i aktivista, analize su ukazale da osnovni problemi, pre svega odsustvo jasne svrhe, neproporcionalnost obrade i rizik od neselektivnog nadzora, nisu bili adekvatno rešeni.³⁰

Ovaj slučaj ilustrativno pokazuje kako prikupljanje podataka u savremenom javnom sektoru može preras-

ti u praksu masovnog nadzora kada izostanu jasni normativni okviri, institucionalna odgovornost i javna kontrola. Istovremeno, ovaj slučaj otvara pitanje usklađenosti digitalnih inovacija sa osnovnim pravima građana i standardima vladavine prava.



U Beogradu je 2025. godine pokrenut još jedan ambiciozan projekat koji su gradske vlasti najavile kao model koji može biti primenjen u celoj Srbiji. Reč je o centralizovanom sistemu video nadzora koji sa 5000 kamera pokriva dvorišta svih 261 beogradskih škola. Ovaj napredni video nadzor ima sposobnost otkrivanja prisustva hladnog ili vatrenog oružja, kao i drugih potencijalno opasnih predmeta. Prema postojećim navodima, kamere nemaju opci-



ju za prepoznavanje lica, ali im se naknadno mogu izdati nove instrukcije za prepoznavanje određenih predmeta.³¹

Gradonačelnik Beograda istakao je da je projekat video nadzora škola „produžena ruka bezbednosnog sistema u Beogradu“, na čijem vrhu se nalazi MUP. Situacija na terenu se u realnom vremenu prati iz „komunalno-bezbednosnih stanica“ u kojoj se nalaze pripadnici Komunalne milicije, *Belih* i *Obezbeđenja grada*, direktno povezanih sa Policijom koja paralelno koristi ovaj sistem. Predviđeno je da do 2026. godine u funkciji bude 104 komunalno-bezbednosne stanice, a postoje planovi da se u sistem postepeno uključe i predškolske ustanove.³² Iako postoje prethodni primeri upotrebe video nadzora u obrazovnim ustanovama – vrtićima, srednjim i osnovnim školama širom Srbije,³³ ovaj sistem predstavlja sistemski i centralizovani pristup nadzoru obrazovnih ustanova.

Što se tiče Komunalne milicije, ovaj sektor koristi brojne sisteme za prikupljanje podataka o vozilima i automatsko prepoznavanje registarskih tablica,³⁴ kao i sistem „*Oko sokolovo*“, tehnologiju nadzora koja se koristi za identifikaciju i kažnjavanje nepropisno parkiranih vozila. Sistem je 2020. godine instaliralo javno preduzeće „*Parking servis*“ u saradnji sa Komunalnom milicijom, a funkcioniše zahvaljujući vozilima opremljenim kamerama visoke rezolucije i softverom za automatsko prepoznavanje registarskih tablica. Ovako uspostavljen sistem prepoznaje prekršaje parkiranja u realnom vremenu i izdaje kazne automatski bez kontakta sa građanima. Osim u Beogradu, sistem je implementiran i na ulicama Niša, Novog Sada i Kragujevca.³⁵

Pored fiksnih sistema video nadzora, MUP poseduje i veliki broj „pokretnih kamera“ u vidu dronova, sa značajno većim operativnim mogućnostima. Napredni tehnološki uređaji kineskih kompanija Yuneec, DJI i AFT opremljeni su kamerama visoke rezolucije, a neki čak poseduju i modul za automatsko praćen-

je osobe ili objekta, određivanje njihove tačne geolokacije, prebrojavanje ljudi ili objekata u masi, ali i modul za prepoznavanje i detekciju lica, a policija ih koristi za taktičko-obaveštajno izviđanje, nadzor granica i obala, kao i kontrolu protesta.³⁶

Pored bezbednosnih državnih institucija i obrazovnih ustanova, ustanove zdravstva uveliko su deo bezbednosnog sistema u Srbiji. Video nadzor u zdravstvenim ustanovama u Srbiji, poput Ginekološke klinike „*Narodni front*“ i Kliničkog centra Bežanijska kosa u Beogradu ili Opšte bolnice „*Dr Radivoj Simonović*“ u Somboru, obrazložen je ciljem veće bezbednosti pacijenata, osoblja i imovine, odnosno unapređenjem kontrole pristupa. Međutim nije poznato da li i na koji način zdravstvene ustanove kontrolišu potencijalna prekoračenja u korišćenju video nadzora za svrhe bezbednosti, a na štetu poverljivosti podataka i privatnosti pacijenata.

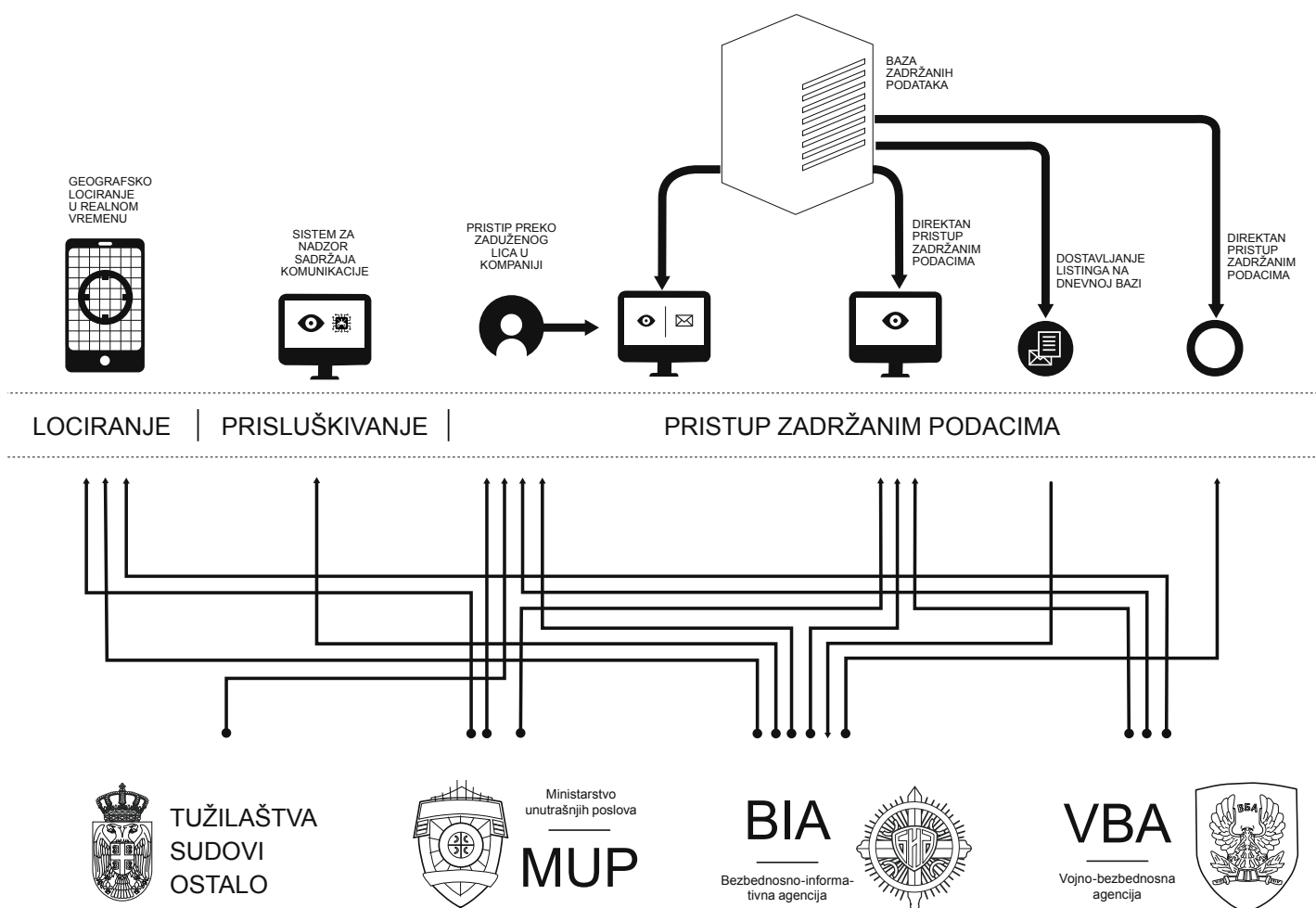
U jednom takvom slučaju Dom zdravlja Stari Grad u Beogradu implementirao je biometrijski softver za kontrolu prisustva zaposlenih, koristeći tehnologiju prepoznavanja lica. Zaposleni su morali da budu fotografisani po dolasku i odlasku sa posla pomoću tableta postavljenog na ulazu u objekat, nakon čega se preuzimaju lični podaci iz baze koji odgovaraju identifikovanoj osobi, prenose se na korisnički uređaj koji podatke u konačnici i prikazuje.³⁷ Nakon burne reakcije civilnog društva i neutemeljenosti primene ove napredne tehnologije u pravnom sistemu Srbije, ovaj sistem nadzora je ukinut.

Upotreba video nadzora zabeležena je i u pojedinim prihvatnim i azilnim centrima, poput Prihvatnog centra Principovac i Centra za azil u Vranju.³⁸ Ipak, pretpostavlja se da je obim masovnog video-nadzora i prikupljanja podataka građana ovim putem znatno širi od onoga što je dostupnim istraživanjem moguće utvrditi, što dodatno ukazuje na problem nedostatka transparentnosti u ovoj oblasti.

Napredne tehnologije za targetirani nadzor

Potreba da nadležni organi prate aktivnosti građana postoji odavno. U vreme kada se komunikacija uglavnom odvijala uživo, licem u lice, prikupljanje informacija podrazumevalo je fizičko prisustvo na mestima koje su pojedinci često posećivali. Sa prelaskom komunikacije na infrastrukturu mobilnih mreža, nadležni organi su razvili nove metode nadzora poput prisluškivanja putem mobilnih operatora.

Targetirani (digitalni) nadzor predstavlja proces nadzora ili špijuniranja određene osobe ili organizacije koje su od interesa za nadležne organe, korišćenjem digitalnih tehnologija. Targetirani nadzor može uključivati kompromitaciju uređaja usled instaliranja malvera i spajvera ili kompromitaciju komunikacija različitim tehnikama i tehnologijama.³⁹



U slučaju Srbije, pored zakonski propisanih mehanizama za nadzor komunikacija, nadležni organi, pre svega MUP i BIA, uspostavili su i neformalne, paralelne načine pristupanja metapodacima građana i prisluškivanja komunikacije.⁴⁰ Ove prakse, koje su u više navrata problematizovane zbog netransparentnosti i izostanka adekvatnog nadzora, ukazuju na širi institucionalni obrazac koji omogućava zloupotrebu tehničkih kapaciteta za praćenje građana. Cellebrite

Takva zloupotreba manje naprednih tehnologija već sama po sebi ukazuje na visok rizik i potencijal za zloupotrebu savremenijih, naprednih tehnologija. Danas, kada se komunikacija pretežno odvija putem interneta i privatnih aplikacija za razmenu poruka, država pribegava još invazivnijim tehnikama nadzora, među kojima posebno mesto zauzima upotreba špijunskih softvera. Ovi alati, osim mogućnosti presretanja i praćenja komunikacije, omogućavaju pristup ličnim podacima, kao i aktiviranje mikrofona i kamere na uređajima korisnika, što otvara dodatna pitanja o granicama zakonitosti, proporcionalnosti i zaštite privatnosti u digitalnom okruženju.

Prilikom mapiranja naprednih tehnologija u Srbiji identifikovano je osam naprednih tehnologija korišćenih u svrhu targetiranog nadzora, a svih osam primenjuju nadležni državni organi u oblasti bezbednosti. Konkretno, identifikovana su dva alata za presretanje komunikacije kompanija *Trovisor* i *Circles*, jedan alat za digitalnu forenziku UFED kompanije *Cellebrite* i pet špijunskih softvera za koje postoje indikacije da su korišćeni u Srbiji, uključujući *RCS* alat Hacking Teama, *FinFisherov FinSpy*, *Intelexin Predator*, *Pegasus* NSO Grupe i tzv. *NoviSpy*, za koji se sumnja da je domaće proizvodnje.

U okviru istraživanja naprednih tehnologija u Srbiji, identifikovana je primena dva alata za presretanje komunikacije kompanija *Circles* i *Trovisor*. Po svojim karakteristikama, ovi alati omogućavaju presretanje i praćenje telefonskih poziva, poruka, kao i lokacije uređaja u

slučaju alata *Circles* koji iskorišćavaju ranjivosti Signaling System 7 (SS7) protokola mobilne telefonije,⁴¹ i internet saobraćaja u slučaju alata *Trovisor* putem specijalizovanih monitoring centara.⁴² Oba alata možemo svrstati u tradicionalne tehnologije za presretanje komunikacije koje imaju utemeljenje u pravnom sistemu Srbije jer ne poseduju kapacitete za špijuniranje uređaja, dok njihova upotreba podleže obavezama transparentnosti i zakonitosti.

Na osnovu izveštaja Citizen Laba, alati kompanije *Circles* povezivani su sa Bezbednosno-informativnom agencijom, koja je identifikovana kao korisnik ove tehnologije.⁴³ U slučaju alata kompanije *Trovisor*, dokumenti koje je objavio WikiLeaks pokazuju da su predstavnici ove kompanije često posećivali Srbiju radi prodaje nadzorne opreme, te se na osnovu dostupnih informacija pretpostavlja da je do kupovine zaista došlo. Ipak, i dalje ostaje nepoznato koja je bezbednosna služba koristila tu opremu.⁴⁴

Najveći broj mapiranih naprednih tehnologija u oblasti targetiranog nadzora predstavljaju špijunski softveri. Špijunski softveri predstavljaju tehnologije koje pored sposobnosti koje poseduju alati za presretanje komunikacije, poseduju i veliki broj drugih mogućnosti kojima se ostvaruje pristup gotovo svim postojećim podacima na targetiranom uređaju. Hacking Team i FinFisher su začetnici ove industrije, dok su *Predator* i *Pegasus* – alati kompanija *Intellexa* i *NSO Grupe* – poznati po svojoj intruzivnosti i sofisticiranosti, nastali kao posledica velike ekspanzije industrije vođene velikom potražnjom vlada širom sveta. *NoviSpy* i slični alati domaće proizvodnje, uglavnom predstavljaju kopije naprednih, komercijalno dostupnih špijunskih softvera, najčešće u cilju smanjenja troškova, zaobilaženja diplomatskih prepreka u slučaju trgovinskih barijera ili maskiranja trago-va isključivanjem posrednika, tj. komercijalnih kompanija koje prodaju špijunске softvere.

Špijunski softveri koriste skrivene ili do tada neotkrivene ranjivosti uređaja, operativnih

sistema, ili pojedinih aplikacija preko kojih se instaliraju na uređaj. Fizički pristup je potreban za NoviSpy, dok se ostali špijunski softveri oslanjaju na daljinsku instalaciju i to najčešće putem slanja poruke koja sadrži maliciozan link. Ukoliko meta klikne na takav link, pokreće se čitav niz procesa koji za cilj imaju kompromitaciju uređaja (1-klik napad). Najnapredniji alati, poput Pegasusa, omogućavaju zaražavanje uređaja bez interakcije mete, kada sam postupak slanja maliciozne poruke ili poziva pokreće proces inficiranja uređaja (0-klik napad). U najvećem broju slučajeva, špijunski softveri su programirani da brišu tragove infekcije, te je meta digitalne špijunaže najčešće toga nesvesna.

Nakon instalacije na uređaj, špijunski softveri daljinski prate, prikupljaju, eksfiltriraju, kontrolišu ili manipulišu podacima sa uređaja.⁴⁵ Ostvaruju pristup svim postojećim podacima, uključujući pristup svim vidovima komunikacije, i preko mobilnih operatora, ali i preko interneta, svim fajlovima i dokumentima, fotografijama, video snimcima i aplikacijama. Špijunski softveri imaju i mogućnost da daljinski kontrolišu i aktiviraju kameru, mikrofona, lokaciju, kao i da šalju slike ekrana u određenim vremenskim intervalima, i sve to bez pratećih notifikacija koje se pojavljuju prilikom redovnih aktivnosti.

Uprkos intruzivnoj i neselektivnoj prirodi špijunskih softvera, kao i izostanku zakonskog osnova za njihovu upotrebu, Srbija je identifikovana kao korisnik svih pet alata. Prema procurelim podacima kompanije Hacking Team, Bezbednosno-informativna agencija povezana je sa alatom RSC već 2012. godine.⁴⁶ Istraživanje Citizen Laba potvrdilo je kupovinu FinSpy proizvoda kompanije FinFisher 2014. godine, ali i potkrepilo sumnje da je Vlada Srbije korisnik Predator alata kompanije Intellexa, što je zaključeno uz saradnju sa Guglovim timom za analizu pretnji 2022. godine.⁴⁷

Vredi izdvojiti dva slučaja upotrebe špijunskih softvera u Srbiji, kako zbog postojanja pouzdanih dokaza, tako i zbog identiteta samih

meta targetiranog nadzora. Upotreba sofisticiranijeg špijunskog softvera Pegasus potvrđena je u najmanje dva dokumentovana slučaja. Prvi slučaj zabeležen je mesec dana pre izbora u Srbiji 2023. godine, kada je dvoje pripadnika civilnog društva dobilo upozorenje kompanije Apple da su potencijalne mete državno sponzorisanih tehničkih napada. Pošto se upozorenje pokazalo osnovanim, SHARE Fondacija je u saradnji sa organizacijama Access Now i Amnesty International utvrdila da su na uređajima pronađeni tragovi pokušaja infekcije koji su imali obeležja ranijih napada Pegasus alatom preko ranjivosti u HomeKit funkcionalnosti iPhone uređaja.⁴⁸

Drugi zabeležen slučaj odnosi se na pokušaj napada špijunskim softverom Pegasus iz 2025. godine usmeren ka istraživačkim novinarkama portala BIRN Srbija. Napad je analizirala i potvrdila organizacija Amnesty International, a organizovan je kao „1-klik“ napad, kroz sumnjivu poruku poslatu preko aplikacije Viber sa nepoznatog broja iz Srbije.⁴⁹

NOVISPY

Slučaj koji je privukao najviše pažnje stručnjaka i javnosti u Srbiji jeste dokazana nezakonita upotreba špijunskog softvera NoviSpy protiv novinara, aktivista i pripadnika civilnog društva, zabeležena u izveštaju organizacije Amnesty International.⁵⁰ Stručnjaci ove organizacije pouzdano su utvrdili da su srpska policija i Bezbednosno-informativna agencija rutinski koristili novi tip špijunskog alata NoviSpy uz zloupotrebu alata za digitalnu forenziku, UFED, izraelske kompanije Cellebrite. Mete su bile inficirane špijunskim softverom tokom informativnih razgovora, u momentima kada su im uređaji bili oduzeti ili privremeno van nadzora. Nakon što su pripadnici policije ili BIA došli u posed telefona, korišćen je alat za digitalnu forenziku kako bi se uređaji

prisilno otključali i preuzeli postojeći i obrisani podaci, a zahvaljujući ostvarenom fizičkom pristupu instaliran je softver nazvan NoviSpy.⁵¹

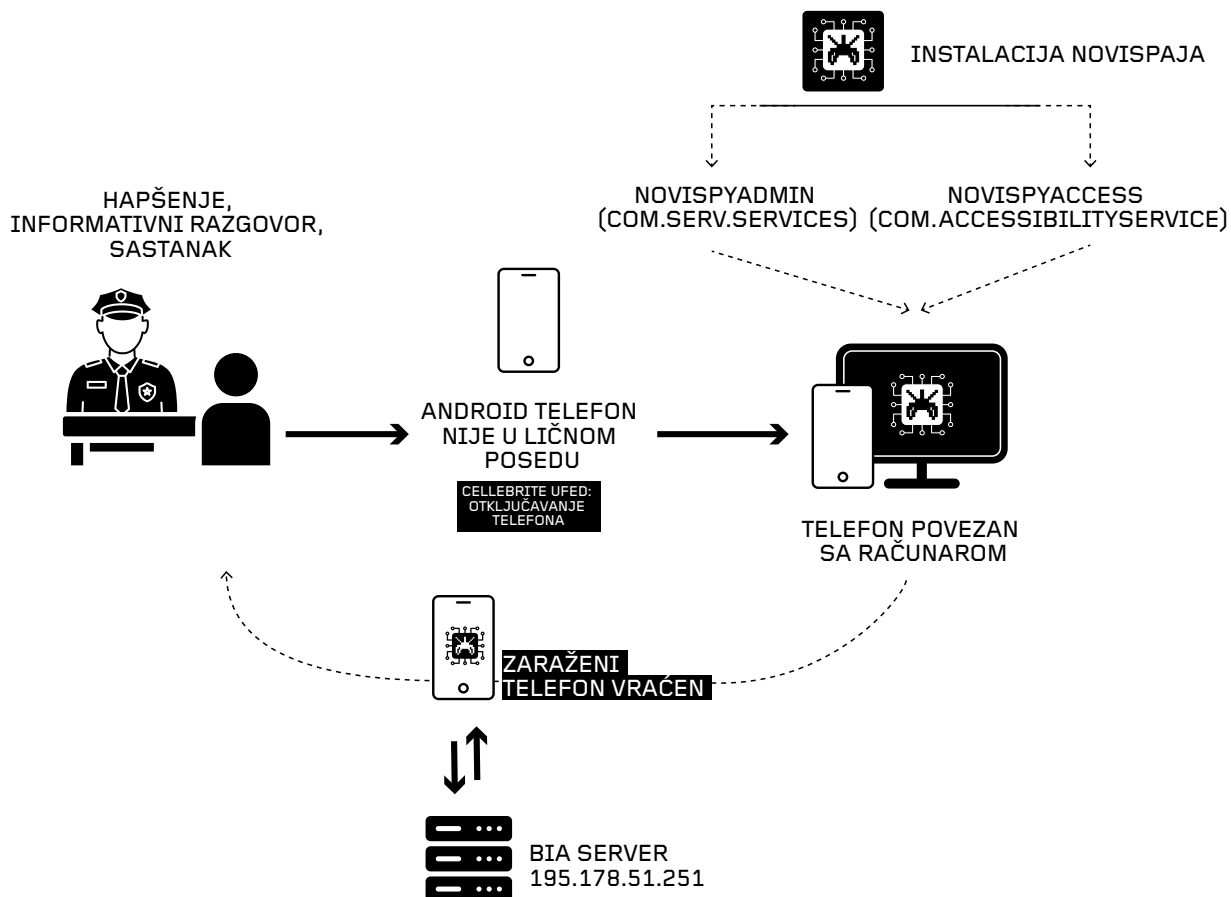
Uprkos reakciji civilnog društva i podnetim krivičnim prijavama protiv NN osoba zaposlenih u policiji i BIA Tužilaštvu za visokotehnološki kriminal povodom slučaja NoviSpy, nezakonito špijuniranje građana se nastavilo. U februaru 2025. godine potvrđen je još jedan slučaj pokušaja instaliranja nepoznate Android aplikacije, za koju se veruje da je bila deo paketa špijunskog softvera NoviSpy, ovog puta na telefon aktiviste i studenta Univerziteta Union.⁵² Međutim naknadnom analizom pronađeni su samo forenzički tragovi uspešnog korišćenja alata Cellebrite koji je eksfiltrirao sve podatke sa uređaja studenta. Sverasprostranjenija upotreba špijunskih softvera dešava se paralelno sa povećanom fizičkom i digitalnom državnom represijom koje se javila kao posledica masovnih protesta u Srbiji. U prethodnih nekoliko godina građani su svoje nezadovoljstvo izražavali na brojnim protestima protiv režima, a trenutno je u toku najveći i najmasovniji talas protesta predvođen studentima univerziteta širom Srbije, zbog čega najnoviji slučaj instalacije špijunskog softvera predstavlja još jedan pokušaj zastrešivanja, represije i gušenja mirnih i demokratskih protesta.⁵³

Za razliku od alata za presretanje komunikacije i digitalnu forenziku, čija je primena u specifično određenim slučajevima zakonski regulisana, upotreba špijunskih softvera u Srbiji ne samo da nije pravno dozvoljena, već predstavlja krivično delo. Krivični zakonik Republike Srbije ovakvu praksu prepoznaje kao kršenje člana 300,

koji se odnosi na pravljenje i unošenje računarskih virusa, i člana 302, koji se odnosi na neovlašćeni pristup zaštićenim računarima, mrežama i elektronski obrađenim podacima.⁵⁴ Dodatno, zbog svoje izrazito intruzivne i neselektivne prirode, špijunski softveri narušavaju i osnovna načela neophodnosti i srazmernosti propisana Zakonom o zaštiti podataka o ličnosti.⁵⁵

Špijunski softveri ugrožavaju ljudska prava direktno i indirektno kroz tzv. efekat zebnje. Najdirektnije, upotreba špijunskih softvera ugrožava pravo na privatnost i zaštitu podataka o ličnosti targetirane osobe, ali i svih lica povezanih sa tom osobom čiji se podaci mogu naći na zaraženom uređaju, uključujući maloletna lica i druge članove porodice, advokate, novinarske izvore, kolege i prijatelje.

Društveni uticaj špijunskog softvera ide još dalje. Njegove intruzivne mogućnosti doprinose širem efektu zebnje koji narušava javno poverenje i ugrožava slobodu. Strah da bilo ko može postati meta targetiranog nadzora, a naročito špijunskih softvera, ima dalekosežne posledice, ograničavajući sposobnost pojedinaca da ostvaruju zakonski zaštićena prava. Pretnja nadzorom guši slobodu izražavanja, slobodu udruživanja i okupljanja, kao i druge osnovne slobode, jer se pojedinci mogu cenzurirati ili uzdržavati od učestvovanja u javnom diskursu kako ne bi postali mete državne represije.



Ubrzani razvoj industrije špijunskih softvera i njihova učestala upotreba za potrebe državnih organa, dovela je do porasta tražnje za sličnim, komercijalnim rešenjima dostupnim široj javnosti. Razvijeni pod izgovorom veće bezbednosti i produktivnosti, rešenja kao što su aplikacije za praćenje i nadgledanje aktivnosti intimnih partnera (stalkerware) i dece (parentalware), ali i kontrolu i nadgledanje zaposlenih na radnom mestu (bossware) predstavljaju sve veću pretnju po bezbednost i privatnost.⁵⁶ Pored rasta popularnosti ovih aplikacija na globalnom tržištu i privatnoj upotrebi, mnoge kompanije, ali i državne institucije u Srbiji implementirale su ih u svoje poslovne sisteme.

Republički geodetski zavod, prema nalazima dobijenim istraživanjem dokumenata prikupljenih na sajtu portala javnih nabavki, već nekoliko godina unazad plaća održavanje jednog takvog softvera, Honesty, po ceni od preko osam miliona dinara.⁵⁷ Honesty softver, koji je razvila beogradska kompanija Melon

interactive, „vrši merenje performansi zaposlenih na računarima i daje odgovore na pitanja, ko koliko radi, šta radi i da li stvarno radi“. Iako veb-sajt kompanije ne pruža informacije o svim funkcijama softvera, navodi se da on prati vreme provedeno u radu, sajtove koji zaposleni posećuju na računaru, vreme koje zaposleni provode na društvenim mrežama i „konkretnim projektima“, uz napomenu da softver ne ugrožava privatnost zaposlenih.⁵⁸ Jasna kontradiktornost koja proizlazi iz te tvrdnje, ali i navodi pojedinih zaposlenih da je saglasnost za korišćenje ovog softvera bila obavezna za pristup samom računaru, te obavljanju samih radnih zadataka, predstavlja vrlo zabrinjavajuću sliku.

Izazovi upotrebe naprednih tehnologija za prikupljanje podataka

Upotreba naprednih tehnologija za prikupljanje podataka u javnom sektoru može

doprineti unapređenju javnih usluga, naročito u demokratskim sistemima koji se odlikuju snažnom vladavinom prava. Međutim, u Srbiji njihova primena otvara prostor za značajne rizike, pre svega po privatnost i bezbednost podataka, posebno kada se tehnologije koriste u svrhu nadzora.

Nadzor je oduvek predstavljao ključni mehanizam za održavanje kontrole i stabilnosti društvenih sistema. U prošlosti, nadzor je bio ograničen ljudskim sposobnostima, tehnološkim mogućnostima i dostupnim resursima. Razvojem tehnologije značajno su proširene mogućnosti i alati nadzora, a tehnologija je postala centralno sredstvo kontrole i moći. U savremenom društvu, usled masovnog i u nekim slučajevima automatskog prikupljanja podataka o ličnosti u gotovo svim sferama života, formira se narativ o uzaludnoj borbi za privatnost u dobu posle privatnosti.⁵⁹ Istovremeno, sve veće zadiranje u privatnost, pogotovo u slučajevima kada to čine državni organi, pravda se bezbednosnim potrebama borbe protiv kriminala i terorizma.

U takvom kontekstu, koncept društva nadzora (surveillance society) odnosi se na svako društvo u kojem su administrativni i kontrolni procesi zavisni od informacionih tehnologija.⁶⁰ Nadzor nije isključivo tehnološki problem, jer je tehnologija samo alat, već leži u načinu njegovog sprovođenja i svrhe, kao i upotrebe tehnologije kao sredstva uspostavljanja i održavanja društvene kontrole i moći. Posebno, nadzor postaje problematičan onda kada

služi za jačanje asimetrične moći, čime se produbljuju postojeće društvene, političke ili ekonomske razlike.⁶¹

Mapiranje naprednih tehnologija u Srbiji pokazuje njihovu sve veću zastupljenost u sferi nadzora. Država i njene institucije sve intenzivnije koriste nove tehnološke mogućnosti iako neretko za to ne postoji pravno utemeljenje, svrha upotrebe nije dovoljno i jasno obrazložena, a nedefinisani opseg i granice primene tehnologije sve učestalije podrivaju osnovna ljudska prava i slobode. Primer Srbije ukazuje da društveni razvoj i napredak nije neposredno tehnološki determinisan, već da upotreba naprednih tehnologija, posebno u sferi nadzora, mora biti zakonita i usklađena sa ljudskim pravima, kao i da svaki vid njene zloupotrebe mora biti sankcionisan. U suprotnom, tehnologija u rukama države može biti neograničeni resurs koji vodi ka totalnom društvenom nadzoru.

Pregled tehnologija u sferi nadzora u Srbiji ukazuje na paralelan tok uvođenja naprednih tehnoloških rešenja za masovni i targetirani nadzor. Komplementarna primena raznovrsnih alata za nadzor funkcioniše na principu veće nadzorne efikasnosti, a sve pod ključnim argumentom bezbednosti. Međutim, princip bezbednosti pravnom sistemu Srbije morao bi da bude usklađen sa principima privatnosti i zaštite podataka o ličnosti koje ove tehnologije značajno narušavaju.

Druga problemska paralela upotrebe tehnologija za nadzor odvija se između transparentnosti i tajnosti. Posebno je zabrinjavajuće to što ove tehnologije koriste uglavnom bezbednosne institucije, koje nabavke opreme sprovode sa oznakom tajnosti, što ceo proces čini vrlo netransparentnim i omogućava upotrebu i onih tehnologija koje mogu biti nesrazmerno štetne po ljudska prava i slobode.

Zatim, imperativ efikasnosti ovih tehnologija ne znači nužno i efikasnost kontrole njihove upotrebe. Civilno-demokratska kontrola službi bezbednosti koja po zakonu pripada najvišem

predstavničkom telu, Narodnoj skupštini, često se svodi na proceduralne zadatke koji se obavljaju iza zatvorenih vrata, pri čemu izostaje neophodna rasprava o suštinskim pitanjima vezanim za bezbednost građana Srbije. Indicije protivpravnog postupanja policije i službi bezbednosti se u najvećoj meri odbacuju bez istražnog postupka i šire javne debate, a njihovo delovanje se pravda „ovlašćenjima“ koja proizilaze iz široko postavljene pravne formulacije „zaštite nacionalne bezbednosti“. Narodna skupština Srbije ne samo da ne obavlja ulogu delotvornog kontrolora policije i bezbednosnih službi, već često funkcioniše kao instrument za zvanično menjanje „pravila igre“ i dalje slabljenje mehanizama nadzora nad mogućim zloupotrebama u sektoru bezbednosti.⁶²

Nedelotvorni mehanizmi kontrole u slučaju Srbije takođe ukazuju na širok prostor mogućnosti zloupotrebe ovih tehnologija u skladu sa partikularnim interesima onih koji raspolažu monopolom nad sektorom bezbednosti, a mimo pravnih i etičkih normi. Najzad, zatvaranje kruga totalnog nadzora u društvenom ambijentu kakav je trenutno u Srbiji odvija se na jačanju kulture nadzora i kontrole koju generiše država i uspostavlja kao princip koji se preliiva u komercijalni sektor, sferu privatnosti i slično.

Velike konceptualne dileme upotrebe naprednih tehnologija za nadzor u Srbiji dodatno se komplikuju kada da se sagleda mehanizam ovih tehnologija, kojima su ključni resurs podaci o ličnosti. Kako se ti podaci prikupljaju, analiziraju, čuvaju, štite i cirkulišu, ko njima ima pristup, u koje svrhe se sve mogu koristiti i sa kakvim posledicama, predstavljaju maglovito polje pitanja na koje država do sada nije pokazala ni principijelnu ni praktičnu odgovornost.

Sve navedeno ukazuje da proces prikupljanja podataka u javnom sektoru više ne predstavlja samo tehničko pitanje, već duboko političko i društveno polje u kojem se prepliću interesi države, privatnog sektora i bezbednosnih struktura. Napredne tehnologije za masovni i ciljani nadzor omogućavaju stvaranje ogromnih

količina informacija o građanima, ali ostaje nejasno gde ti podaci završavaju, na koji način se analiziraju i u koje svrhe se dalje koriste. Upravo od načina na koji se prikupljeni podaci transformišu, analiziraju i povezuju zavisi njihova stvarna uloga, bilo da se koriste za unapređenje javnih politika i usluga, ili za potrebe kontrole i profilisanja stanovništva. U narednom poglavlju razmatra se kako se podaci prikupljeni kroz različite napredne tehnologije dalje analiziraju, upravljaju i pretvaraju u resurs koji oblikuje odlučivanje u javnom sektoru.

Analiza podataka i automatizovano odlučivanje

Kao što je već pomenuto, podaci u svom izvornom, sirovom obliku retko imaju neposrednu vrednost za javni sektor. Prava vrednost se najčešće ostvaruje tek kada se podaci strukturiraju, obrađuju i interpretiraju. Upravo zbog toga faza analize podataka predstavlja centralni deo životnog ciklusa podataka i najčešće je prepoznata u svim modelima upravljanja podacima. Njena ključna uloga je transformacija velikih količina prikupljenih informacija u korisna saznanja koja mogu oblikovati odluke i politike u javnom sektoru. U ovoj fazi primenjuju se različiti napredni tehnički sistemi, uključujući sisteme za analizu velikih podataka (big data), mašinsko učenje i veštačku inteligenciju. Krajnji rezultat ovog procesa su nova saznanja, otkrivanje obrazaca i trendova, interpretacije i često kreiranje novih baza podataka, koje postaju unosna jedinica za naredne korake automatizovanog odlučivanja, gde se rezultati analize direktno koriste za donošenje odluka u javnom sektoru, često uz minimalnu ljudsku intervenciju.⁶³

Mnoge državne institucije koriste manje ili više napredne tehnologije za analizu velikih skupova podataka. Kao i u fazi prikupljanja, i u fazi analize podataka dominiraju nadležni organi u oblasti bezbednosti i to primarno MUP. Situacija je nešto drugačija kada pogledamo institucije koje vrše analizu podataka u svrhe automatizovanog odlučivanja gde se ističu državne institucije u oblasti socijalne zaštite, pravosuđa, trgovine, zdravstva, obrazovanja i energetike. v

Uprkos činjenici da upotreba kamera i softvera sa mogućnostima biometrijskog prepoznavanja lica nema utemeljenje u pravnom sistemu Srbije, prethodno kupljene i postavljene Huawei kamere se i dalje nalaze na preko 800 lokacija u Beogradu, dok se sistemi za biometrijsku

analizu video nadzora istog proizvođača i dalje nalaze u posedu MUP-a. Pored toga, ovo ministarstvo nastavilo je da iskazuje interesovanje za nabavku naprednih tehničkih softvera za prepoznavanje lica sa analizom velikih skupova podataka. Tako se MUP dovodi u vezu sa kompanijama poput Magnet Forensics, koja proizvodi poznati alat Griffeye Analyze,⁶⁴ odnosno ClearviewAI⁶⁵ koja proizvodi slična rešenja.

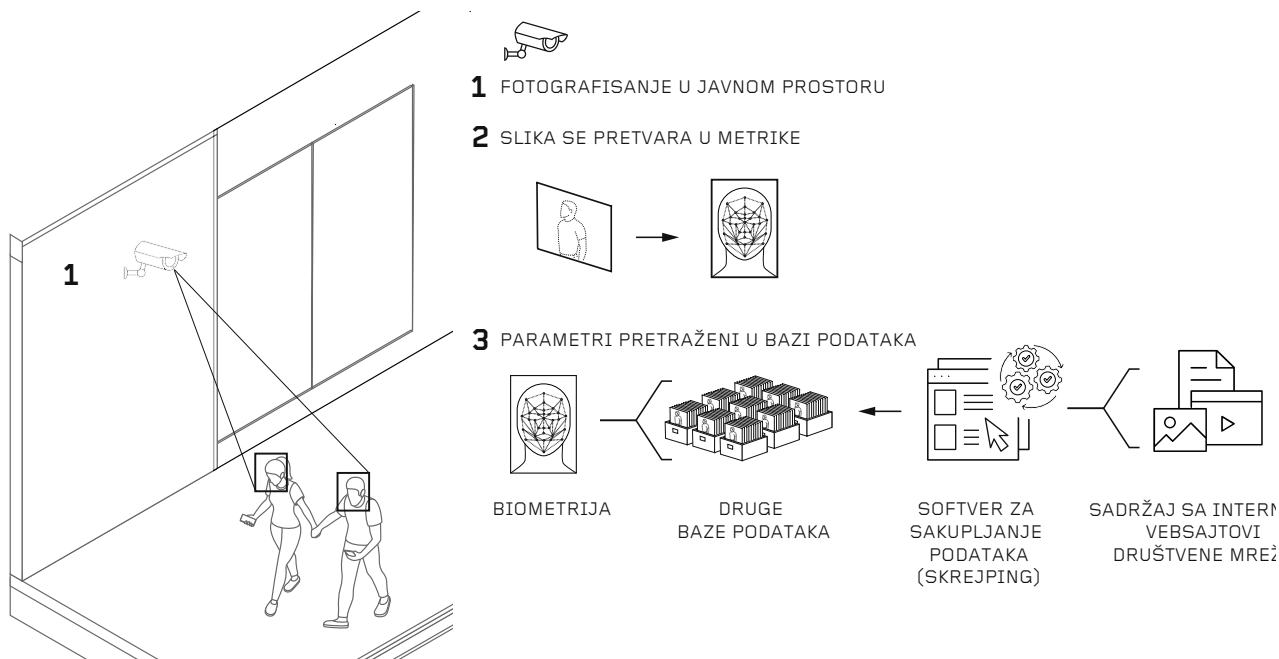
Ovi softveri funkcionišu tako što automatski obrađuju veliki broj slika i video-zapisa i upoređuju lica ili objekte sa drugim izvorima podataka, uključujući informacije pronađene na internetu. U praksi, oni mogu da identifikuju osobu na slici ili snimku i povežu taj identitet sa javno dostupnim sadržajima, povezujući inače teško povezive skupove podataka. Iako razvijeni u svrhu otkrivanja i sprečavanja seksualnog zlostavljanja dece, karakteristike ovih softvera čine verovatnim i praćenje aktivista ili demonstranata i njihovu identifikaciju, pogotovo u državama koje se ne odlikuju visokim stepenom vladavine prava i demokratskog nadzora sektora bezbednosti.⁶⁶

CLEARVIEWAI

Američka kompanija ClearviewAI proizvodi tehnološka rešenja bazirana na veštačkoj inteligenciji za nadležne organe širom sveta. Ovaj softver automatski prikuplja podatke u procesu onlajn skrejpinga podataka sa društvenih mreža (online social media scraping) i drugih onlajn resursa i skladišti ih, kreirajući bazu podataka od preko 60 milijardi slika, što predstavlja jednu od najvećih baza podataka slika sa interneta. Na kraju, softver koristi algoritam koji spaja lica sa slike koja je ubačena u ClearviewAI sa svim slikama tog lica koje su pronađene na internetu sa linkovima koji ukazuju na to odakle je slika preuzeta.⁶⁷

Ovakvo automatsko prikupljanje biometrijskih podataka predstavlja ozbiljnu pretnju po ljudska prava, pogotovo pravo na privatnost. Upravo zbog toga, brojne organizacije civilnog društva iz država širom sve-

ta, pokrenule su sudske postupke protiv kompanije, od kojih je većina bila uspešna, a rezultati su bili brisanje podataka o građanima specifičnih zemalja i novčano kažnjavanje kompanije.⁶⁸



MUP, pored naprednih tehničkih softvera sa sposobnostima biometrijskog nadzora, zainteresovan je i za tehnologije za prikupljanje obavestajnih podataka iz otvorenih izvora (OSINT), poput rešenja kompanija Maltego,⁶⁹ Social Links,⁷⁰ Mozenda⁷¹ i Cognyte.⁷² Pored MUP-a, ove alate nabavilo je i nekadašnje Ministarstvo trgovine, turizma i telekomunikacija za potrebe tržišne inspekcije i Poreske uprave, verovatno za potrebe praćenja, nadzora i otkrivanja nepravilnosti u poslovanju i poreskim obavezama, iako mogućnosti ovih alata daleko prevazilaze potrebe ovih institucija.

Ovi alati omogućavaju prikupljanje i objedinjavanje informacija iz različitih izvora, analizu i vizualizaciju veza i obrazaca između ljudi, organizacija i aktivnost uz pomoć veštačke inteligencije, a pojedini sistemi takođe koriste aktivne metode praćenja i kreiranja lažnih profila, što znači da prelaze iz same analize podataka u invazivni nadzor.⁷³ Iako ove tehnologije prikupljaju ogromnu količinu podataka iz različitih

izvora, takvi podaci u sirovom obliku nemaju posebnu vrednost i obimom daleko prevazilaze mogućnosti ljudske obrade. Tek kroz procese objedinjavanja, filtriranja i analize, uz podršku algoritama i veštačke inteligencije, oni dobijaju smisao i praktičnu upotrebljivost.

Kada je reč o naprednim tehničkim sistemima za analizu podataka u cilju automatizacije odlučivanja, oni se najčešće primenjuju radi povećanja efikasnosti i brzine rada javnog sektora, naročito u slučajevima kada se rukuje velikim količinama podataka koje nadilaze ljudske kapacitete analize. Međutim, primena ovakvih sistema mora ići dalje od puke potrebe za digitalizacijom i zahteva visok stepen transparentnosti, odgovornosti i zaštite prava građana, jer algoritamske odluke mogu imati direktan i neposredan uticaj na živote pojedinaca, a greške ili zloupotrebe u procesu odlučivanja mogu dovesti do ozbiljnih posledica po privatnost i pravnu sigurnost građana.

U oblasti pravosuđa u Srbiji se primenjuju napredni tehnički sistemi za analizu podataka među kojima se ističu sistemi SIPRI, SIPRES, SAPO i SAPA. SIPRI predstavlja centralizovanu platformu za vođenje predmeta i sudskih registara u privrednim sudovima, oslanjajući se na automatizovani sistem vođenja predmeta (AVP) i povezujući se sa drugim internim i eksternim bazama podataka. Sličnu funkciju ima SIPRES, koji centralizuje informacije o predmetima u prekršajnim sudovima, beleži sve radnje korisnika i omogućava razmenu podataka sa drugim pravosudnim servisima, uključujući i javno dostupne registre neplaćenih novčanih kazni.⁷⁴

SAPO, centralizovani elektronski sistem za upravljanje predmetima javnih tužilaštava, omogućava objedinjenu evidenciju svih podataka o predmetima u tužilaštvima, uključujući informacije o radnjama tužilaca, statusu predmeta i povezanim dokumentima, čime se podržava praćenje i upravljanje procesima donošenja odluka u tužilaštvima.⁷⁵

Sistem SAPA, kojim upravlja Uprava za izvršenje krivičnih sankcija, objedinjeno vodi podatke o licima lišenim slobode i ustanovama za izvršenje kazni, prateći kompletnu proceduru od prijema zatvorenika, preko izdržavanja kazne, do puštanja na slobodu. SAPA standardizuje procedure za različite tokove rada, uključujući tretman maloletnih prestupnika, izvršenje obaveznih psihijatrijskih mera i programe lečenja zavisnosti.⁷⁶

Iako se u oblasti pravosuđa za sada primenjuju samo napredne tehnologije za analizu velikih skupova podataka, postoji tendencija Ministarstva pravde za automatizacijom određenih procesa, poput raspodele predmeta sudijama.⁷⁷

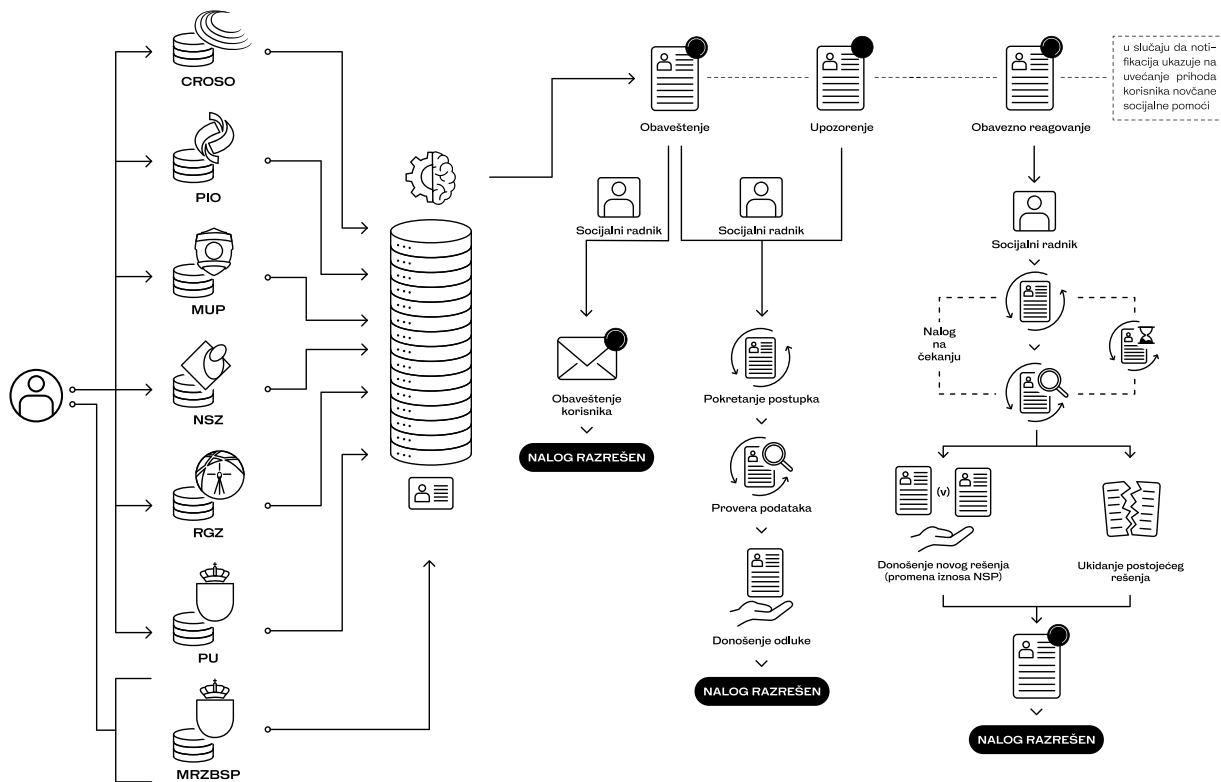
SISTEM SOCIJALNE KARTE

Sistem Socijalne karte predstavlja jedan od najkontroverznijih slučajeva upotrebe tehnologije u držav-

nom sektoru u Srbiji. Zakon o Socijalnoj karti donesen je 2021. godine i zamišljen je radi „automatizacije postupaka i procesa vezanih za postupanje u oblasti socijalne zaštite“ kako bi se sprečila zloupotreba sistema.⁷⁸ Sistem funkcioniše tako što uz pomoć algoritma sabira više od 130 kategorija podataka lica, korisnika socijalne pomoći, kao i podatke lica povezanih sa njima, na osnovu čega, svakom korisniku pojedinačno, kreira Socijalnu kartu koja određuje da li će to lice primati socijalnu pomoć ili ne.⁷⁹

Međutim, kako tvrde mnoge organizacije civilnog društva, posredni cilj uvođenja ove tehnologije bio je da se odstrani što je moguće više ljudi iz sistema socijalne zaštite. Činjenica je da se nakon početka primene zakona broj korisnika sistema socijalne karte smanjio za 10 odsto ili za više od 22.000, iako se broj siromašnih nije značajno menjao u tom periodu. Ono što algoritam ne može da ustanovi jesu sve one informacije koje ne pišu u bazama podataka, a za koje socijalni radnici, kao stručnjaci za socijalni rad, znaju u praksi. Zbog toga su lica koja su imala jednokratna primanja, minimalne prihode od prodaje sekundarnih sirovina ili lica koja su formalno povezana sa drugim licima sa određenim prihodom (bez procene u kakvom su odnosu ta lica) ostajala bez socijalne zaštite i bez mogućnosti uvida u odluku ili žalbe na istu.⁸⁰ Evropski centar za prava Roma istakao je da su Romi u najvećoj meri isključeni iz sistema socijalne zaštite zbog primene ovog zakona.⁸¹

Jedna od ključnih osobina sistema Socijalne karte jeste njena povezanost sa širokim spektrom državnih registara. Socijalna karta funkcioniše kao



LEGENDA:

CROSO - Centralni registar obaveznog socijalnog osiguranja

CRS - Centralni registar stanovništva

MRZBSP - Ministarstvo za rad, zapošljavanje, boračka i socijalna pitanja

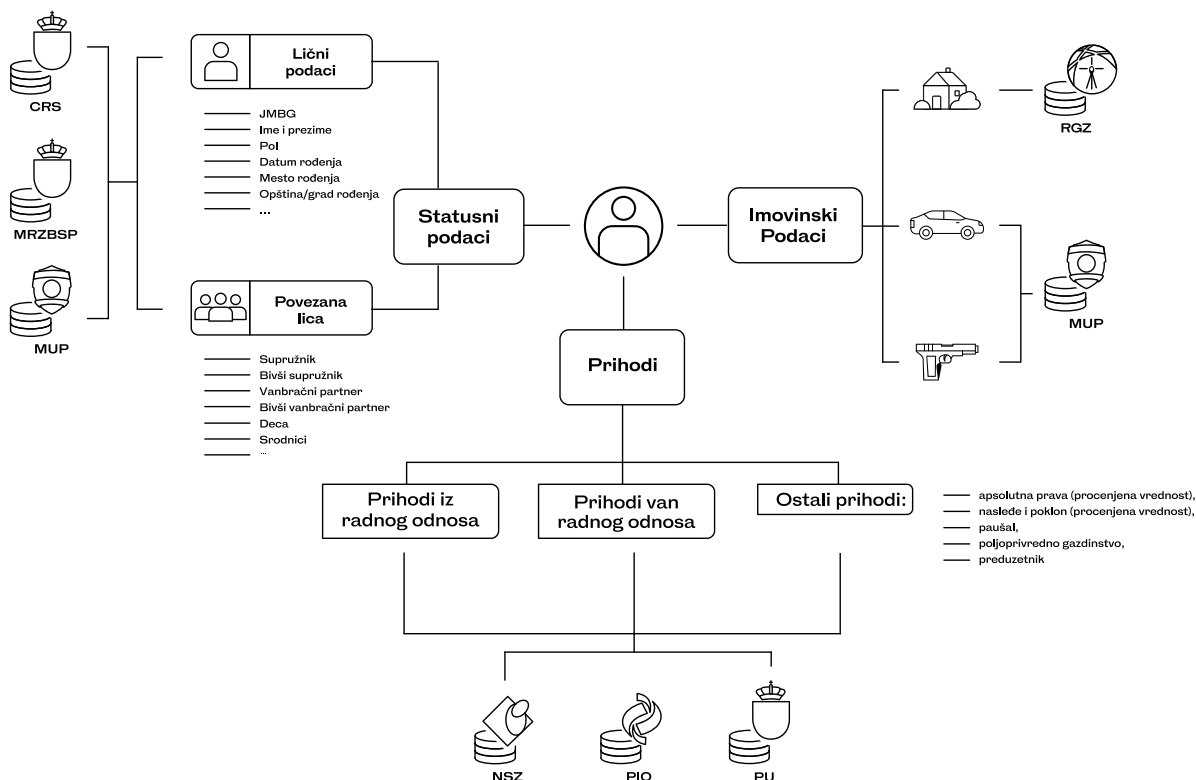
MUP - Ministarstvo unutrašnjih poslova

NSZ - Nacionalna služba za zapošljavanje

PIO - Republički fond za penzijsko i invalidsko osiguranje

PU - Poreska uprava

RGZ - Republički geodetski zavod



LEGENDA:

CROSO - Centralni registar obaveznog socijalnog osiguranja

CRS - Centralni registar stanovništva

MRZBSP - Ministarstvo za rad, zapošljavanje, boračka i socijalna pitanja

MUP - Ministarstvo unutrašnjih poslova

NSZ - Nacionalna služba za zapošljavanje

PIO - Republički fond za penzijsko i invalidsko osiguranje

PU - Poreska uprava

RGZ - Republički geodetski zavod

čvorište koje povremeno povlači podatke iz drugih informacionih sistema, ali im i prosleđuje nove informacije. Ministarstvo za rad, zapošljavanje, boračka i socijalna pitanja najavilo je dogradnju i modifikaciju sistema Socijalne karte i integraciju sa sistemima IS SOZIS, IS DD-RD, IS Boračko invalidske zaštite.⁸²

Sistem Socijalne karte izazvao je brojne kritike, od etičkih problema i dehumanizacije procesa koji zahteva razumevanje konteksta i ljudskih potreba, preko pitanja zaštite podataka o ličnosti i privatnosti, do netransparentnosti algoritama koji odlučuju o životima građana i potpune neodgovornosti u slučaju grešaka.⁸³ Ne samo da nadležno ministarstvo ne adresira ove kritike, već se planira proširenje sistema povezivanjem sa drugim bazama podataka. Imajući u vidu intruzivnost ovog sistema, kao i realne, jasno vidljive posledice koje za sobom ostavlja, pre svega isključivanje hiljada najugroženijih iz sistema socijalne zaštite, neophodno je insistirati na transparentnosti procesa i na značajnijoj ljudskoj intervenciji.

Digitalizacija zdravstvenog sistema Srbije zaživela je tokom pandemije Covid-19, kada su stari sistemi dobili dodatne funkcije, dok su zbog novih potreba razvijana nova rešenja. Jedna od prvih novina u oblasti zdravstva je portal **e-Zdravlje**, koji je prvobitno služio samo kao kanal komunikacije između građana i zdravstvenih institucija. Međutim nakon što je proglašena pandemija, portal je dobio dodatne funkcije namenjene praćenju poštovanja izrečenih epidemioloških mera, pri čemu je portal postao još jedan sistem nadzora. Svi građani, ali i strani državljani koji su doputovali u Srbiju bili su u obavezi da se registruju na e-Zdravlje portalu.⁸⁴

Poreska uprava Republike Srbije, tačnije Odeljenje za strateške rizike i Departman za matematiku i informatiku ispred Prirodno-matematičkog fakulteta Univerziteta u Novom Sadu 2021. godine potpisali su saradnju na istraživačkom projektu „Detektovanje rizika od izbegavanja plaćanja poreza na dohodak građana na osnovu odgovarajućih metoda upotrebom veštačke inteligencije”.⁸⁵ Iako i dalje ne postoje konkretne i javno dostupne informacije o načinu funkcionisanja ovog sistema, veruje se da on funkcioniše slično drugim evropskim sistemima koji ukrštaju finansijske podatke obveznika i otkrivaju anomalije i neprijavljene prihode. Takvi programi u sistem veštačke inteligencije unose velike količine podataka, poput poreske prijave, podatke o bankovnim računima, registracije nekretnina i vozila, vlasništvo nad preduzećima i slično, nakon čega se prepoznaju sumnjivi obrasci.⁸⁶ Analizom velikih baza podataka razvijaju se modeli za razotkrivanje osumnjičenih za izbegavanje plaćanja poreza na dohodak ili lica za koja postoji rizik da u budućnosti počine to delo.⁸⁷

Državno **elektroprivredno** preduzeće, Elektroprivreda Srbije (EPS), u saradnji s kompanijom Microsoft i domaćom IT kompanijom Informatika A.D, primenila je sistem baziran na veštačkoj inteligenciji koji za automatizaciju prognoze potrošnje električne energije.⁸⁸ Cilj primene je da se istorijski i trenutni podaci o potrošnji objedine kako bi se dobile pouzdane prognoze buduće tražnje.⁸⁹

Problem analize velikih skupa podataka i automatizacije donošenja odluka

Problemi koji nastaju u fazi prikupljanja podataka prenose se na naredne faze analize i automatizovanog odlučivanja, gde dobijaju novu dimenziju rizika. U trenutku kada se podaci, prikupljeni često bez adekvatne pravne osnove ili informisanog pristanka, unesu u složene algoritamske sisteme, oni postaju deo procesa koji je građanima uglavnom nevidljiv, ali koji može imati direktan uticaj na njihova prava. Na taj način, čitav ciklus, od prikupljanja, preko analize, do automatizovanog odlučivanja, funkcioniše kao zatvoreni sistem u kojem se odgovornost teško može pratiti i utvrditi.

U tom smislu, poseban problem u javnom sektoru predstavlja kvalitet prikupljenih podataka. Kvalitetni podaci su tačni, potpuni, ažurni, dosledni, standardizovani i dovoljno precizni. Oni omogućavaju pouzdano vođenje politika, upravljanje procesima i pružanje javnih usluga, dok podaci lošeg kvaliteta mogu dovesti do pogrešnih zaključaka, neefikasnog odlučivanja i narušavanja poverenja građana.⁹⁰ U slučaju Srbije, čini se da je primarni cilj prikupljanje što većeg broja podataka, a ne nužno prikupljanje kvalitetnih podataka. To znači da se podaci često razlikuju po kvalitetu, iako se uglavnom objedinjavaju u iste baze i prolaze kroz iste analitičke procese, što čini pouzdanost i relevantnost tih podataka upitnom.

Iz ugla javnog sektora, napredni tehnički sistemi, čija se uloga jasno vidi u procesu analize podataka i automatizovanog odlučivanja, su prvenstveno zamišljeni kao instrumenti za unapređenje efikasnosti i kvaliteta usluga, olakšavanje rada zaposlenih i povećanje dostupnosti usluga građanima. Na prvi pogled, ovakav cilj deluje jednostavno i opravdano, ali snažna strateška usmerenost ka ubrzanju digitalizaciji često rizike njihove upotrebe potiskuje u drugi plan. Međutim, iz perspektive pravne države i ljudskih prava, nekritička i ubrzana digi-

talizacija bez jasnog pravnog okvira i etičkih standarda, naročito u uslovima slabe vladavine prava i izraženog nepoverenja građana, otvara ozbiljne pretnje po bezbednost i privatnost, dok se u fokusu nalaze problemi transparentnosti i odgovornosti.

Od samog početka, netransparentnost procesa digitalizacije, u kombinaciji sa upotrebom naprednih tehničkih sistema u radu organa bezbednosti, predstavlja značajan izazov. Građani često nisu adekvatno informisani o implementaciji i načinu funkcionisanja ovih sistema, a u mnogim slučajevima imaju pristup samo onim podacima koje državne institucije koriste da javno demonstriraju tehnološki napredak Srbije. Suštinske informacije postaju dostupne javnosti tek kroz rad istraživačkih novinara ili organizacija civilnog društva. Takav pristup stvara konfuziju, zabrinutost i nepoverenje građana, posebno u situacijama kada su njihova prava i podaci ugroženi primenom ovih tehnologija. Posebno zabrinjava praksa organa bezbednosti da ove sisteme koriste za nadzor građana bez odgovarajuće pravne osnove i njihovog znanja. Na kraju, nedostatak transparentnosti otvara i brojne mogućnosti zloupotrebe.

Dodatni i sve ozbiljniji rizik odnosi se na potencijalnu diskriminaciju i algoritamsku pristranost u procesima automatizovanog odlučivanja. Budući da sistemi veštačke inteligencije uče iz postojećih podataka, oni ne samo da reprodukuju već i pojačavaju postojeće društvene nejednakosti i stereotipe sadržane u tim podacima. Na taj način, odluke o zapošljavanju, dodeli socijalne pomoći, određivanju rizika od kriminalnog ponašanja ili ocenjivanju sudskih predmeta mogu postati pristrasne i diskriminatorne prema određenim grupama građana, na osnovu pola, etničke pripadnosti, socioekonomskog statusa ili političkih uverenja. U kontekstu Srbije, gde pravni i institucionalni mehanizmi zaštite od diskriminacije i dalje pokazuju ozbiljne slabosti, ovakvi sistemi mogu značajno produbiti postojeće društvene nejednakosti i dovesti do nevidljive, ali sistemske

diskriminacije.

Sledeće pitanje koje se nameće upotrebom ovih tehnologija je pitanje odgovornosti. Pre svega, odgovornost za adekvatnu edukaciju zaposlenih o načinu funkcionisanja sistema, ali i kako njima upravljati na bezbedan i ispravan način kako bi se predupredili i izbegli bezbednosni propusti koji mogu dovesti do ugrožavanja osetljivih podataka i privatnosti građana. Još značajnije je pitanje odgovornosti u pogledu adekvatnih kontrolnih mehanizama i mehanizama sankcionisanja odgovornih lica u slučaju bezbednosnih incidenata ili zloupotreba sistema. Brojni primeri curenja podataka jasno ukazuju da implementaciju i upotrebu naprednih tehnologija odlikuje izrazita neodgovornost zaposlenih, institucija i nadzornih organa, što samo dovodi do novih bezbednosnih incidenata, uz zanemarivanje važnosti zaštite osetljivih podataka građana, njihove privatnosti, i u krajnjoj liniji njihove bezbednosti.

Koren ovih problema predstavlja neadekvatna osnova primene naprednih tehničkih sistema jer je izostala sveobuhvatna javna rasprava o etičkim principima upotrebe ovakvih sistema u javnom sektoru koji prikuplja i analizira najosetljivije podatke građana. Takođe, izostao je rad na pravnom okviru koji bi, uz konsultaciju sa relevantnim akterima, sadržao jasne etičke i bezbednosne standarde, mehanizme nadzora i adekvatne sankcije za povredu prava. Postojeće probleme dodatno pogoršava nepoštovanje postojećeg pravnog okvira i izostanak procene rizika, ključne za sigurnu i odgovornu implementaciju ovih sistema.

Brza primena veštačke inteligencije i sistema pametnog odlučivanja dodatno opterećuje ovaj sistem, koji je već opterećen brojnim manama i propustima, povećavajući rizik po prava i slobode građana.

Završna faza životnog ciklusa podataka odnosi se na njihovu dalju upotrebu, arhiviranje ili brisanje, čime se krug upravljanja podacima formalno zatvara. Nakon što su podaci iskorišćeni

za analizu i automatizovano donošenje odluka, oni bi u skladu sa principima zaštite podataka trebalo da budu obrisani ili arhivirani u skladu sa jasno definisanim rokovima i svrhom obrade. U praksi javnog sektora u Srbiji, međutim, ova faza je najčešće potpuno netransparentna i nedovoljno regulisana. Ne postoje precizni mehanizmi koji obezbeđuju da se podaci građana po okončanju njihove upotrebe zaista brišu ili čuvaju na bezbedan način, niti postoji javni uvid u to ko im i pod kojim uslovima kasnije pristupa. Time se rizici iz prethodnih faza, masovnog prikupljanja, neadekvatne obrade i netransparentnog odlučivanja, prenose i na kraj ciklusa, produžavajući život podataka daleko izvan njihove prvobitne svrhe.

Odsustvo jasne politike arhiviranja i brisanja podataka ne samo da podriva poverenje građana u digitalne procese, već stvara i realnu opasnost od produženog nadzora, sekundarne upotrebe i zloupotrebe informacija. U praksi, podaci prikupljeni za jednu svrhu često se kasnije koriste za potpuno druge administrativne, bezbednosne ili komercijalne namene, čime se brišu granice između legitimne upotrebe i nadzora. Umesto zatvorenog i kontrolisanog ciklusa, podaci građana ulaze u stalnu cirkulaciju unutar institucionalnih i tehničkih sistema, što produžava rizike po privatnost i druga prava.

Kritična infrastruktura i skladištenje podataka

Kritična infrastruktura su sistemi, mreže, objekti ili njihovi delovi, čiji prekid funkcionisanja ili prekid isporuke roba odnosno usluga može imati ozbiljne posledice na nacionalnu bezbednost, zdravlje i živote ljudi, imovinu, životnu sredinu, bezbednost građana, ekonomsku stabilnost, odnosno ugroziti funkcionisanje Republike Srbije.⁹¹

Paralelno sa odvijanjem različitih faza životnog ciklusa podataka u javnom sektoru, od njihovog prikupljanja i analize, do upotrebe u procesima odlučivanja, odvija se i njihovo skladištenje i čuvanje u različitim oblicima. U zavisnosti od svrhe prikupljanja i analize, podaci se čuvaju u internim bazama institucija, centralizovanim državnim registrima ili na infrastrukturnim platformama kojima često upravljaju eksterni, pa i privatni akteri. Skladištenje podataka predstavlja ključnu tačku u lancu upravljanja, jer od načina na koji su podaci organizovani, zaštićeni i dostupni zavisi bezbednost čitavog sistema.⁹² Ipak, u praksi javnog sektora u Srbiji, čuvanje podataka karakteriše visok stepen netransparentnosti i nesrazmernosti. U velikom broju slučajeva, podaci se čuvaju duže nego što je to neophodno, bez jasnog plana arhiviranja ili brisanja, a ponekad i bez evidencije o tome ko im pristupa i u koje svrhe.

Na taj način, skladištenje podataka u javnom sektoru postaje „siva zona“ digitalizacije, faza koja se formalno podrazumeva, ali u kojoj se često gube tragovi o poreklu, svrsi i bezbednosti informacija. Umesto da bude garant kon-

tinuiteta i integriteta sistema, neadekvatno skladištenje podataka dodatno produžava rizike koji su nastali u ranijim fazama životnog ciklusa, čineći građane trajno izloženima mogućnostima nadzora, profilisanja i zloupotrebe njihovih informacija.

U Srbiji, skladištenje podataka državnih institucija bilo je prilično decentralizovano, najčešće u lokalne data centre samih institucija koje su mahom bile međusobno nepovezane.⁹³ Međutim, 2020. godine započet je proces centralizacije podataka, otvaranjem nove hardverske kritične infrastrukture – Državnog data centra u Kragujevcu koji predstavlja centralnu bazu za skladištenje podataka u čijem sklopu je smeštena „ključna informaciono-komunikaciona infrastruktura Republike Srbije“.⁹⁴

Pored fizičkog smeštanja opreme državnih organa, Državni data centar obezbeđuje i uslugu državnog klada (government cloud), koji omogućava organima javne uprave pristup infrastrukturnim resursima za skladištenje, obradu i razmenu podataka u okviru jedinstvenog digitalnog okruženja. Iako ovaj proces centralizacije donosi određene benefite u pogledu racionalizacije troškova i podizanja tehničke bezbednosti, istovremeno otvara i niz pitanja u vezi sa transparentnošću, pristupom, nadzorom i suverenitetom nad podacima, naročito u kontekstu poverljivih ili osetljivih informacija građana.⁹⁵

Nakon izgradnje Državnog data centra, država je intenzivirala kampanju usmerenu na institucije, pozivajući ih da svoje lokalne baze podataka premeste u centralni sistem. U jednom od obraćanja, predsednik Srbije je čak upozorio da bi zaposleni mogli snositi krivičnu odgovornost ukoliko ne izvrše migraciju podataka i dođe do tehničkih ili bezbednosnih incidenata.⁹⁶ Ipak, ovakve odluke treba donositi na osnovu sveobuhvatne procene rizika centralizacije podataka, a ne političkih pritisaka, naročito imajući u vidu da je sposobnost države da zaštiti podatke građana upitna, s obzirom na to da gotovo svake godine bar jedna držav-

na institucija pretrpi značajan sajber napad ili curenje podataka, dok odgovornost nadležnih za ove propuste gotovo uvek izostaje.

SAJBER NAPADI I CURENJE PODATAKA IZ DRŽAVNIH INSTITUCIJA I PREDUZEĆA

U prošlosti, Srbija se suočila sa brojnim slučajevima curenja podataka o ličnosti građana iz raznih državnih baza podataka usled napada hakera, ali i neodgovornosti zaposlenih u državnim institucijama. Srbija je pretrpela tri značajna ransomver napada, uključujući napad na JKP Informatika u Novom Sadu 2021. godine,⁹⁷ što je ujedno bio i prvi slučaj napada na kritičnu infrastrukturu u Srbiji, zatim napad na Republički geodetski zavod 2022. godine,⁹⁸ napad na informacione sisteme Elektroprivrede Srbije (EPS) 2023. godine,⁹⁹ i Ministarstvo pravde 2025. godine.¹⁰⁰

Brojni su i slučajevi neodgovornosti institucija koje prave velike sigurnosne propuste koji dovode do curenja podataka o građanima, kao što je bilo u slučaju Agencije za privatizaciju, kada je 2014. godine, sa zvaničnog sajta procurela tekstualna baza sa podacima o ličnosti preko pet miliona građana Srbije¹⁰¹ kao i u slučaju kada su korisničko ime i lozinka za pristup Informacionom sistemu Covid-19, koji je sadržao brojne zdravstvene podatke građana, osam dana bili javno dostupni na sajtu jedne zdravstvene ustanove.¹⁰² U velikom broju primera, ističe se i slučaj kada su procureli podaci sa portala „Moja srednja škola“, još jednog primera nespretno digitalizacije u prosveti, koji je namenjen završnom ispitu učenika osnovnih škola i upisu u srednje škole. Otkriveno je da je bilo moguće pristupiti imenima učenika kroz kod sajta. Na sajtu su

bili vidljivi podaci kao što su informacije o osnovnoj školi, ocenama i rezultatima koji su mogli biti povezani sa svakim učenikom kroz jedinstveni numerički identifikator (ID).¹⁰³

U okviru Državnog data centra, Kancelarija za IT i eUpravu uspostavila je *Centralni registar stanovništva* u kojem se nalaze „podaci o građanima iz svih državnih institucija, poput Ministarstva unutrašnjih poslova, Ministarstva državne uprave i lokalne samouprave, Centralnog registra obaveznog socijalnog osiguranja, a u ovom trenutku više od 160 različitih institucija pristupa Centralnom registru stanovništva kako bi se povukli ažurni podaci građana“.¹⁰⁴

Pored centralizacije podataka, u Državnom data centru smeštena su dva superkomputera koja čine jezgro Nacionalne platforme za veštačku inteligenciju, a koji podržavaju zadatke koji se intenzivno bave podacima, kao što su obuka naprednih modela mašinskog učenja, zaključivanje dubokog učenja i simulacije visoke vernosti.¹⁰⁵ Uprkos svojim naprednim mogućnostima, integracija superračunarskog sistema u nacionalne digitalne strategije takođe zahteva značajni stepen kontrole i odgovornosti. Potencijal za centralizovanu kontrolu nad podacima i analitičke moći izazivaju zabrinutost. Ako Nacionalna platforma ostane rezervisana za komercijalne, vladine ili interese vezane za nadzor, ona može ojačati postojeće asimetrije moći i ugroziti prava i slobode građana Srbije.¹⁰⁶

Evropska unija pruža značajnu podršku Srbiji u oblasti veštačke inteligencije, fokusirajući se na istraživanje, inovacije i razvoj digitalnih tehnologija kroz finansijske podsticaje, strateške projekte, poput izgradnje nove „AI fabrike“,¹⁰⁷ kao i institucionalnu podršku.¹⁰⁸ Međutim postavlja se pitanje u kojoj meri Evropska unija, kroz svoje programe podrške, uzima u obzir lokalni kontekst u kojem se inovacije često razvijaju uz zanemarivanje ljudskih prava i ograničenu institucionalnu odgovornost.

Fokus na razvoj infrastrukture koja olakšava primenu i razvoj veštačke inteligencije predviđen je ciljem četiri Strategije o razvoju veštačke inteligencije u Republici Srbiji za period 2025-2030. godine, „unapređenje infrastrukture i resursa neophodnih za razvoj i primenu veštačke inteligencije”.¹⁰⁹ Međutim, pored unapređenja postojećih sistema, najsavremenija tehnološka infrastruktura poput superkompjutera može služiti i **treniranju sopstvenog modela veštačke inteligencije** koja se trenira na lokalnim podacima kako bi što bolje ispunjavala potrebe lokalnog konteksta. Jedan od najznačajnijih ciljeva je rad na razvoju jezičkih modela koji će biti prilagođeni specifičnim potrebama srpskog jezika i kulture.¹¹⁰

Peti cilj Strategije „korišćenje podataka kao značajnog resursa za razvoj veštačke inteligencije” podstiče otvaranje velikih baza podataka u državnom, ali i privatnom sektoru za potrebe treniranja novih modela veštačke inteligencije.¹¹¹ Međutim, iako tehnološki napredak u vidu razvoja veštačke inteligencije potencijalno može doneti koristi, izuzetno je važno da se taj napredak temelji na jakoj pravnoj osnovi, funkcionalnoj vladavini prava, tehnološkoj transparentnosti i sistemskoj odgovornosti. Razvoj i primena veštačke inteligencije sa sobom nosi brojne rizike, koji postaju izraženiji u okruženju u kojem tehnološki napredak dolazi pre adekvatnih pravnih, tehnoloških i društvenih okvira. Jedan od najznačajnijih rizika povezan je sa zaštitom podataka o ličnosti.

Kao što se navodi u cilju pet Strategije, podaci su ključni resurs razvoja veštačke inteligencije, te samim tim postoji realna opasnost da se potrebe treniranja veštačke inteligencije nađu u potpunoj suprotnosti sa načelima propisanim u Zakonu o zaštiti podataka o ličnosti i drugim pravnim aktima koji regulišu ovu oblast. U najvećem broju slučajeva, državne baze podataka poseduju veliku količinu osetljivih podataka građana, uključujući medicinske, socijalne, finansijske i druge podatke. Dosadašnja praksa u Srbiji ukazuje na nizak nivo institucionalne posvećenosti zaštiti podataka o ličnosti. Os-

etljivi podaci iz državnih baza neretko su se pojavljivali u javnosti, bilo u tabloidnim medijima ili kao instrument političkog obračuna sa neistomišljenicima.¹¹² Takvi slučajevi ozbiljno narušavaju poverenje građana u institucije i postavljaju dodatna pitanja o bezbednosti budućih sistema veštačke inteligencije koji će, između ostalog, koristiti državne baze podataka za treniranje modela.

Još jedan rizik centralizacije, ukrštanja i masovne obrade podataka jeste mogućnost da bezbednosne službe zloupotrebe podataka u svrhe nelegalnog nadzora građana, pogotovo imajući u vidu da je jedan deo Data centra rezervisan za vojsku, policiju i Bezbednosno-informativnu agenciju (BIA).¹¹³ Od masovnog nezakonitog pristupa metapodacima građana,¹¹⁴ preko praćenja lica preko bezbednosnih kamera¹¹⁵ do nezakonite rasprostranjene upotrebe špijunskih softvera,¹¹⁶ bezbednosne institucije su pokazale da su spremne da zloupotrebe svaku naprednu tehnologiju za nadzor građana. Primena i treniranje veštačke inteligencije takođe nosi rizik razvoja diskriminatorskih tehnologija, naročito kada se oslanjaju na neadekvatne ili pristrasne baze podataka. Ilustrativan primer predstavlja slučaj Socijalne karte.¹¹⁷

„PAMETNA SRBIJA” I CENTRALIZACIJA PODATAKA

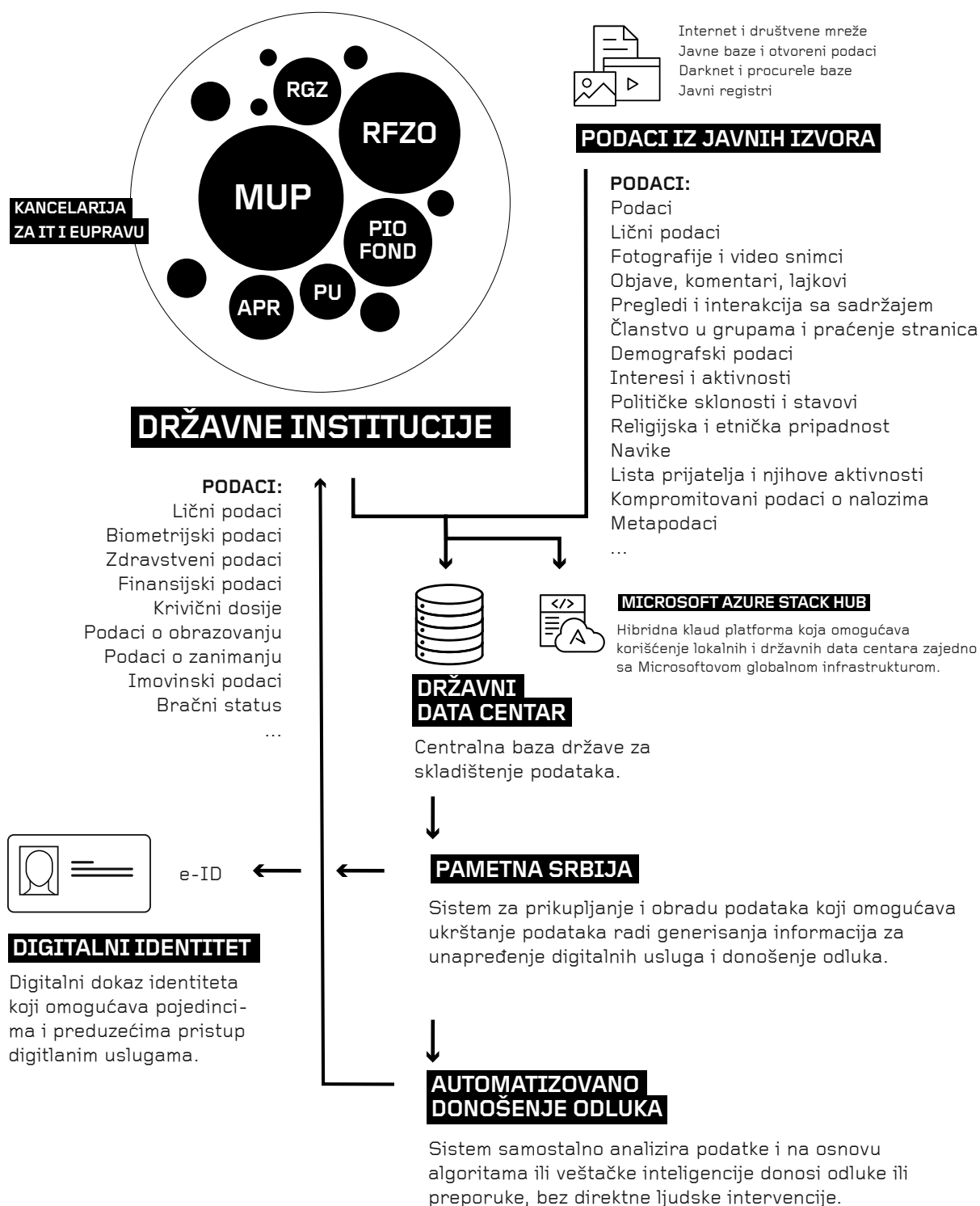
Pametna Srbija predstavlja ključnu nacionalnu inicijativu za integraciju državnih podataka i izgradnju usluga javne uprave zasnovanih na veštačkoj inteligenciji. Tehnički posmatrano, to je centralizovana platforma za prikupljanje i obradu podataka iz više javnih izvora, postavljena u Državnom data centru u Kragujevcu.¹¹⁸

Platforma Pametna Srbija zamišljena je da funkcioniše kao „mozak” eUprave, povezujući razdvojene baze u jedinstveno skladište podataka sposobno da podrži naprednu anali-

tiku, aplikacije veštačke inteligencije i modernizovane digitalne usluge. U objašnjenju rada platforme pominje se i mogućnost pametnog odlučivanja za šta se kao primer navodi projekat „Moja prva plata“. Iako predstavnici Kancelarije za IT i eUpravu navode da nemaju pristup podacima o ličnosti, ističu da imaju „ID“ građana, što navodi na zaključak da se podaci ipak mogu spojiti sa konkretnom os-

obom.¹¹⁹ Takođe, platforma podstiče razvoj inovacija u oblasti veštačke inteligencije omogućavanjem pristupa državnim podacima za treniranje sopstvenog modela veštačke inteligencije.¹²⁰

Međutim, ovakav sistemski pristup nosi i ozbiljne rizike. Centralizacija osetljivih informacija otvara prostor za bezbednosne rizike i zloupotrebu, dok algoritamsko odlučivanje



postavlja zahteve za veću transparentnost i odgovornost. Posebno je problematično ukrštanje ličnih i drugih podataka i potencijalna mogućnost stvaranja „digitalnih profila“ građana.¹²¹ Iako je platforma projektovana da bude skalabilna za buduće servise veštačke inteligencije, poput prediktivnih modela i interfejsa zasnovanih na prirodnom jeziku, još uvek nije jasno u kojoj meri će ti alati biti podložni kontroli i etičkom nadzoru.

Na kraju, jedan od najupečatljivijih pokazatelja ambicije Vlade Srbije da se pozicionira kao regionalni lider u primeni veštačke inteligencije jeste **obimno javno finansiranje programa i projekata** u ovoj oblasti. Mapirana su četiri ključna državna fonda koja zajedno oblikuju institucionalnu podršku razvoju VI: *Fond za investicionu delatnost*, koji obuhvata više od 13 različitih programa, uključujući i strateški značajan GovTech program; Fond za nauku, sa 10 aktivnih linija finansiranja istraživanja; zatim fond Instituta za veštačku inteligenciju, koji podržava preko 30 specijalizovanih projekata u oblasti VI; i, konačno, program AI4SME Srbija, usmeren na mala i srednja preduzeća, koji je do sada omogućio realizaciju 10 uspešnih inicijativa u oblasti veštačke inteligencije.

GovTech program posebno se ističe po tome što državne institucije identifikuju izazove u svom radu, nakon čega traže razvoj inovativnih rešenja od kompetentnih aktera. U prvom GovTech programu izdvojeno je 24 izazova, među kojima se traži izrada sistema spajanja poslodavaca i kandidata (MatchTech) za potrebe Nacionalne službe za zapošljavanje, sistema telemedicine za potrebe Doma zdravlja „Zvezdara“ i sistema za efikasnu konverziju za potrebe Ministarstva građevinarstva, saobraćaja i infrastrukture.¹²²

Ovakva široko postavljena finansijska podrška ukazuje na stratešku opredeljenost države da razvija ekosistem veštačke inteligencije u Sr-

biji. Međutim, i pored intenzivnih ulaganja, još uvek ne postoji adekvatan pravni okvir koji bi regulisao ovu oblast. Iako je formirana Radna grupa za izradu Nacrta zakona o veštačkoj inteligenciji Republike Srbije, koja bi trebalo da se u svom pristupu oslanja na evropski Akt o veštačkoj inteligenciji (AI Act), sam zakon je i dalje u ranoj fazi i daleko je od usvajanja i primene.¹²³

Problem ubrzane inovacije

Savremeni proces digitalizacije u Srbiji jasno pokazuje da su podaci postali osnovni resurs ali i glavni kamen spoticanja funkcionisanja javnog sektora. Kroz različite faze njihovog životnog ciklusa, od prikupljanja, preko analize i automatizovanog odlučivanja, do skladištenja i čuvanja, podaci oblikuju način na koji država planira, odlučuje i komunicira sa građanima. Međutim, paralelno sa tehničkim unapređenjem infrastrukture, rastu i izazovi povezani sa bezbednošću, privatnošću i odgovornošću u upravljanju podacima.

U tom kontekstu, veštačka inteligencija se pojavljuje kao sledeća faza u korišćenju digitalne infrastrukture. Kao tehnologija koja se oslanja na ogromne količine podataka, ona produbljuje postojeće izazove, posebno u pogledu transparentnosti, odgovornosti i zaštite privatnosti. Bez jasnog pravnog i etičkog okvira, primena sistema koji automatizuju odlučivanje u javnim institucijama nosi rizik da ojača već prisutne obrasce netransparentnosti i nejednakog tretmana građana. Umesto da doprinese efikasnosti i objektivnosti, automatizacija može postati instrument za širenje postojećih nepravdi – od diskriminatornih algoritama do nevidljivog nadzora.

Pored toga, centralizacija i ukrštanje baza podataka, zajedno sa razvojem sistema „pametne države“, povećavaju mogućnost stvaranja jedinstvenih digitalnih profila građana, čime se otvara prostor za masovni i nekontrolisani nadzor. U uslovima slabe institucionalne kontrole,

ovakav model skladištenja i analize podataka predstavlja ozbiljan rizik po ljudska prava i demokratske procese. Građani najčešće nisu informisani o tome gde i kako se njihovi podaci čuvaju, niti o tome ko ima pristup tim informacijama. Odsustvo javnog nadzora dodatno produbljuje nepoverenje, dok odgovornost za eventualne zloupotrebe ostaje nejasna.

Zato je neophodno da razvoj infrastrukture i naprednih tehnologija bude praćen uspostavljanjem jasnih pravila o upravljanju podacima u svim fazama njihovog životnog ciklusa, od prikupljanja i analize, do arhiviranja i brisanja. Samo sistem koji podrazumeva kontrolu pristupa, transparentnost i mogućnost revizije može garantovati da digitalizacija služi građanima, a ne obrnuto.

Bez takvog pristupa, rizik je da će podaci, umesto da budu alat za javno dobro, postati osnova novog oblika digitalne nejednakosti i nadzora. Tek kada se zatvori krug odgovornog upravljanja podacima – kroz jasne politike čuvanja, brisanja i ograničavanja pristupa, može se govoriti o digitalnom razvoju koji istinski poštuje prava građana i principe vladavine prava.

Otvorena pitanja

Mapiranje naprednih tehnologija u Srbiji pokazuje njihovu široku upotrebu u različitim oblastima. Uprkos metodološkim ograničenjima u pogledu istraživačkog obuhvata svih naprednih tehnologija koje se koriste u Srbiji, primetna je visoka zastupljenost naprednih tehnoloških rešenja u oblastima kojima rukovodi država. Takva rešenja se uglavnom predstavljaju sa stanovišta benefita, čime se principijelno uspostavlja opšti okvir upotrebe naprednih tehnologija bez dovoljne pažnje koja bi bila posvećena prevenciji i suzbijanju štete koja može nastati njihovom upotrebom.

Ova studija pokazuje da se naprednim tehnologijama u Srbiji dominantno pristupa iz perspektive inovacija i tehnološkog razvoja, a značajno manje iz perspektive zaštite ljudskih prava i šire društvene odgovornosti. Takođe, priroda (nedostatka) izvora informacija za ovo mapiranje značajno je oblikovala istraživački domet, ali je i sama ta činjenica važan istraživački nalaz. Ona ukazuje na ograničen pristup informacijama o razvoju i primeni naprednih tehnologija u javnom sektoru, kao i na potrebu za dubljim, sistemskim istraživanjem ove oblasti koje bi obuhvatilo i perspektivu građana, organizacija civilnog društva i nezavisnih institucija. Zbog toga, umesto zaključka otvaramo pitanja za dalje istraživanje u ovoj oblasti.

I SISTEM I ZAŠTITA PRAVA

- Kako nedostatak transparentnosti utiče na mogućnost građana i nezavisnih aktera da procene rizike po prava i slobode pri primeni ovih tehnologija?
- Da li postoje mehanizmi nadzora i kontrole upotrebe naprednih tehnologija u javnom sektoru?
- Zašto su uloge nezavisnih institucija, poput Poverenika i Zaštitnika građana, margin-

alizovane u nadzoru i regulaciji primene naprednih tehnologija u javnom sektoru?

- Postoji li sistematska evidencija o sprovedenim procenama rizika i njihovim rezultatima?

II TEHNOLOŠKE SPECIFIKACIJE I PODACI

- Koji su stvarni mehanizmi i algoritmi koje koriste napredne tehnologije u javnom sektoru, s obzirom na ograničen pristup informacijama?
- Jačanje kojih kapaciteta bi moglo da doprinese obezbeđivanju „životnog ciklusa“ podataka?
- Na osnovu čega se biraju oblasti u kojima će napredne tehnologije biti korišćene?

III FINANSIJSKI I REGULATORNI OKVIRI

- Koji su stvarni troškovi i finansijski tokovi povezani sa nabavkom i implementacijom naprednih tehnologija u javnom sektoru?
- Kako se finansijska sredstva za ove tehnologije raspoređuju i koji su kriterijumi donošenja odluka o njihovoj upotrebi?
- Kolika je uloga Evropske unije u finansiranju i podsticanju razvoja i primene naprednih tehnologija u Srbiji, i u kojoj meri se pri tome uzima u obzir lokalni kontekst?
- Do koje mere spoljna (EU) regulativa može da utiče na promenu domaćeg okvira oko naprednih tehnologija?

IV GRAĐANI I JAVNA SVEST

Koliko građani znaju o primeni naprednih tehnologija u javnom sektoru i uticaju na njihova prava?

Beleške

- 1 European Commission: Executive Agency for Small and Medium-sized Enterprises, Fraunhofer ISI, IDC, IDEA Consult, Technopolis Group, Izsak, K., Carosella, G., Kroll, H., Wydra, S., Velde, E. v. d. Micheletti, G., Advanced technologies for industry – Final report – Report on technology trends and technology adoption, Publications Office, 2021, <https://data.europa.eu/doi/10.2826/321124>
- 2 Strategija razvoja veštačke inteligencije u Republici Srbiji za period 2020-2025. godine, <https://prosveta.gov.rs/wp-content/uploads/2019/11/1-Nacrt-strategije-razvoja-vestacke-inteligencije-u-Republici-Srbiji-za-period-2020.-2025.-godine.pdf>
- 3 Institut za veštačku inteligenciju, <https://ivi.ac.rs/about-us/>
- 4 Etičke smernice za razvoj, primenu i upotrebu pouzdane i odgovorne veštačke inteligencije, „Sl. glasnik RS”, br. 23/2023, http://demo.paragraf.rs/demo/combined/Old/t/t2023_03/SG_023_2023_007.htm
- 5 Strategija razvoja veštačke inteligencije u Republici Srbiji za period 2025-2030. godine, <https://nitra.gov.rs/images/vesti/2025/2025-01-10-link/Strategija%20razvoja%20vestacke%20inteligencije%202025-2030.pdf>
- 6 Milica Milosavljević, „Srbija treba da postane lider u primeni veštačke inteligencije”, RTS, 03. decembar 2024., <https://www.rts.rs/magazin/tehnologija/5595342/srbija-treba-da-postane-lider-u-primeni-vestacke-inteligencije.html>
- 7 „Srbija u naredne tri godine predsedavajuća GPAI”, Vlada Republike Srbije, 08. mart 2024., <https://www.srbija.gov.rs/vest/770097/srbija-u-naredne-tri-godine-predsedavajuca-gpai.php>
- 8 Nisha Talagala, „Data as The New Oil Is Not Enough: Four Principles For Avoiding Data Fires”, Forbes, 02. mart 2022., <https://www.forbes.com/sites/nishatalagala/2022/03/02/data-as-the-new-oil-is-not-enough-four-principles-for-avoiding-data-fires/>
- 9 Felix M. Simon, „Artificial Intelligence in the News: How AI Retools, Rationalizes, and Reshapes Journalism and the Public Arena”, Columbia Journalism Review, februar 2024, https://www.cjr.org/tow_center_reports/artificial-intelligence-in-the-news.php; John V. Pavlik „Collaborating With ChatGPT: Considering the Implications of Generative Artificial Intelligence for Journalism and Media Education”, Journalism & Mass Communication Educator, 78(1), 84-93, januar 2023, <https://onlinedegrees.sandiego.edu/artificial-intelligence-business/>
- 10 Fabio Duarte, „Amount of Data Created Daily (2025)”, Exploding topics, april 2025, <https://explodingtopics.com/blog/data-generated-per-day#how-much-data-is-generated-every-day>
- 11 Van Ooijen, Charlotte, Barbara Ubaldi, and Benjamin Welby, „A data-driven public sector: Enabling the strategic use of data for productive, inclusive and trustworthy governance”, OECD, 2019, https://www.oecd.org/content/dam/oecd/en/publications/reports/2019/05/a-data-driven-public-sector_1c183670/09ab162c-en.pdf?utm_source=chatgpt.com
- 12 David Lyon, „Surveillance society”, Open University Press, 2001.
- 13 „Portal eUprava”, Kancelarija za IT i eUpravu, <https://www.ite.gov.rs/tekst/77/portal-euprava.php>
- 14 eUprava, <https://euprava.gov.rs/>
- 15 Zakon o osnovama sistema obrazovanja i vaspitanja („Sl. glasnik RS”, br. 88/2017, 27/2018 - dr. zakon, 10/2019, 27/2018 - dr. zakon, 6/2020, 129/2021, 92/2023 i 19/2025)
- 16 Član 176, Zakon o osnovama sistema obrazovanja i vaspitanja („Sl. glasnik RS”, br. 88/2017, 27/2018 - dr. zakon, 10/2019, 27/2018 - dr. zakon, 6/2020, 129/2021, 92/2023 i 19/2025)
- 17 „Pušten u rad jedinstveni informacioni sistem prosvete: JISP objedinjuje sve informacije o ustanovama i zaposlenima unutar obrazovnog sistema, kao i o učenicima i studentima”, Paragraf Lex, mart 2022, <https://www.paragraf.rs/dnevne-vesti/210322/210322-vest10.html>
- 18 „esDnevnik”, Vlada Republike Srbije, februar 2019, <https://www.srbija.gov.rs/tekst/364772/esdnevnik.php>
- 19 Vesna Andrić, „Ko je privatnoj firmi dao podatke đaka”, Danas, maj 2020, <https://www.danas.rs/vesti/drustvo/ko-je-privatnoj-firmi-dao-podatke-djaka/>
- 20 Strategija razvoja obrazovanja i vaspitanja u Republici Srbiji do 2030. godine, <https://prosveta.gov.rs/wp-content/uploads/2021/09/SROVRS-2030-1.pdf>
- 21 „Portal Zdravitas je digitalizacija vođenja evidencije u okviru predmeta Fizičko i zdravstveno

- vaspitanje", Ministarstvo prosvete, novembar 2024, <https://prosveta.gov.rs/vesti/portal-zdravitas-je-digitalizacija-vodjenja-evidencije-u-okviru-predmeta-fizicko-i-zdravstveno-vaspitanje/>
- 22 „Saopštenje Poverenika: 'Zdravitas'", Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti, oktobar 2024, <https://www.poverenik.rs/sr-yu/saopstenja/4275-%D1%81%D0%B0%D0%BE%D0%BF%D1%88%D1%82%D0%B5%D1%9A%D0%B5%D0%B7%D0%B4%D1%80%D0%B0%D0%B2%D0%B8%D1%82%D0%B0%D1%81.html>
 - 23 „Ministarstvo prosvete Srbije potvrdilo da se odlaže primena portala Zdravitas", NIN, novembar 2024, <https://www.nin.rs/drustvo/vesti/62808/potvrdeno-odlaganje-primene-portala-zdravitas>
 - 24 „Закључак (Владе о успостављању јединственог и централизованог софтверског решења – Информациони систем COVID-19 (ИС COVID-19))": 50/2020-9, 57/2020-17, Правно-информациони систем Републике Србије | Јавно предузеће „Службени гласник", <https://pravno-informacioni-sistem.rs/eli/rep/sgrs/vlada/zakljucak/2020/50/1/reg>
 - 25 „Pandemija jedne lozinke. Kako je šifra za Covid-19 završila na internetu?", SHARE Fondacija, 20. april 2020, <https://sharefoundation.info/pandemija-jedne-lozinke-kako-je-sifra-za-covid-19-zavrsila-na-internetu/>
 - 26 Mila Bajić Duje Prkut, „Praksa" u: Ella Jakubowska, Andrej Petrovski & Danilo Krivokapić (ur.) „S one strane lica: Biometrija i društvo", SHARE Fondacija, 2025. <https://sharefoundation.info/wp-content/uploads/2025/04/BMS-study-srpski-2025.pdf>
 - 27 Natalija Jovanović, „'Mali brat i velike sestre'", Radio Slobodna Evropa, jul 2023, <https://www.slobodnaevropa.org/a/video-nadzor-kineske-kamere-srbija/32507504.html>
 - 28 Hiljade kamera, <https://hiljade.kamera.rs/sr/pocetna/>
 - 29 Mila Bajić Duje Prkut, „Praksa" u: Ella Jakubowska, Andrej Petrovski & Danilo Krivokapić (ur.) S one strane lica: Biometrija i društvo, SHARE Fondacija, 2025. <https://sharefoundation.info/wp-content/uploads/2025/04/BMS-study-srpski-2025.pdf>
 - 30 „Biometrijski nadzor na javnim površinama u Srbiji: Pozicija SHARE Fondacije nakon predloženih nacrti zakona", SHARE Fondacija, decembar 2022. godine, https://www.sharefoundation.info/wp-content/uploads/SHARE_Pozicija_Biometrijski_Nadzor.pdf
 - 31 „Šapić: Realizacijom bezbednosnog projekta Grada Beograda podižemo bezbednost građana, posebno dece, na najviši mogući nivo", Grad Beograd, 26.02.2025. <https://www.beograd.rs/lat/beoinfo-vesti/a106656/Sapic-Realizacijom-bezbednosnog-projekta-Grada-Beograda-podizemo-bezbednost-gradjana-posebno-dece-na-najvisi-moguci-novo.html>
 - 32 Ibid.
 - 33 „Javne nabavke opreme za nadzor: Tanka linija između bezbednosti i privatnosti", BIRN Srbija, januar 2024, <https://birnsrbija.rs/javne-nabavke-opreme-za-nadzor-tanki-linija-izmedu-bezbednosti-i-privatnosti/>
 - 34 "Transforming Serbian Road Monitoring with Adaptive Recognition's Vidar ANPR Cameras", Adaptive Recognition, <https://adaptiverecognition.com/case-study/transforming-serbian-road-monitoring-with-adaptive-recognition-vidar-cameras/>
 - 35 Oko sokolovo, <https://okosokolovo.com/>
 - 36 Aleksa Tešić, „Policijski dronovi: Moćni alati koji se koriste bez dovoljno nadzora", BIRN, 29. Decembar 2023, <https://birn.rs/upotreba-policijskih-dronova-bez-dovoljno-kontrole/>
 - 37 Bojan Perkov, „Tehnologija" u: Ella Jakubowska, Andrej Petrovski & Danilo Krivokapić (ur.) S one strane lica: Biometrija i društvo, SHARE Fondacija, 2025. <https://sharefoundation.info/wp-content/uploads/2025/04/BMS-study-srpski-2025.pdf>
 - 38 „Javne nabavke opreme za nadzor: Tanka linija između bezbednosti i privatnosti", BIRN Srbija, januar 2024, <https://birnsrbija.rs/javne-nabavke-opreme-za-nadzor-tanki-linija-izmedu-bezbednosti-i-privatnosti/>
 - 39 "Ending the Targeted Digital Surveillance of Those Who Defend Our Rights", Amnesty International, 2019, <https://www.amnesty.org/en/wp-content/uploads/2021/05/ACT3013852019ENGLISH.pdf>
 - 40 „Nevidljive infrastrukture: Elektronski nadzor i zadržavanje podataka sa mobilnih telefona", SHARE Labs, jun 2015, <https://labs.rs/sr/nevidljive-infrastrukture-elektronski-nadzor-i-zadrzavanje-podataka-sa-mobilnih-telefona/>
 - 41 Bill Marczak, John Scott-Railton, Siddharth Prakash Rao1, Siena Anstis, and Ron Deibert, "Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles", Citizen Lab, December 2020, <https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/>
 - 42 „Uvoz i upotreba opreme za nadzor u Srbiji: Slučaj Trovicor", SHARE Fondacija, novembar 2013, <https://resursi.sharefoundation.info/sr/resource/uvoz-i-upotreba-opreme-za-nadzor-u-srbiji-slucaj-trovicor/>
 - 43 Bill Marczak, John Scott-Railton, Siddharth

- Prakash Rao¹, Siena Anstis, and Ron Deibert, "Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles", Citizen Lab, decembar 2020, <https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/>
- 44 "The Spy Files 3", WikiLeaks, septembar 2013, https://wikileaks.org/spyfiles/docs/SERBIA_2012_WLCIRS_en.html
- 45 "Spyware and state abuse: The case for an EU-wide ban", EDRi, <https://edri.org/our-work/spyware-and-state-abuse-the-case-for-an-eu-wide-ban-position-paper/>
- 46 "Spyware in Serbia: civil society under attack", Access Now, novembar 2023, <https://www.accessnow.org/spyware-attack-in-serbia/>
- 47 Ibid.
- 48 „Otkriveni pokušaji špijunskih napada na mobilne uređaje pripadnika civilnog društva“, SHARE Fondacija, novembar 2023, <https://sharefoundation.info/otkriveni-pokusaji-spijunskih-napada-na-mobilne-uredjaje-pripadnika-civilnog-drustva/>
- 49 „Novinarke BIRN Srbija targetirane špijunskim softverom“, SHARE Fondacija, mart 2025, <https://sharefoundation.info/novinarke-birn-srbija-targetirane-spijunskim-softverom/>
- 50 "'A Digital Prison': Surveillance and the suppression of civil society in Serbia", Amnesty International, decembar 2024, <https://www.amnesty.org/en/documents/eur70/8813/2024/en/>
- 51 „MUP i BIA nezakonito upadaju u telefone aktivista i novinara“, SHARE Fondacija, decembar 2024, <https://sharefoundation.info/mup-i-bia-nezakonito-upadaju-u-telefone-aktivista-i-novinara/>
- 52 Aleksa Tešić, „Nova žrtva špijunskog nadzora: Student priveden na šest sati, telefon mu hakovan“, BIRN Srbija, februar 2025, <https://birn.rs/student-spijunski-nadzor-hakovan-telefon/>
- 53 "Vlast uhapsila najmanje 920 ljudi od pada nadstrešnice", Vreme, 16. septembar 2025, <https://vreme.com/vesti/vlast-uhapsila-najmanje-920-ljudi-od-pada-nadstresnice/>
- 54 Krivični zakonik Republike Srbije („Sl. glasnik RS“, br. 85/2005, 88/2005 - ispr., 107/2005 - ispr., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016, 35/2019 i 94/2024)
- 55 Zakon o zaštiti podataka o ličnosti Republike Srbije („Sl. glasnik RS“, br. 87/2018), član 6
- 56 Zoë Corbyn, "'Bossware is coming for almost every worker': the software you might not realize is watching you", The Guardian, 27 April 2022, <https://www.theguardian.com/technology/2022/apr/27/remote-work-software-home-surveillance-computer-monitoring-pandemic>
- 57 „Nabavka usluge održavanja aplikacije Honesty, Republički geodetski zavod“, Portal javnih nabavki <https://www.nabavke.com/javne-nabavke-tenderi-srbija/nabavka-usluge-odrzavanja-aplikacije-honesty/republicki-geodetski-zavod/beograd/3093771>
- 58 „Honesty softver“, Melon interactive, <https://www.meloninteractive.com/content/company3/honesty.html>
- 59 Alexander Stingl, "Technology and Surveillance", EBSCO, 2021, <https://www.ebsco.com/research-starters/technology/technology-and-surveillance>
- 60 David Lyon, "Surveillance society", Open University Press, 2001.
- 61 Dianna Taylor, "Michel Foucault: key concepts", Routledge, 2014.
- 62 Katarina Đokić, Saša Đorđević, Marija Ignjatijević, Jelena Pejić Nikić i Predrag Petrović, „Zarobljavanje sektora bezbednosti u Srbiji“, Beogradski centar za bezbednosnu politiku, jun 2020, <https://bezbednost.org/wp-content/uploads/2020/11/NED-srb-screen-fin.pdf>
- 63 Shah, Syed Iftikhar Hussain, Vassilios Peristeras, and Ioannis Magnisalis, "DaLiF: a data lifecycle framework for data-driven governments", Journal of Big Data 8.1 (2021): 89.
- 64 Magnet Forensics, <https://www.magnetforensics.com/products/magnet-griffeye/>
- 65 ClearviewAI, <https://www.clearview.ai/>
- 66 Aleksa Tešić, „MUP planira nabavku tehnologije za prepoznavanje lica, Poverenik kaže da nemaju pravo“, BIRN Srbija, april 2022, <https://birn.rs/mup-planira-nabavku-tehnologije-za-prepoznavanje-lica/>
- 67 "About ClearviewAI's mockery of human rights, those fighting it, and the need for EU to intervene", RECLAIM YOUR FACE, mart 2022, <https://reclaimyourface.eu/about-clearviewai-mockery-human-rights-those-fighting-eu-intervene/>
- 68 Ibid.
- 69 Maltego, <https://static.maltego.com/cdn/Infographics/Maltego-Platform-Brief.pdf>
- 70 Social Links, <https://sociallinks.io/?r=0>
- 71 Mozenda, <https://www.mozenda.com/about/>
- 72 Cognate, <https://www.cognyte.com/>
- 73 Aleksa Tešić, „Softveri za obradu ličnih po-

- dataka, potencijalna pretnja po privatnost građana", BIRN Srbija, jun 2022, <https://birn.rs/softveri-za-obradu-licnih-podataka-potencijalna-pretnja-po-privatnost-gradana/>
- 74 Strategija razvoja pravosuđa za period 2020-2025. godine, „Službeni glasnik RS“, br. 101/2020 http://demo.paragraf.rs/demo/combined/Old/t/2020_07/SG_101_2020_001.htm
 - 75 „Od papirologije do digitalizacije: Javno tužilaštvo“, Comtrade System Integration, <https://comtradeintegration.com/sr/resource/od-papirologije-do-digitalizacije-javno-tuzilas-tvo/>
 - 76 „Strategija razvoja sistema izvršenja krivičnih sankcija za period od 2021. do 2027. godine – Nacrt“, Uprava za izvršenje krivičnih sankcija, Ministarstvo pravde Republike Srbije, 2021, <https://www.mpravde.gov.rs/sr/tekst/33173/strategija-razvoja-sistema-izvrsenja-krivicnih-sankcija-u-republici-srbiji-za-period-2021-2027-godina.php>
 - 77 „Konkursna dokumentacija za java nabavku usluga u otvorenom postupku 30/2018“, Ministarstvo pravde, <https://www.mpravde.gov.rs/files/6%20konkursna%20dokumentacija%20D0%B0%20-%20preciscen%20tekst%2030.pdf>
 - 78 „Zakon o socijalnoj karti“, „Sl. glasnik RS“, -14/2021, <https://www.paragraf.rs/propisi/zakon-o-socijalnoj-karti.html>
 - 79 „(Anti)socijalne karte“, Inicijativa za ekonomska i socijalna prava A11, oktobar 2022, <https://www.a11initiative.org/antisocijalne-karte/>
 - 80 Ibid.
 - 81 Natalija Jovanović i Dušan Komarčević, „Digitalizacija bede u Srbiji: Skinuti sa pomoći jer prodaju sekundarne sirovine“, Radio Slobodna Evropa, novembar 2022, <https://www.slobodnaevropa.org/a/srbija-socijalne-karte-algoritam/32153869.html>
 - 82 „JN 24/2023 – Dogradnja i modifikacija sistema IS Registar socijalna karta i integracija sa sistemima IS SOZIS, IS DD-RD, IS Boračko invalidske zaštite“, Ministarstvo za rad, zapošljavanje, boračka i socijalna pitanja, <https://www.minrzs.gov.rs/srb-lat/konkursi/jn-24/2023---dogradnja-i-modifikacija-sistema-is-registar-socijalna-karta-i-integracija-sa-sistemima-is-sozis-is-dd-rd-is-boracko-invalidske-zastite>
 - 83 „(Anti)socijalne karte“, Inicijativa za ekonomska i socijalna prava A11, oktobar 2022, <https://www.a11initiative.org/antisocijalne-karte/>
 - 84 „Privacy and Personal Data Protection in Serbia“, Partneri Srbija, april 2021, [https://www.partners-serbia.org/public/news/Privacy_and_Personal_Data_Protection_in_Serbia-An_Analysis_of_Selected_Sectoral_Regulations_and_Their_Implementation,_PS\(2\).pdf](https://www.partners-serbia.org/public/news/Privacy_and_Personal_Data_Protection_in_Serbia-An_Analysis_of_Selected_Sectoral_Regulations_and_Their_Implementation,_PS(2).pdf)
 - 85 „Potpisan Sporazum o poslovnoj saradnji između Poreske uprave Republike Srbije i PMF-a“, Prirodno-matematički fakultet, Univerzitet u Novom Sadu, maj 2021, <https://www.dmi.uns.ac.rs/2021/05/2595/>
 - 86 Denaura Bordandini i Massimo Borgobello, „Vera, AI at the service of the Revenue Agency: how the anti-evasion algorithm works“, Network360, jul 2022, <https://www.agendadigitale.eu/documenti/vera-lai-al-servizio-dellagenzia-delle-entrate-come-funziona-lalgoritmo-anti-evasione/>; „How Vera works, the anti-tax evasion algorithm“, BusinessWeekly, jul 2022, <https://businessweekly.it/notizie/attualita/come-funziona-vera-lalgoritmo-anti-evasione-fiscale/>
 - 87 Zoran Skopljak & Jasna Atanasijević, „Tackling Tax Evasion in Serbia with Big Data“, World Bank Blogs, januar 2024, <https://blogs.worldbank.org/en/governance/tackling-tax-evasion-serbia-big-data>
 - 88 „Serbian leading energy provider boosts trading profits with predictive artificial intelligence“, Microsoft, april 2020, <https://docslib.org/doc/8661823/jp-elektroprivreda-srbije-eps>
 - 89 „How Public Sectors across region use technology to power up economic output“, Microsoft, mart 2023, <https://news.microsoft.com/en-ee/2023/03/22/how-public-sectors-across-region-use-technology-to-power-up-economic-output/>
 - 90 Shah, Syed Iftikhar Hussain, Vassilios Peristeras, and Ioannis Magnisalis, „DaLiF: a data lifecycle framework for data-driven governments“, Journal of Big Data 8.1 (2021): 89.
 - 91 Zakon o kritičnoj infrastrukturi („Sl. glasnik RS“, br. 87/2018)
 - 92 Shah, Syed Iftikhar Hussain, Vassilios Peristeras, and Ioannis Magnisalis, „DaLiF: a data lifecycle framework for data-driven governments“, Journal of Big Data 8.1 (2021): 89.
 - 93 „Podaci građana u javnom sektoru: Kako država rukuje podacima“, SHARE Labs, avgust 2017, <https://labs.rs/sr/podaci-gradana-u-javnom-sektoru/>
 - 94 Strategija razvoja veštačke inteligencije u Republici Srbiji za period 2025-2030. godine („Sl. glasnik RS“, br. 5/2025)
 - 95 Ibid.
 - 96 Vojislav Stojavljević, „‘Svi će biti uhapšeni’: Nenadležni Vučić pretil javnim preduzećima zbog hakera i usput reklamira državni data centar“, Danas, <https://www.danas.rs/vesti/ekonomija/sajber-napad-drzavne-institucije-data-centar-zastita-podataka/>

- 97 „Kako je Novi Sad otet i zaključan“, SHARE Fondacija, jun 2021, <https://sharefoundation.info/kako-je-novi-sad-otet-i-zakljucan/>
- 98 „Geodetski zavod: Hakerski napad na IT infrastrukturu katastra, servisi nedostupni korisnicima“, Euronews Srbija, jul 2022, <https://www.euronews.rs/biznis/biznis-vesti/52053/geodetski-zavod-hakerski-napad-na-it-infrastrukturu-katastra-servisi-nedostupni-korisnicima/vest>
- 99 Natalija Jovanović, „Elektroprivreda Srbija pod ucenom hakera“, Radio Slobodna Evropa, decembar 2023, <https://www.slobodnaevropa.org/a/srbija-elektroprivreda-hakeri-ucena/32751103.html>
- 100 Daniela Ilić Krasić, „Hakerski napad na ministarstvo i dalje pravi problem: U katastar se ne upisuju novi vlasnici, list nepokretnosti bez ažurnih podataka“, N1, avgust 2025, <https://n1info.rs/biznis/hakerski-napad-na-ministarstvo-i-dalje-pravi-problem-u-katastar-se-ne-upisuju-novi-vlasnici-list-nepokretnosti-bez-azurnih-podataka/>
- 101 Marko Mudrinić, „Procureli lični podaci više od 5 miliona građana Srbije: Glavni krivac država?“, Netokracija, decembar 2014, <https://www.netokracija.com/srbija-licni-podaci-93750>
- 102 „Pandemija jedne lozinke. Kako je šifra za Covid-19 završila na internetu?“, SHARE Fondacija, april 2020, <https://sharefoundation.info/pandemija-jedne-lozinke-kako-je-sifra-za-covid-19-završila-na-internetu/>
- 103 SHARE Monitoring, jun 2021, <https://monitoring.labs.rs/data>
- 104 „Kancelarija za IT i eUpravu glavni motor digitalne transformacije javne uprave: Srbija spremno dočekuje uspostavljanje Digitalnog novčanika“, Kancelarija za IT i eUpravu, septembar 2024, <https://www.ite.gov.rs/vest/sr/8187/kancelarija-za-it-i-eupravu-glavni-motor-digitalne-transformacije-javne-uprave-srbija-spremno-dočekuje-uspostavljanje-digitalnog-novcanika.php>
- 105 „Nacionalna AI platforma“, Nacionalna platforma za veštačku inteligenciju, <https://www.ai.gov.rs/tekst/sr/189/nacionalna-ai-platforma.php>
- 106 Charlotte Trueman, „Serbian gov't signs contact with Eviden for €50m supercomputer“, Data Center Dynamics, april 2025, <https://www.datacenterdynamics.com/en/news/serbian-govt-signs-contact-with-eviden-for-50m-supercomputer/>
- 107 Gojko Vlaović, „EU u Srbiji gradi fabriku veštačke inteligencije“, NIN, oktobar 2025, <https://www.nin.rs/ekonomija/vesti/92059/eu-u-srbiji-gradi-fabriku-vestacke-inteligencije>
- 108 „Veštačka inteligencija – sadašnjost i budućnost“, EU u Srbiji, mart 2023, <https://europa.rs/vestacka-inteligencija-sadasnjost-i-buducnost/>
- 109 Strategija razvoja veštačke inteligencije u Republici Srbiji za period 2025-2030. godine („Sl. glasnik RS“, br. 5/2025)
- 110 „Veliki jezički modeli za srpski jezik – značaj, primena, potencijal“, Institut za veštačku inteligenciju, <https://ivi.ac.rs/news/veliki-jezicki-modeli-za-srpski-jezik-znacaj-primena-potencijal/>
- 111 Strategija razvoja veštačke inteligencije u Republici Srbiji za period 2025-2030. godine („Sl. glasnik RS“, br. 5/2025)
- 112 Anđela Milivojević i Milica Stojanović, „Privatnost građana godinama na izvolte“, CINS, jun 2017, https://www.cins.rs/privatnost-gradjana-godinama-na-izvolite/?utm_source=chatgpt.com; „Novosti objavile fotografije pasoša studenata“, SHARE Monitoring, januar 2025, <https://monitoring.labs.rs/data?caseId=1051>; „Uznemirujući snimak: Kamere zabeležile udes ispred Vlade Srbije“, Mondo, jun 2020, <https://mondo.rs/Info/Crna-hronika/a1338056/Nesreca-ispred-Vlade-Srbije-snimak-trenutak-udes.html>
- 113 Ana Ristović, „Srbija kupuje novi superkompjuter i planira da servisira region“, Bloomberg Adria, mart 2025, <https://rs.bloombergadria.com/tehnologija/inovacije/76468/novim-superkompjuterom-srbija-moze-da-servisira-region/news>
- 114 „Nevidljive infrastrukture: Elektronski nadzor i zadržavanje podataka sa mobilnih telefona“, SHARE Labs, jun 2015, <https://labs.rs/sr/nevidljive-infrastrukture-elektronski-nadzor-i-zadrzavanje-podataka-sa-mobilnih-telefona/>
- 115 Nemanja Rujević, „Aerodrom ne zna otkud Infomeru snimci Nikole Ristića“, Nedeljnik Vreme, novembar 2024, <https://vreme.com/vesti/aerodrom-ne-zna-otkud-informeru-snimci-nikole-ristica/>
- 116 „MUP i BIA nezakonito upadaju u telefone aktivista i novinara“, SHARE Fondacija, decembar 2024, <https://sharefoundation.info/mup-i-bia-nezakonito-upadaju-u-telefone-aktivista-i-novinara/>
- 117 „(Anti)socijalne karte“, A11, <https://antisocijalnekarde.org/>
- 118 „Predstavljena nova državna platforma 'Pametna Srbija'“, Vlada Republike Srbije, jun 2021, <https://www.srbija.gov.rs/vest/552405/predstavljena-nova-drzavna-platforma-pametna-srbija.php>
- 119 Bojan Prerad i Andreja Gluščević, „Pametna Srbija – platforma za donošenje pametnih odlu-

ka", Konferencija Sinergija, decembar 2021, <https://www.youtube.com/watch?v=zCMYPJnf-gfM&list=PPSV>

120 „Predstavljena nova državna platforma ‘Pametna Srbija’“, Vlada Republike Srbije, jun 2021, <https://www.srbija.gov.rs/vest/552405/predstavljena-nova-drzavna-platforma-pametna-srbija.php>

121 „Cyberama 4: Veštačka inteligencija, Pametna Srbija?“, SHARE Fondacija, jun 2021, <https://www.youtube.com/watch?v=qZTcMTCljPk&t=5s>

122 „GovTech“, Fond za investicionu delatnost, <https://www.inovacionifond.rs/lat/program/govtech>

123 „Održan prvi sastanak Radne grupe za izradu Nacrta zakona o veštačkoj inteligenciji Republike Srbije“, Nacionalna platforma za veštačku inteligenciju, jun 2024, <https://www.ai.gov.rs/vest/sr/1110/odrzan-prvi-sastanak-radne-grupe-za-izradu-nacrta-zakona-o-vestackoj-inteligenciji-republike-srbije.php>



This publication was funded partially by a grant from the United States Department of State. The opinions, findings and conclusions stated herein are those of the authors and do not necessarily reflect those of the United States Department of State.