



# ***Tajnost podataka: pravni okvir i praksa***



**Autorka:**

Kristina Obrenović, Partneri Srbija

**Istraživači i saradnici na istraživanju:**

Ana Toskić Cvetinović

Blažo Nedić

Milica Tošić

**Recenzent:**

Uroš Mišljenović

**Prelom i dizajn:**

Partneri Srbija

**Izdavač:**

Partneri Srbija

Beograd, januar 2026.

*Izradu ove publikacije omogućila je Misija OEBS-a u Srbiji u okviru projekta „Konsolidovanje procesa demokratizacije u sektoru bezbednosti u Republici Srbiji” koji je finansijski podržala Vlada Švedske.*

*Stavovi izrečeni u publikaciji pripadaju isključivo autorima i ne predstavljaju nužno zvaničan stav Misije OEBS-a u Srbiji.*

*Svi pojmovi koji su u publikaciji upotrebljeni u muškom gramatičkom rodu obuhvataju muški i ženski rod lica na koja se odnose.*

**Sadržaj:**

|                                                                                                      |    |
|------------------------------------------------------------------------------------------------------|----|
| <i>Ključni nalazi</i> .....                                                                          | 5  |
| Uvod .....                                                                                           | 7  |
| Pravni okvir .....                                                                                   | 9  |
| Zakon o tajnosti podataka .....                                                                      | 10 |
| Nedostaci Zakona o tajnosti podataka i problemi u njegovoj primeni .....                             | 14 |
| Odnos Zakona o tajnosti podataka i Zakona o slobodnom pristupu informacijama od javnog značaja ..... | 28 |
| Žalbe zbog tajnosti- pregled prakse Poverenika .....                                                 | 30 |
| Sankcionisanje povreda Zakona o tajnosti podataka .....                                              | 39 |
| Praksa prekršajnih sudova.....                                                                       | 39 |
| Krivični postupci .....                                                                              | 39 |
| Praksa Evropskog suda za ljudska prava.....                                                          | 42 |
| Perspektiva civilnog sektora i novinara .....                                                        | 47 |
| Zaključak.....                                                                                       | 53 |
| Aneks 1:Metodologija istraživanja .....                                                              | 56 |

## Ključni nalazi

*Ova publikacija razmatra pravni okvir i praksu primene Zakona o tajnosti podataka u Republici Srbiji. Iako je Zakon o tajnosti podataka usvojen 2009. sa ciljem uspostavljanja jedinstvenog i savremenog sistema zaštite tajnih podataka, nalazi ove analize ukazuju da ovaj sistem ni nakon petnaest godina primene nije funkcionalno zaokružen.*

*Normativni okvir karakterišu neprecizno i preširoko definisani pojmovi, nedovoljno jasni kriterijumi za klasifikaciju, kao i izostanak mehanizma za delotvoran nadzor nad primenom Zakona o tajnosti podataka. Poseban problem predstavljaju kaznene odredbe, koje nezakonito označavanje podataka kao tajnih i zloupotrebe u postupku klasifikacije ne prepoznaju kao povrede jednake težine onima koje se odnose na neovlašćeno odavanje tajnih podataka. U važećem pravnom okviru u potpunosti izostaju krivične ili druge ozbiljnije pravne posledice za organe ili pojedince koji nezakonito, neopravdano ili zloupotrebom ovlašćenja proglašavaju podatke tajnim, iako takvo postupanje može proizvesti podjednako teške posledice po državne interese.*

*Dodatni strukturni nedostatak Zakona ogleda se u činjenici da je značajan deo zakonske materije prepušten uređenju kroz podzakonska akta. Time se ključni elementi sistema tajnosti, uključujući kriterijume za klasifikaciju i postupke kontrole, izmeštaju iz zakonskog okvira u akte izvršne vlasti, čime se onemogućava participacija javnosti i zakonodavno-kontrolna uloga Narodne skupštine, što može negativno uticati na pravnu sigurnost, transparentnost i demokratski nadzor nad ovom oblašću.*

*Nadzor nad primenom Zakona pokazao se kao najslabija karika sistema. Ministarstvo pravde, koje je zakonom određeno kao ključni nadzorni organ, u praksi već godinama ne sprovodi nadzor.*

*Sudska i prekršajna praksa u ovoj oblasti gotovo da ne postoji. Podaci prikupljeni od prekršajnih sudova ukazuju da se postupci po osnovu povreda Zakona o tajnosti podataka ne vode, iako zakon propisuje širok spektar prekršaja. Krivični postupci su izuzetno retki, a izrečene kazne pretežno blage, što dodatno potvrđuje nefunkcionalnost sistema sankcionisanja.*

*U takvom institucionalnom kontekstu, jedini stvarni mehanizam kontrole nad prekomernom tajnošću ostaje žalbeni postupak pred Poverenikom za informacije od javnog značaja i zaštitu podataka o ličnosti. Međutim, praksa Poverenika ne obezbeđuje uvek delotvornu i blagovremenu zaštitu prava na pristup informacijama. Žalbeni postupci često traju mesecima, pa i godinama.*

*Konačno, dodatni problem predstavlja širenje režima tajnosti kroz sektorske zakone, naročito u oblasti bezbednosti. Uvođenjem posebnih pravila i izuzetaka kroz sektorske propise narušava se jedinstvenost sistema zaštite tajnih podataka i dodatno sužava prostor za javni nadzor nad radom institucija.*

## Uvod

Preispitivanje efekata primene Zakona o tajnosti podataka, koji je u primeni od 1. januara 2010, neophodno je kako zbog njegovog značaja za ostvarivanje prava na slobodan pristup informacijama, tako i zbog obezbeđivanja opšte pravne sigurnosti i zaštite bezbednosnih interesa države. Ne može se zanemariti činjenica da odsustvo rezultata koji su od ovog zakona očekivani već duže vreme ukazuje na duboke probleme u načinu na koji se sistem tajnosti primenjuje u praksi.

Zakon o tajnosti podataka predstavlja prvi pokušaj da se u Srbiji na sveobuhvatan i centralizovan način uredi oblast klasifikacije i zaštite tajnih podataka. Njegove ambicije bile su visoke, ali istovremeno i teško ostvarive: trebalo je prevazići dotadašnju decentralizaciju i neujednačene kriterijume koji su postojali u različitim delovima državne uprave, raskinuti sa nasleđem komunističkog perioda u kojem su ovlašćenja bezbednosnih službi bila široka, nejasna i slabo kontrolisana, te usmeriti državne institucije ka savremenim demokratskim standardima kojima je Srbija u prvoj deceniji XXI veka težila.

Cilj analize koja je pred vama teži da omogući što sveobuhvatnije sagledavanje primene Zakona o tajnosti podataka i povezanih propisa, kao i da identifikuje ključne izazove u praksi. Ovakav pregled posebno je važan u svetlu nedavne najave Ministarstva pravde<sup>1</sup> da je formirana radna grupa za izmenu Zakona o tajnosti podataka, što analizu čini pravovremenim doprinosom budućem reformskom procesu.

Analiza se, najpre, bavi **normativnim okvirom**, načinom na koji je Zakon o tajnosti podataka postavljen, njegovim osnovnim institutima, kriterijumima za označavanje podataka kao tajnih, pitanjem nadzora i sankcija za kršenje zakona. U okviru ovog dela razmatraju se i ključne nedorečenosti, neusklađenosti i pravne praznine koje su tokom godina stvorile značajne probleme u primeni zakona.

Drugo poglavlje **usmereno je na odnos Zakona o tajnosti podataka i Zakona o slobodnom pristupu informacijama od javnog značaja**. Tajnost podataka i pravo na pristup informacijama od javnog značaja često se posmatraju kao suprotstavljeni interesi. U uređenom demokratskom društvu ovi interesi nisu suprotstavljeni već ih možemo posmatrati kao komplementarne. Pored navedenih interesa, sa razvojem svesti i pravnog okvira, pojavljuje se i interes zaštite privatnosti građana, koji zajedno sa prethodna dva čini

<sup>1</sup> Ova informacija dobijena je kao odgovor na zahtev za pristup informacijama od javnog značaja. Zahtev Partnera Srbija, kao i odgovor možete pogledati na sledećim linkovima:

Zahtev za pristup informacijama od javnog značaja: [https://foi.partners-serbia.org/wp-content/uploads/prilog\\_310/Zahtev%20za%20pristup%20informacijama%20od%20javnog%20zna%C4%8Daja%20Partneri%20Srbija.pdf](https://foi.partners-serbia.org/wp-content/uploads/prilog_310/Zahtev%20za%20pristup%20informacijama%20od%20javnog%20zna%C4%8Daja%20Partneri%20Srbija.pdf)

Ministarstvo pravde odgovor: [https://foi.partners-serbia.org/wp-content/uploads/prilog\\_310/Odgovor%20Ministarstvo%20pravde.pdf](https://foi.partners-serbia.org/wp-content/uploads/prilog_310/Odgovor%20Ministarstvo%20pravde.pdf)

okosnicu prilikom uređivanja upravljanja informacijama. U okviru ovog poglavlja kroz praksu postupanja Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti pokušano je predstavljanje balansa između prava javnosti da zna i tajnosti podataka.

Treće poglavlje ove publikacije analizira **praksu prekršajnih i viših sudova** u cilju preispitivanje politike sankcionisanja za kršenja Zakona o tajnosti podataka.

Četvrto poglavlje pruža pregled **prakse Evropskog suda za ljudska prava** u cilju približavanja i boljeg razumevanja evropskih standarda u pogledu pronalaženja ravnoteže između zaštite interesa nacionalne bezbednosti i prava javnosti da zna.

Peto poglavlje donosi pregled **uticaja nedostupnosti informacija na rad organizacija civilnog društva i istraživačkih novinara**, zasnovano na intervjuima i konsultativnim sastancima. U ovom delu su predstavljena iskustva i izazovi civilnog društva i istraživačkih novinara prilikom prikupljanja informacija o radu organa javne vlasti.

Na kraju, analiza identifikuje ključne **preporuke za unapređenje zakonskog i institucionalnog okvira**.

Nadamo se da ova analiza može da doprinese unapređenju zakonskog okvira u procesu reforme Zakona o tajnosti podataka, ali i u svakodnevnoj praksi organa javne vlasti pri odlučivanju o zahtevima za pristup informacijama od javnog značaja. Partneri Srbija ostaju otvoreni za sugestije i predloge, i posvećeni saradnji sa institucijama, civilnim društvom i stručnom javnošću.



## Pravni okvir

Tajnost podataka posmatrana u smislu obaveze da se ograniči pristup podacima od interesa za nacionalnu i javnu bezbednost, odbranu, unutrašnje i spoljne poslove Republike Srbije treba da se odnosi na ograničene i jasnim kriterijumima utvrđene setove podataka čijim bi javnim objavljivanjem mogle da nastanu ozbiljne/ teške posledice po gorenavedene interese. „Klasifikacija podataka prema nivou osetljivosti i rizika koji njihovo obelodanjivanje može doneti omogućava stvaranje bezbednosnih mehanizama koji štite kako nacionalne interese, tako i privatnost građana. Informacije kvalifikovane kao „štićene“ ili „tajne“ najčešće se odnose na nacionalnu bezbednost, ekonomsku stabilnost ili lične podatke pojedinaca, zbog čega je njihova obrada strogo regulisana propisima i bezbednosnim procedurama.”<sup>2</sup>

Tajni podaci predstavljaju podatke koji imaju značaj za nacionalnu bezbednost, odbranu, spoljnu politiku ili druge vitalne interese Republike Srbije. Podaci od javnog značaja su podaci koji se odnose na rad ili su nastali u vezi sa radom organa javne vlasti. Podaci o ličnosti su podaci koji se odnose na fizička lica (građane) a pomoću kojih identitet lica može biti određen ili određiv, neposredno ili posredno.

Svi ovi interesi uređeni su u Republici Srbiji, kao i u većem delu sveta kroz zakone i druga pravna akta. U Republici Srbiji, u sklopu približavanja pravnog okvira zemljama Evropske unije, prvo je donet Zakon o slobodnom pristupu informacijama od javnog značaja<sup>3</sup> 2004. godine, zatim Zakon o zaštiti podataka o ličnosti 2008.<sup>4</sup> koji je 2018. zamenjen novim Zakonom<sup>5</sup> 2018. i naposljetku Zakon o tajnosti podataka<sup>6</sup> koji je usvojen 2009, ujedno i jedini od tri koji nije menjan od usvajanja. Sa aspekta upravljanja podacima koji uživaju poverljivost ovde je važno spomenuti i Zakon o zaštiti poslovne tajne<sup>7</sup> usvojen 2021.

Predmet ove analize je pre svega primena Zakona o tajnosti podataka, kao i njegov odnos sa pravom na pristup informacijama od javnog značaja, stoga će u nastavku najveća pažnja biti

<sup>2</sup> Prof. dr Goran D. Matić, tajni podaci, javna politika i bezbednosna politika: Stubovi nacionalne bezbednosti Republike Srbije, 2025, str. 19, <https://nsa.gov.rs/extfile/sr/5031/TPJavna%20i%20bezbednosna%20politika-NBRS.pdf>

<sup>3</sup> Zakon o slobodnom pristupu informacijama od javnog značaja ("Sl. glasnik RS", br. 120/2004, 54/2007, 104/2009, 36/2010 i 105/2021),

[https://www.paragraf.rs/propisi/zakon\\_o\\_slobodnom\\_pristupu\\_informacijama\\_od\\_javnog\\_znacaja.html](https://www.paragraf.rs/propisi/zakon_o_slobodnom_pristupu_informacijama_od_javnog_znacaja.html)

<sup>4</sup> Zakon o zaštiti podataka o ličnosti ("Službeni glasnik RS", br. 97/08 104/09-dr.zakon, 68/12 -odluka US 107/12)

<https://www.poverenik.rs/images/stories/dokumentacija-nova/zzpl.doc>

<sup>5</sup> Zakon o zaštiti podataka o ličnosti ("Sl. glasnik RS", br. 87/2018)

[https://www.paragraf.rs/propisi/zakon\\_o\\_zastiti\\_podataka\\_o\\_licnosti.html](https://www.paragraf.rs/propisi/zakon_o_zastiti_podataka_o_licnosti.html)

<sup>6</sup> Zakon o tajnosti podataka ("Sl. glasnik RS", br. 104/2009),

[https://www.paragraf.rs/propisi/zakon\\_o\\_tajnosti\\_podataka.html](https://www.paragraf.rs/propisi/zakon_o_tajnosti_podataka.html)

<sup>7</sup> Zakon o zaštiti poslovne tajne ("Sl. glasnik RS", br. 53/2021)

[https://www.paragraf.rs/propisi/zakon\\_o\\_zastiti\\_poslovne\\_tajne.html](https://www.paragraf.rs/propisi/zakon_o_zastiti_poslovne_tajne.html)

posvećena ovom zakonu. Zakon o zaštiti podataka o ličnosti, iako važan sa aspekta upravljanja podacima od strane organa javne vlasti, kao i Zakon o zaštiti poslovne tajne, neće biti predmet ove analize.

## Zakon o tajnosti podataka

Zakon o tajnosti podataka usvojen je 2009, a njegova primena započeta je 01.01.2010. godine. Suštinski je uveo jedinstven, centralizovan sistem zaštite tajnih podataka u Republici Srbiji, a u cilju usklađivanja sa standardima koji su postojali u Evropskoj uniji i NATO, kako bi se pored ostalog, otklonile prepreke za saradnju i razmenu tajnih podataka sa drugim državama i međunarodnim organizacijama.

Zakon o tajnosti podataka uspostavlja jedinstven i sveobuhvatan sistem za određivanje, čuvanje, korišćenje, razmenu i prestanak tajnosti podataka od interesa za Republiku Srbiju. **Osnovni cilj ovog zakona je da zaštiti informacije koje su važne za nacionalnu i javnu bezbednost, odbranu, unutrašnje i spoljne poslove, kao i ustavni poredak, prava i slobode građana.** Pored nacionalnih podataka, zakon uređuje i postupanje sa stranim tajnim podacima koji su Srbiji povereni kroz međunarodnu saradnju. Zakon posebno definiše pojmove tajnih podataka, uslove pod kojima se podatak može klasifikovati, kao i kriterijume na osnovu kojih se određuje stepen tajnosti. Tajni podaci mogu biti označeni jednim od četiri stepena tajnosti<sup>8</sup>:

- ❖ **Državna tajna** - koji se određuje radi sprečavanja nastanka neotklonjive teške štete po interese Republike Srbije.
- ❖ **Strogo poverljivo** - koji se određuje radi sprečavanja nastanka teške štete po interese Republike Srbije.
- ❖ **Poverljivo** - koji se određuje radi sprečavanja nastanka štete po interese Republike Srbije.
- ❖ **Interno** - koji se određuje radi sprečavanja nastanka štete za rad, odnosno obavljanje zadataka i poslova organa javne vlasti koji ih je odredio.

**Rokovi čuvanja** zavise od stepena tajnosti i kreću se od dve godine za najniži stepen do trideset godina za najviši, uz mogućnost produženja u izuzetnim okolnostima. Tajnost prestaje istekom roka, nastupanjem određenog događaja, opozivom ili ako su razlozi za tajnost prestali.

<sup>8</sup> Član 14. Zakona o tajnosti podataka: [https://www.paragraf.rs/propisi/zakon\\_o\\_tajnosti\\_podataka.html](https://www.paragraf.rs/propisi/zakon_o_tajnosti_podataka.html)

**Ovlašćenja za određivanje stepena tajnosti** imaju najviši državni funkcioneri, poput predsednika Republike, predsednika Narodne skupštine i predsednika Vlade, kao i rukovodioci organa javne vlasti i posebno ovlašćeni funkcioneri i zaposleni. Svaki organ javne vlasti odgovoran je za sprovođenje mera zaštite, uključujući fizičko-tehničke mere, IT i kriptozastitu, određivanje posebnih bezbednosnih zona i organizovanje obuke zaposlenih. Pored toga, rukovalac tajnim podacima ima dužnost da preduzima sve organizacione i tehničke mere radi sprečavanja neovlašćenog pristupa, gubitka i otkrivanja podataka.

**Posebno značajne uloge u primeni Zakona imaju Kancelarija Saveta za nacionalnu bezbednost i zaštitu tajnih podataka i Ministarstvo pravde**, o čemu će biti više reči u delu analize o nadzoru nad sprovođenjem zakona.

Najviši državni funkcioneri imaju pravo pristupa tajnim podacima bez sertifikata, dok ostalim licima pristup može biti omogućen samo uz posedovanje odgovarajućeg sertifikata. Sertifikate izdaje **Kancelarija Saveta za nacionalnu bezbednost i zaštitu tajnih podataka**, nakon sprovedene bezbednosne provere koju vrši nadležni bezbednosni organ, najčešće Bezbednosno-informativna agencija ili Ministarstvo unutrašnjih poslova. Bezbednosna provera može biti osnovna, potpuna ili posebna, u zavisnosti od stepena tajnosti podataka za koje se traži pristup. Pristup stranim tajnim podacima uređen je međunarodnim sporazumima i posebnim procedurama, a Kancelarija Saveta vodi centralni registar stranih tajnih podataka i vrši razmenu sa međunarodnim partnerima.

Nadzor nad sprovođenjem zakona poveren je **Ministarstvu pravde**, koje treba da prati celokupno stanje u oblasti zaštite tajnih podataka, kontroliše primenu kriterijuma za označavanje tajnosti, predlaže i priprema propise, daje mišljenja i preduzima mere u slučaju utvrđenih nepravilnosti. Ministarstvo je ovlašćeno da podnosi krivične prijave i pokreće prekršajne postupke kada organi javne vlasti ne postupaju u skladu sa zakonom. Ministarstvo pravde ima obavezu i podnošenja godišnjih izveštaja o aktivnostima u sprovođenju i kontroli primene ovog zakona odboru Narodne skupštine nadležnom za nadzor i kontrolu u oblasti odbrane i bezbednosti.

Zakon predviđa i sankcije za povrede i kršenje zakona, koje mogu biti krivične i prekršajne. Organi javne vlasti odgovaraju za brojne povrede, kao što su nepropisno određivanje stepena tajnosti, nesprovođenje periodične provere opravdanosti tajnosti, kao i nepostojanje propisanih mera zaštite. Rukovalac tajnim podacima koji ne preduzima potrebne mere zaštite može biti kažnjen novčanom kaznom od 5.000 do 50.000 dinara, dok je za teža kršenja Zakona predviđena krivična odgovornost i zatvorske kazne u rasponu od 3 meseca do 15 godina.

## Usklađivanje sa EU i međunarodna razmena tajnih podataka

Donošenje Zakona o tajnosti podataka bio je preduslov da Republika Srbija 2011. potpiše sporazum sa Evropskom unijom o bezbednosnim procedurama za razmenu i zaštitu tajnih podataka.<sup>9</sup> Sporazumom se definišu bezbednosne procedure za razmenu i zaštitu tajnih podataka sa EU, a odnosi se na tajne podatke ili materijale u bilo kom obliku i iz bilo koje oblasti koje Srbija i EU dostavljaju ili razmenjuju. Ovaj sporazum je i dalje na snazi, a u izveštajima Evropske Komisije za 2024. i 2025. se povodom ovoga samo konstatuje da „*Kad je reč o merama za zaštitu tajnosti, Srbija je nastavila da sprovodi svoj Sporazum sa EU o bezbednosnim procedurama za razmenu i zaštitu informacija sa oznakom tajnosti.*”<sup>10</sup>

Srbija je 2008. potpisala i Sporazum sa organizacijom Severnoatlantskog pakta (NATO) o bezbednosti informacija i kodeksa o postupanju, koji je potvrđen u Narodnoj Skupštini tek 2011. Njime se, kao i sporazumom sa EU, ustanovljavaju najopštije obaveze strana potpisnica u vezi sa razmenom i rukovanjem osetljivim, odnosno poverljivim podacima.

U prethodnim godinama, Srbija je potpisala i slične bilateralne sporazume sa Slovačkom, Bugarskom, Češkom, Slovenijom, Bosnom i Hercegovinom, Severnom Makedonijom, Rusijom, Poljskom, Francuskom, Španijom i drugima.<sup>11</sup>

Imajući u vidu, da većina dokumenata i izveštaja koje država izrađuje za potrebe pristupanja EU nisu javno dostupni, teško je oceniti u kojoj meri je Srbija usklađena sa standardima EU u ovoj oblasti.

Povlačeći paralele sa drugim sektorima, moguće je zaključiti da je i u oblasti tajnosti, neophodno dodatno **usaglašavanje sa međunarodnim standardima koji se ubrzano menjaju u eri digitalizacije**, jačanje kadrova radi primene novih standarda, i digitalno unapređivanje procesa rada.

Iz naučnog rada direktora Kancelarije Saveta bezbednosti i zaštite tajnih podataka o trendovima u oblasti bezbednosnih provera pripadnika Ministarstva unutrašnjih poslova (MUP), a u kontekstu sprovođenja Zakona o tajnosti podataka mogu se posredno utvrditi i kapaciteti državnih organa u ovoj oblasti. Ovaj rad konstatuje da međunarodna saradnja i potreba za dostizanjem međunarodnih standarda bitno utiče na izmene bezbednosne

<sup>9</sup> Na osnovu sporazuma donet je Zakon o potvrđivanju sporazuma između Republike Srbije i Evropske unije o bezbednosnim procedurama za razmenu i zaštitu tajnih podataka ("Sl. glasnik RS - Međunarodni ugovori", br. 1/2012) [http://demo.paragraf.rs/demo/combined/Old/t/t2012\\_03/t03\\_0077.htm](http://demo.paragraf.rs/demo/combined/Old/t/t2012_03/t03_0077.htm)

<sup>10</sup> Izveštaj Evropske komisije za Srbiju za 2024, str. 109:

[https://www.mei.gov.rs/upload/documents/eu\\_dokumenta/2024/izvestaj\\_24.pdf](https://www.mei.gov.rs/upload/documents/eu_dokumenta/2024/izvestaj_24.pdf)

Izveštaj Evropske komisije za Srbiju za 2025, str 118:

<sup>11</sup> Lista država sa kojima je potpisan sporazum, nalazi se na sajtu Kancelarija saveta za nacionalnu bezbednost i zaštitu tajnih podataka: <https://nsa.gov.rs/tekst/sr/81/međunarodni-sporazumi.php>

politike i institucionalne reforme, kao i postupke bezbednosne provere. U radu se između ostalog navodi i da je međunarodna saradnja jedan od važnijih razloga naglog skoka u broju izdatih sertifikata za pristup i rad sa tajnim podacima.<sup>12</sup> Kao izazovi za državne organe u oblasti tajnosti, kao i sistema tajnosti navode se: nedostatak stručnih kadrova, nedostatak sistemskih obuka i profesionalizacija kadrova, nejasno razgraničenje nadležnosti između MUP, BIA i Kancelarije Saveta za nacionalnu bezbednost i zaštitu tajnosti podataka, nedovoljna standardizacija postupanja, nizak stepen digitalizacije, decentralizovanost sistema i podataka, zastareli IT sistemi, nepovezanost baza podataka i ručna obrada informacija.<sup>13</sup>

---

<sup>12</sup> U periodu od 2019. do 2025, Kancelarija Saveta izdala je reko 18000 sertifikata za pristup tajnim podacima. Za više videti: prof. dr Goran Matić, Analiza trendova u bezbednosnim proverama pripadnika Ministarstva unutrašnjih poslova u kontekstu sprovođenja Zakona o tajnim podacima, (2019–2024) str 126, <https://scindeks-clanci.ceon.rs/data/pdf/0409-2953/2025/0409-29532503123M.pdf>

Sajt Kancelarije Saveta, izdat broj sertifikata po godinama: <https://nsa.gov.rs/tekst/sr/72/sertifikati.php>

<sup>13</sup> Za više videti: prof. dr Goran Matić, Analiza trendova u bezbednosnim proverama pripadnika Ministarstva unutrašnjih poslova u kontekstu sprovođenja Zakona o tajnim podacima, (2019–2024): <https://scindeks-clanci.ceon.rs/data/pdf/0409-2953/2025/0409-29532503123M.pdf>

## Nedostaci Zakona o tajnosti podataka i problemi u njegovoj primeni

### I. Zakonski tekst je previše sažet i oslanja se na veliki broj podzakonskih akata

Iako je uobičajeno da zakoni ne budu preopterećeni detaljnim procedurama, **analiza Zakona o tajnosti podataka pokazuje da je zbog nedostatka precizno definisanih normi, pojmova i kriterijuma njegova primena u praksi značajno otežana**. Već prilikom donošenja ovog zakona bilo je jasno da će se veliki deo materije uređivati podzakonskim aktima, čija je izrada unapred planirana. Međutim, ovakvo oslanjanje na sekundarno zakonodavstvo predstavlja ozbiljnu manjkavost.

Dodatni problem jeste što se na donošenje pojedinih podzakonskih akata **čekalo više od pet godina** nakon stupanja zakona na snagu.<sup>14</sup> Ovo kašnjenje nije samo tehničke prirode, ono je dovelo do perioda u kome su organi javne vlasti morali da primenjuju zakon bez adekvatnih smernica, standarda i procedura. Time je u praksi nastao vakuum u primeni, različita tumačenja, što je direktno suprotno principima pravne sigurnosti i predvidivosti.

Radi ilustracije da sveobuhvatna usaglašenost sa Zakonom o tajnim podacima nikada nije postignuta, važno je napomenuti da je tek prilikom poslednjih izmena Krivičnog zakonika (koje su i dalje u toku) predloženo prenošenje člana 98. Zakona o tajnosti podataka, koja se odnosi na krivičnu odgovornost, u Krivični zakonik.

Prekomerna razuđenost normativnih akata dovodi do pravne nesigurnosti i otežava doslednu primenu zakona, jer se ključni elementi sistema, uključujući kriterijume za klasifikaciju, postupke procene i zaštite tajnih podataka, postupci interne kontrole, izmeštaju u uredbe i pravilnike. Time se omogućava da se kroz podzakonske akte uređuje materija koja bi morala biti u domenu zakonodavne vlasti. Ovo ujedno podriva demokratski i participativni proces izrade javnih politika, jer donošenje i izmena podzakonskih akata ne zahtevaju javnu raspravu, uključivanje javnosti, niti parlamentarnu raspravu, već se sprovode isključivo voljom izvršne vlasti.

<sup>14</sup> Rodoljub Šabić, 2014, Pet godina „primene“ zakona o tajnosti podataka, Primena Zakona o tajnosti podataka, 10 najznačajnijih prepreka (zbornik radova), od str. 33 <http://repozitorijum.pravnifakultet.edu.rs/314/>

## Uvođenje tajnosti sektorskim zakonima

Odredbe o odnosu prema drugim zakonima posebno zakonima o bezbednosnim službama, i sektoru bezbednosti, kao i krivičnom postupku nisu sistematično „ukrštene“, zbog čega dejstvo *lex specialis* rešenja ostavlja prostor da se preko sektorskih zakona uvodi tajnost. Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti podneo je u junu 2018. Ustavnom sudu predloge za ocenu ustavnosti pojedinih odredbi Zakona o odbrani i Zakona o Bezbednosno-informativnoj agenciji, nakon izmena ovih zakona.<sup>15</sup> Poverenik je smatrao da su navedenim izmenama Ministarstvo odbrane, Vojska Srbije i BIA faktički izuzeti iz jedinstvenog sistema slobode pristupa informacijama i sistema zaštite tajnih podataka, čime se narušava koherentnost pravnog okvira u ovoj oblasti.

Ovim predlozima posebno su problematizovane odredbe koje omogućavaju Vladi da, na predlog Ministarstva odbrane, dodatno uređuje koje informacije se štite ili isključuju od pristupa javnosti, kao i rešenja kojima se dokumenti BIA klasifikuju prema vrsti, a ne prema sadržini. Takva rešenja su ocenjena kao suprotna Zakonu o slobodnom pristupu informacijama od javnog značaja, Zakonu o tajnosti podataka i članu 51. Ustava Republike Srbije, koji garantuje pravo na pristup informacijama u skladu sa zakonom.

Poverenik je ukazivao i na nesaglasnost pojedinih odredbi Zakona o odbrani sa Ustavom Republike Srbije, kojim se predviđa i demokratska i civilna kontrola Vojske Srbije, budući da se izmenama omogućava ograničavanje prava javnosti da zna van zakonom propisanih kriterijuma.

U godišnjem izveštaju Poverenika za 2019. se navodi da je inicijativa za ocenu ustavnosti odbačena.<sup>16</sup>

Pitanje prekomernog i neujednačenog širenja režima tajnosti otvorilo se i u procesu izrade novog Zakona o unutrašnjim poslovima<sup>17</sup>. Prema jednom od poslednjih nacrtu zakona u koji su istraživači imali uvid, predviđeno je da se ovim zakonom unapred definišu vrste podataka iz oblasti rada Ministarstva unutrašnjih poslova koje se smatraju tajnim. Jedno od rešenja jeste da pravilnik o sistematizaciji radnih mesta u MUP-u bude označen stepenom tajnosti.

Takav pristup predstavlja dodatno odstupanje od osnovnog principa da se tajnost određuje na osnovu sadržine informacije i procene štete, a ne prema vrsti dokumenta ili oblasti rada.

<sup>15</sup> Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti, Poverenik podneo predloge za ocenu ustavnosti Zakona o odbrani i Zakona o BIA, <https://www.poverenik.rs/sr-yu/saopstenja/2881>

<sup>16</sup> Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti, Izveštaj o radu za 2019, 2018, <https://www.poverenik.rs/images/stories/dokumentacija-nova/izvestajiPoverenika/2019/Izvestajza2019lat.pdf>

<sup>17</sup> Proces izmena ovog zakona traje već nekoliko godina, tokom kojih je javno bilo dostupno više nacrtu Zakona.

Time se dokument koji je po svojoj prirodi organizaciono-administrativni, i koji je od neposrednog značaja za razumevanje strukture i funkcionisanja organa, unapred izuzima iz režima javnih podataka.

Ovakva normativna rešenja dodatno učvršćuju trend institucionalnog zatvaranja i stvaranja paralelnih režima tajnosti unutar sektora bezbednosti, čime se sužava prostor za javni nadzor nad sektorom bezbednosti i otežava primena Zakona o slobodnom pristupu informacijama od javnog značaja.

## **II. Neprecizno i preširoko definisanje pojma tajnog podatka i kriterijuma za određivanje stepena tajnosti**

Jedan od ključnih nedostataka Zakona o tajnosti podataka odnosi se na način na koji je određen pojam tajnog podatka, odnosno interes koji država nastoji da zaštiti klasifikacijom informacija. Zakon u članovima 1, 2, i 8. polazi od kategorije „podatka od interesa za Republiku Srbiju“, ali ova sintagma, iako se u zakonu ponavlja više puta, nigde nije definisana. Time se već u polaznoj tački ostavlja širok i nedovoljno razgraničen normativni okvir za odlučivanje o tome šta uopšte može biti označeno stepenom tajnosti.

Član 2:

*tajni podatak je podatak od interesa za Republiku Srbiju koji je zakonom, drugim propisom ili odlukom nadležnog organa donesenom u skladu sa zakonom, određen i označen određenim stepenom tajnosti;*

Član 8:

### **Podatak koji se može odrediti kao tajni**

*Kao tajni podatak može se odrediti podatak od interesa za Republiku Srbiju čijim bi otkrivanjem neovlašćenom licu nastala šteta, ako je potreba zaštite interesa Republike Srbije pretežnija od interesa za slobodan pristup informacijama od javnog značaja.*

*Podaci iz stava 1. ovog člana odnose se naročito na:*

- 1) nacionalnu bezbednost Republike Srbije, javnu bezbednost, odnosno na odbrambene, spoljnospolitičke, bezbednosne i obaveštajne poslove organa javne vlasti;*
- 2) odnose Republike Srbije sa drugim državama, međunarodnim organizacijama i drugim međunarodnim subjektima;*



3) sisteme, uređaje, projekte, planove i strukture koji su u vezi sa podacima iz tač. 1) i 2) ovog stava;

4) naučne, istraživačke, tehnološke, ekonomske i finansijske poslove koji su u vezi sa podacima iz tač. 1) i 2) ovog stava.

Zakon nabroja oblasti u kojima podatak može biti klasifikovan: teritorijalni integritet i suverenost, ustavni poredak, javna i nacionalna bezbednost, odbrana, unutrašnji i spoljni poslovi i dr, ali ne razlaže šta tačno čini sadržinu tih interesa, niti daje jasne kriterijume za određivanje da li bi određeno otkrivanje informacija zaista moglo proizvesti štetu. Iako formulacija uključuje element štete i obavezu balansiranja sa pravom javnosti da zna, ona je istovremeno **preopšta** i ostavlja široku diskreciju organima da tumače kada je „interes države“ pretežniji. Ovako široko postavljena norma znatno odstupa od evropskih standarda koji zahtevaju **jasnu, taksativnu i predvidivu definiciju zaštićenih interesa**.

Sličan problem javlja se i kod definisanja **stepena tajnosti**. Član 14. Zakona propisuje četiri stepena (DRŽAVNA TAJNA, STROGO POVERLJIVO, POVERLJIVO i INTERNO) i povezuje ih sa vrstom štete koja bi nastala otkrivanjem informacije. Međutim, i ovde je reč o **opštim, načelnim kategorijama** „teška šteta“, „šteta“, „šteta za rad organa“, bez konkretnog objašnjenja šta ovi pojmovi obuhvataju u praksi.

Naknadna razrada ovih kriterijuma prepuštena je podzakonskim aktima<sup>18</sup>, što dodatno slabi jasnoću i konzistentnost sistema. Iako uredbe, koje je izradila Vlada sadrže detaljnije liste mogućih posledica (npr. ugrožavanje suvereniteta, ekonomskih interesa, aktivnosti bezbednosnih službi, međunarodne saradnje, kulturnog nasleđa, finansijskog poslovanja organa, pa čak i narušavanje poverenja građana u rad institucije), **ove liste su veoma široke i raznorodne da gotovo svaka informacija može potencijalno biti označena kao tajna**.

Na primer, kriterijumi za određivanje stepena „POVERLJIVO“ u uredbama obuhvataju sve od ugrožavanja ustavnog poretka i ljudskih života, preko ekonomskih interesa države, do saradnje sa drugim državama, sudskih postupaka, aktivnosti bezbednosnih službi, pa čak i „negativan uticaj na materijalno-finansijsko poslovanje“ organa. U sferi „INTERNO“ dovoljna je mogućnost „smanjenja operativnih sposobnosti organa“ ili „narušavanje poverenja građana“.

**Prema zakonu, stepen tajnosti „INTERNO“ se koristi kada bi otkrivanje informacije izazvalo „štetu za rad organa javne vlasti.“ Međutim, ovakav standard je previše širok i**

<sup>18</sup> Linkovi do uredbi kojima se određuju kriterijumi za određivanje stepena tajnosti dostupni su na sajtu Kancelarije saveta za nacionalnu bezbednost i zaštitu tajnosti: <https://nsa.gov.rs/tekst/sr/576/domace-zakonodavstvo.php>

**neprecizan, jer šteta za rad organa ne mora nužno predstavljati štetu po državne interese, što je osnovni uslov za primenu tajnosti.** Takve formulacije su izuzetno rastegljive, pa pod oznakom „INTERNO“ može završiti veliki broj informacija koje u međunarodnim praksama ne potpadaju pod klasifikaciju tajnosti. **Ovaj stepen tajnosti stoga postaje mesto sudara između podataka od javnog značaja i tajnih podataka.** Reč je o podacima koji po pravilu ne bi trebalo da budu tajni, ali ih organi često nastoje zaštititi kako bi ograničili pristup javnosti. Zbog toga se u mnogim pravnim sistemima kategorija „RESTRICTED“ (kojoj „INTERNO“ odgovara u NATO i EU sistemu) i ne tretira kao tajna informacija, već kao posebna kategorija ograničenog pristupa.<sup>19</sup>

**Kako je upravo ovakvih podataka najviše u svakodnevnom radu uprave, to otvara i najveće mogućnosti za zloupotrebe.**

Ovakva normativna rešenja imaju nekoliko ozbiljnih posledica:

- ❖ **Dozvoljavaju nesrazmerno široku primenu Zakona o tajnosti podataka,** uključujući na informacije koje po međunarodnim standardima ne bi trebalo da budu tajne, poput budžetskih podataka, ugovora, upravnih odluka ili statističkih informacija.
- ❖ **Onemogućavaju predvidivost,** jer građani, ali ni organi javne vlasti, nemaju pouzdan pravni kriterijum na osnovu kojeg mogu proceniti da li informacija ispunjava uslove za klasifikaciju.
- ❖ **Otežava nadzor nad opravdanošću tajnosti,** budući da nadzorni organi u praksi treba da ocenjuju veoma neprecizne pojmove poput „štete po interese Republike Srbije“ ili „narušavanja poverenja u rad organa.“
- ❖ **Narušava načelo transparentnosti,** jer široko definisani kriterijumi otvaraju mogućnost da se oznaka tajnosti koristi kao sredstvo prikrivanja nepravilnosti ili izbegavanja javne kontrole.

Stoga, srpski sistem definisanja tajnih podataka i stepena tajnosti ostaje **preširok, nedovoljno precizan i zavisao od podzakonskih akata,** što značajno umanjuje kvalitet normativnog okvira i povećava rizik od zloupotrebe.

<sup>19</sup> Veljko Porobić, Pravni aspekti tajnosti i zaštite tajnih podataka u Republici Srbiji, Univerzitet u Beogradu, Terorizam, organizovani kriminal i bezbednost 2017.

### III. Nadzor nad primenom zakona

Pitanje nadzora nad primenom Zakona zasigurno je najslabija karika ovog Zakona. Kroz svoj istraživački rad, Partneri Srbija često su isticali ovo kao glavni nedostatak Zakona o tajnosti podataka, pre svega u delu koji se odnosi na nadzor koji treba da sprovodi Ministarstvo pravde.

Za potrebe detaljnijeg osvrta u ovoj analizi pitanje nadzora će biti raščlanjeno na:

1. Interni nadzor (Unutrašnja kontrola)
2. Ulogu Kancelarije Saveta
3. Nadzor koji treba da sprovodi Ministarstvo pravde
4. Ulogu Narodne skupštine

#### Interni nadzor

Zakon o tajnosti podataka predviđa da je za unutrašnju kontrolu nad primenom zakona odgovoran rukovodilac organa javne vlasti (član 84). Istovremeno, prema članu 9, upravo je rukovodilac jedan od ovlašćenih subjekata za određivanje tajnosti podataka, kao i za prenošenje ovlašćenja na druga lica u organu. Time se uspostavlja sistem u kojem **isto lice koje donosi odluke o označavanju podataka stepenom tajnosti ujedno vrši i unutrašnju kontrolu zakonitosti i opravdanosti tih odluka.**

Ovakvo rešenje otvara ozbiljan **konflikt interesa**: rukovodilac je istovremeno i klasifikator i nadzornik sopstvenog postupanja. U praksi to znači da je teško očekivati objektivnu procenu opravdanosti klasifikacije, a posebno identifikovanje grešaka ili zloupotreba u primeni tajnosti. Kako zakon ne propisuje **obavezu** uključivanja nezavisnih ili odvojenih unutrašnjih kontrolnih mehanizama, ovaj tip nadzora ostaje suštinski **autokontrola**, što je suprotno međunarodnim standardima transparentnosti i odgovornosti.

Zakon nominalno predviđa mogućnost da se u pojedinim organima (MUP, Ministarstvo odbrane, BIA) formiraju posebna radna mesta ili organizacione jedinice zadužene za unutrašnju kontrolu. Međutim, ove jedinice su deo hijerarhijske strukture istog organa i podređene su rukovodiocu koji donosi odluke o klasifikaciji. Time se ne obezbeđuje potrebna organizaciona i funkcionalna nezavisnost kontrolnog mehanizma.

Dometi ovakve kontrole su stoga vrlo ograničeni:

- ❖ nadzor često ima formalni karakter i retko dovodi u pitanje opravdanost klasifikacije,

- ❖ postoji visok rizik od potvrđivanja postojećih odluka bez stvarnog ispitivanja njihove zakonitosti,
- ❖ interno preispitivanje se svodi na administrativnu proveru postupka, a ne na suštinsku kontrolu kriterijuma,
- ❖ mogućnost da unutrašnja kontrola otkrije i sankcioniše neopravdanu ili prekomernu klasifikaciju je objektivno mala.

## Uloga Kancelarije Saveta

Kancelarija Saveta za nacionalnu bezbednost i zaštitu tajnih podataka, iako formalno nema nadzornu ulogu nad primenom Zakona o tajnosti podataka, u praksi predstavlja **jedinu instituciju koja poseduje pregled nad sistemom zaštite tajnih podataka u Republici Srbiji**. Njene zakonske nadležnosti obuhvataju izdavanje bezbednosnih sertifikata i dozvola, obezbeđivanje primene standarda, sprovođenje međunarodnih obaveza, vođenje Centralnog registra stranih tajnih podataka, koordinaciju sa stranim i međunarodnim organima, obuku korisnika, opoziv tajnosti i niz drugih poslova koji su ključni za funkcionisanje sistema.<sup>20</sup>

Ovaj širok skup operativnih i tehničkih nadležnosti čini Kancelariju faktičkim „čvorištem“ celokupnog režima tajnosti podataka. Ona raspolaže informacijama o tome koliko se i kako klasifikuje, ko ima pristup, kako se sprovode međunarodni standardi, koji organi ispunjavaju svoje obaveze, a gde postoje odstupanja ili greške. Upravo zbog centralne pozicije i jedinstvenog uvida, Kancelarija je u najboljoj poziciji da uoči systemske nedostatke, negativne prakse i da predlaže unapređenja.

Međutim, uprkos toj ulozi, zakon joj **ne daje formalna nadzorna ovlašćenja**. Kancelarija ne može kontrolisati pravilnost označavanja stepena tajnosti od strane drugih organa, ne može ukidati neosnovane oznake po sopstvenoj inicijativi (osim u uskim slučajevima vezanim za međunarodne obaveze), niti može vršiti inspekcijski nadzor nad sprovođenjem zakona. Njena uloga je pretežno operativna, tehnička i koordinatorska, a ne regulatorna niti nadzorna.

To znači da u sistemu postoji **paradoks**: institucija koja ima najširi uvid u stanje u oblasti tajnosti podataka nema ovlašćenja da utiče na to da se uočene nepravilnosti i zloupotrebe zaista otklone. U praksi, Kancelarija može ukazivati na probleme, obučavati korisnike i predlagati mere unapređenja, ali ne i obavezati organe da otklone nedostatke ili preduzmu

<sup>20</sup> Za više informacija pogledati: Prof. dr Goran D. Matić, Vodič kroz rad Saveta za nacionalnu bezbednost, [https://nsa.gov.rs/extfile/sr/5097/Vodic\\_kroz%20rad\\_KSNB.pdf](https://nsa.gov.rs/extfile/sr/5097/Vodic_kroz%20rad_KSNB.pdf)

mere korekcije. Time se ograničava njena mogućnost da doprinese stvarnom jačanju integriteta sistema.

Istorijski kontekst takođe objašnjava ovaj institucionalni položaj. Kancelarija je formirana kao stručna i administrativna podrška Savetu za nacionalnu bezbednost i Birou za koordinaciju rada službi bezbednosti, čiji je zadatak koordinacija aktivnosti bezbednosnog sektora. Kao takva, Kancelarija je strukturirana pretežno kao **operativno telo izvršne vlasti**, a ne kao nezavisni nadzorni organ, koji postoji u mnogim državama EU u različitim modalitetima (misli se na nacionalne bezbednosne institucije- National Security Authority, skraćeno NSA).

Uporedna praksa pokazuje da u delu evropskih zemalja institucije koje imaju ulogu ekvivalenta Kancelariji (NSA modeli u državama članicama EU i NATO) istovremeno poseduju i određeni stepen nadzornih ili regulatornih ovlašćenja, uključujući pravo da vrše kontrolu primene klasifikacije, nalože otklanjanje nepravilnosti, daju obavezujuće smernice i drugo.<sup>21</sup>

U Češkoj, na primer, NSA vrši kontrolu i inspekcijski nadzor nad primenom propisa o zaštiti klasifikovanih informacija, sprovodi bezbednosne provere i izdaje sertifikate, vodi nacionalni registar klasifikovanih podataka, nalaže otklanjanje nepravilnosti i može odrediti mere za unapređenje sistema, i obavlja druge poslove koji spadaju u isti domen.<sup>22</sup>

### Nadzor koji treba da sprovodi Ministarstvo pravde

Zakon o tajnosti podataka predviđa da nadzor nad sprovođenjem zakona vrši Ministarstvo pravde, **kojem se poverava širok i suštinski ambiciozno postavljen skup nadležnosti**. Ovaj organ zadužen je da prati stanje u oblasti zaštite tajnih podataka, priprema i daje mišljenja na propise, kontroliše primenu kriterijuma za određivanje stepena tajnosti i sprovodi kontrolu mera obezbeđenja, obrade, korišćenja i razmene tajnih podataka. Ministarstvo je ovlašćeno da vrši nadzor bez prethodnog obaveštavanja organa javne vlasti, da nalaže mere za unapređenje zaštite, da pokreće krivične i prekršajne postupke zbog povreda zakona, kao i da jednom godišnje izveštava Narodnu skupštinu o aktivnostima u oblasti kontrole primene zakona. Zakon predviđa i ustanovljavanje posebno ovlašćenih lica za nadzor nad primenom Zakona o tajnosti podataka, koja prolaze bezbednosne provere i postupaju po pravilima inspekcijskog nadzora.

<sup>21</sup> Za više pogledati: Prof. dr Goran D. Matić, Vodič kroz rad Saveta za nacionalnu bezbednost, u ovoj publikaciji je detaljnije predstavljen odnos između Saveta za nacionalnu bezbednost, kancelarija saveta, njihovih oblašćenja kao i njihovih ekvivalenata u drugim državama sveta: [https://nsa.gov.rs/extfile/sr/5097/Vodic\\_kroz%20rad\\_KSNB.pdf](https://nsa.gov.rs/extfile/sr/5097/Vodic_kroz%20rad_KSNB.pdf)

<sup>22</sup> Češki zakon o tajnosti podataka- Act N 412/2005 Coll on the Protection of Classified Information, član 143 i drugi, [https://www.nbu.cz/images/download/act\\_on\\_CI\\_protection.pdf](https://www.nbu.cz/images/download/act_on_CI_protection.pdf)

Na nivou normativnog dizajna, ovaj sistem izgleda snažno i delotvorno: Ministarstvo pravde trebalo bi da bude centralna institucija koja obezbeđuje zakonitost i pravilno postupanje u celom režimu zaštite tajnih podataka. Iako je formalno u Ministarstvu uspostavljena **Grupa za nadzor nad tajnošću podataka**, ova organizaciona jedinica u praksi obavlja samo normativne i proceduralne poslove (učestvovanje u pripremi propisa, vođenje evidencija, praćenje stanja), ali **ne vrši suštinski inspekcijski nadzor**. Važno je istaći i da ova grupa ima svega 3 zaposlena, prema Pravilniku o unutrašnjem uređenju i sistematizaciji radnih mesta u Ministarstvu pravde iz 2023<sup>23</sup>.

Ministarstvo pravde godinama ne sprovodi nadzor nad primenom Zakona o tajnosti podataka, iako je ta obaveza eksplicitno utvrđena. U odgovorima na zahteve za pristup informacijama od javnog značaja koje su dobili Partneri Srbija iz 2017, 2020, 2021. i 2025, **Ministarstvo potvrđuje da nadzor nije vršen kao i većina nadležnosti iz člana 97.**

**Kao objašnjenje za potpuni izostanak nadzora, Ministarstvo godinama navodi identične systemske probleme.** Prvi od njih odnosi se na navodnu nejasnoću u pogledu odnosa između Zakona o inspekcijskom nadzoru i Zakona o tajnosti podataka, konkretno, da li se odredbe o polaganju ispita za inspektora primenjuju i na lica koja vrše nadzor nad tajnim podacima i da li se ova vrsta nadzora može smatrati „inspekcijom“ u formalno-pravnom smislu. Drugi navodni problem tiče se mogućnosti pristupa sadržini tajnih dokumenata: Ministarstvo tvrdi da Zakon o tajnosti podataka ne propisuje izričito da ovlašćeni nadzorni službenici imaju pravo uvida u konkretne klasifikovane dokumente, te da bi nadzirani organ mogao da uskrati taj pristup, čime bi nadzor bio faktički onemogućen. Ministarstvo dodatno ukazuje na obimnost i složenost nadzora, jer bi on podrazumevao analizu velikog broja dokumenata označenih različitim stepenima tajnosti, kao i kontrolu njihovog celokupnog životnog ciklusa.<sup>24</sup>

„Rešenje za ova pitanja Ministarstvo pravde vidi u izmenama i dopunama Zakona o tajnosti podataka. Iz dopisa Ministarstva pravde (12.04.2021. godine), sa rešenjem o obrazovanju posebne radne grupe (19.09.2018. godine), kao i iz godišnjeg izveštaja o radu Kancelarije Saveta za nacionalnu bezbednost i zaštitu tajnih podataka za 2019. godinu, saznaje se da je posebna radna grupa za pripremu radne verzije teksta Zakona o izmenama i dopunama Zakona o tajnosti podataka, koju je obrazovalo i kojom je rukovalo Ministarstvo pravde, počela sa radom 2018. godine, ali da tokom 2019. i 2020. godine sastanci ove radne grupe nisu održavani, iz više razloga, uključujući i vanredno stanje i ukupne vanredne okolnosti vezane za pandemiju, odnosno epidemiju većeg epidemiološkog značaja zarazne bolesti COVID-19 izazvane virusom SARS-CoV-2, kao i parlamentarne izbore, formiranje Vlade i kadrovske promene u organima državne uprave i drugim državnim organima, čiji

<sup>23</sup> Pravilnik o unutrašnjem uređenju i sistematizaciji radnih mesta u Ministarstvu pravde:

<https://informator.poverenik.rs/informator?org=wfcMTJAMmby8vpZHF&ch=B7e85r4rMtMRMMyzb7&code=>

<sup>24</sup> Za više pogledati analizu organizacije Partneri Srbija gde su predstavljeni odgovori na zahteve: Primena Zakona o tajnosti podataka u Republici Srbiji, 2021, <https://www.partners-serbia.org/public/news/primena-zakona-o-tajnosti-podataka.pdf>

predstavnicima su članovi posebne radne grupe, te da je ova posebna radna grupa 2020. godine faktički prestala s radom.“<sup>25</sup> Iz odgovora (oktobar 2025) na zahtev za pristup informacijama od javnog značaja koji je podnet Ministarstvu pravde u okviru ovog istraživanja<sup>26</sup>, saznajemo da je formirana nova radna grupa za rad na izmenama Zakona o tajnosti podataka, čiji sastav, mandat i dokumenti nisu javno dostupni, suprotno propisima o izradi i izmeni zakona.

Ministarstvo pravde ne objavljuje godišnje izveštaje o radu pa je teško proceniti šta je sve u ovoj oblasti rađeno da se sistem nadzora nad tajnim podacima unapredi. Ministarstvo pravde objavljuje Informatore o radu, u kojima nema informacija o aktivnosti Ministarstva u oblasti tajnosti podataka. Ono što još više zabrinjava jeste da se u srednjoročnim planovima Ministarstva pravde za period 2023-2025; 2024-2026. i 2025-2027.<sup>27</sup> tajnost podataka uopšte ne spominje, odnosno nije mapirana kao prioritarna oblast uprkos tome što sistem nadzora u ovoj oblasti ne funkcioniše godinama.

Posledice ovakve institucionalne paralize su višestruke i ozbiljne. Pre svega, nepostojanje nadzora omogućava organima javne vlasti da proizvoljno označavaju podatke stepenima tajnosti, bez ikakvog spoljašnjeg korektiva koji bi mogao sprečiti zloupotrebe ili preteranu klasifikaciju. To direktno ugrožava pravo javnosti na pristup informacijama, jer omogućava da se širok spektar podataka, uključujući one od značaja za javnu kontrolu rada vlasti, neopravdano sakrije iza režima tajnosti. Pored toga, nesprovođenje nadzora slabi efikasnost sistema zaštite tajnih podataka: bez kontrole nad merama obezbeđenja, pristupa i razmene povećava se rizik od gubitka, zloupotrebe ili neovlašćenog otkrivanja informacija koje zaista jesu od vitalnog značaja za nacionalnu i javnu bezbednost. Odsustvo nadzora takođe dovodi Srbiju u nesklad sa obavezama prema NATO-u i Evropskoj uniji, koje zahtevaju postojanje funkcionalnog, nezavisnog i tehnički kompetentnog nadzornog tela.

Sve navedeno otvara pitanje da li Ministarstvo pravde uopšte treba da bude nadležni organ za nadzor nad primenom Zakona o tajnosti podataka. Ministarstvo pravde nema tehničke kapacitete niti se prema institucionalnim nadležnostima uklapa u profil organa koji obavlja ovakav tip nadzora, a činjenica da kapaciteti nisu izgrađeni ni posle 15 godina od donošenja zakona, ukazuje da je ovakvo rešenje pogrešno.

Stoga se nameće zaključak da bi buduća reforma morala da razmotri prenošenje nadzornih funkcija na specijalizovanu instituciju, poput osnažene Kancelarije Saveta za nacionalnu bezbednost ili posebno ustanovljene nacionalne bezbednosne uprave. Sve dok nadzor ostaje u nadležnosti organa koji nema kapacitete za ovu ulogu i koji je praktično odustao od

<sup>25</sup> Partneri Srbija, Primena Zakona o tajnosti podataka u Republici Srbiji, 2021, str 20, <https://www.partners-serbia.org/public/news/primena-zakona-o-tajnosti-podataka.pdf>

<sup>26</sup> Ministarstvo pravde odgovor: [https://foi.partners-serbia.org/wp-content/uploads/prilog\\_310/Odgovor%20Ministarstvo%20pravde.pdf](https://foi.partners-serbia.org/wp-content/uploads/prilog_310/Odgovor%20Ministarstvo%20pravde.pdf)

<sup>27</sup> Srednjoročni planovi Ministarstva pravde se nalaze na sledećem linku: <https://www.mpravde.gov.rs/tekst/38873/srednjorocni-plan-ministarstva-pravde.php>



njegovog vršenja, sistem zaštite tajnih podataka u Srbiji ostaje ozbiljno oslabljen, neefikasan i podložan zloupotrebama.

### Uloga Narodne skupštine

Zakonom o tajnosti podataka, u članu 94, propisano je da Ministarstvo pravde podnosi godišnje izveštaje o aktivnostima u sprovođenju i kontroli primene ovog zakona odboru Narodne skupštine nadležnom za nadzor i kontrolu u oblasti odbrane i bezbednosti. Na ovaj način uspostavljen je mehanizam parlamentarnog nadzora kojim Narodna skupština, kao posebna grana vlasti, kontroliše rad izvršne vlasti u ovoj oblasti.

Nadležni skupštinski odbor, Odbor za odbranu i unutrašnje poslove, se tokom 2025. sastao 11 puta.<sup>28</sup> Međutim, prema javno dostupnim informacijama, u tom periodu Izveštaj Ministarstva pravde o primeni Zakona o tajnosti podataka za 2024. nije bio predmet razmatranja.

Sa druge strane, Odbor je redovno razmatrao izveštaje o radu Ministarstva unutrašnjih poslova, najčešće na kvartalnom nivou, dok su izveštaji o radu Ministarstva odbrane razmatrani ređe. Tokom 2025. Odbor je takođe razmatrao predloge zakona iz oblasti odbrane i vojske, kao i predloge zakona o međunarodnoj saradnji u oblasti odbrane i bezbednosti. Kao što je već navedeno, Ministarstvo pravde ne objavljuje redovno izveštaje o radu na svom sajtu, tako da ne možemo utvrditi da li izveštaji o radu Ministarstva pravde nisu razmatrani od strane Odbora zato što uopšte i nisu izrađeni, ili postoje drugi razlozi zbog kojih nadležni odbor nije u 2025. razmatrao izveštaj o radu Ministarstva pravde u oblasti tajnosti za 2024. godinu.

Tokom godina primene Zakona o tajnosti podataka otvorilo se i pitanje na koji način narodni poslanici dobijaju sertifikate za pristup tajnim podacima. Poslanicima koji su članovi Odbora za odbranu i unutrašnje poslove i Odbora za kontrolu službi bezbednosti sertifikati su neophodni kako bi mogli da imaju uvid u tajne podatke koje im nadležni organi dostavljaju na razmatranje, uključujući izveštaje o stanju bezbednosti, izveštaje o radu službi bezbednosti i druga relevantna dokumenta.

Prema Zakonu o tajnosti podataka, bezbednosnu proveru za pristup tajnim podacima dokumentima stepena tajnosti „DRŽAVNA TAJNA“ i „STROGO POVERLJIVO“, koja prethodi izdavanju sertifikata za pristup tajnim podacima, sprovodi Bezbednosno-informativna agencija (BIA). Bezbednosnu proveru za pristup tajnim podacima i dokumentima stepena tajnosti „POVERLJIVO“ i „INTERNO“ sprovodi ministarstvo nadležno za unutrašnje poslove.

<sup>28</sup> Sajt Narodne skupštine, odeljak aktivnosti odbora, poslednji put pristupljeno sajtu 20.12.2025:  
<http://www.parlament.gov.rs/aktivnosti/narodna-skup%C5%A1tina/radna-tela/odbori-pododbori-radne-grupe.954.html>



Ovakvo zakonsko rešenje otvara ozbiljno pitanje sukoba interesa i funkcionalne nezavisnosti parlamentarnog nadzora, budući da su upravo organi čiji rad narodni poslanici nadziru kroz skupštinske odbore ovlašćeni da sprovedu bezbednosne provere i, posredno, odlučuju o njihovom pristupu tajnim podacima. Time se stvara potencijal za institucionalnu zavisnost i narušava se osnovni princip kontrole izvršne vlasti od strane zakonodavne, jer pristup informacijama koje su ključne za efektivan nadzor može biti ograničen ili uslovljen odlukama organa koji su predmet tog nadzora.

Ovim pitanjem se godinama bavila i grupa organizacija iz Koalicije prEUgovor<sup>29</sup>, zbog sumnji da se poslanicima opozicije namerno uskraćuju sertifikati kako ne bi mogli da sprovedu nadzor. U vezi sa tim Koalicije je 2023. slala zahteve za pristup informacijama Narodnoj skupštini i Kancelariji saveta za bezbednost i zaštitu tajnosti podataka u cilju da dobije informacije o imenima poslanika koji imaju sertifikate za pristup tajnim podacima, međutim obe institucije su odbile da im dostave ove informacije. Ovaj konkretan slučaj će biti detaljnije razmatran u delu analize „Perspektiva civilnog sektora i novinara“.

Odugovlačenje sa dodelom sertifikata za pristup tajnim podacima iskusio je i bivši Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti Rodoljub Šabić, koji se u 2018. ovim povodom obratio BIA i pismom, ali i saopštenjem u kom je tražio da se bezbednosti postupak što pre sprovede.<sup>30</sup>

#### **IV. Kaznene norme- odsustvo krivične (ozbiljne) odgovornosti za nezakonito označavanje podataka kao tajnih**

Kaznene odredbe Zakona o tajnosti podataka zasnovane su na klasičnom, tradicionalnom shvatanju zaštite tajnih podataka, prema kojem je najveća opasnost neovlašćeno otkrivanje podataka koji već jesu zakonito klasifikovani. Stoga Zakon o tajnosti podataka veoma detaljno reguliše krivičnu i prekršajnu odgovornost u tom domenu.

Krivična odgovornost je predviđena za onoga ko neovlašćeno nepozvanom licu saopšti, preda ili učini dostupnim podatke ili dokumenta koji su mu povereni ili do kojih je na drugi način došao ili pribavlja podatke ili dokumenta, a koji predstavljaju tajne podatke. Visina kazne zavisi od nekoliko faktora: kog je stepena tajni podatak (za najviši stepen najveća zatvorska kazna od jedne do deset godina); zatim ukoliko je delo učinjeno iz koristoljublja ili

<sup>29</sup> Koaliciju prEUgovor čini sedam organizacija civilnog društva iz Srbije koje su stručne za različite politike u okviru poglavlja 23 i 24 pregovora o članstvu u Evropskoj uniji: <https://www.preugovor.org/prEUgovor/121/O-nama.shtml> U izveštajima Koalicije se ovo pitanje često razmatra, pogledati PREUGOVOR alarm-izveštaj o napretku Srbije u klasteru 1, 2023, str 32: <https://www.preugovor.org/Alarm-izvestaji/1809/Izvestaj-koalicije-prEUgovor-o-napretku-Srbije-u.shtml>

<sup>30</sup> Insajder, „Bez objašnjenja nadležnih zašto se Šabiću ne izdaje bezbednosni sertifikat“: <https://www.insajder.net/najvaznije-vesti/bez-objasnjenja-nadleznih-zasto-se-sabicu-ne-izdaje-bezbednosni-sertifikat>

radi objavljivanja ili korišćenja tajnih podataka u inostranstvu ili je izvršeno za vreme ratnog ili vanrednog stanja zatvorske kazne se povećavaju spram stepena tajnosti podataka (za najviši stepen tajnosti kazna je od pet do petnaest godina zatvora).

Zakon o tajnosti podataka propisuje prekršajnu odgovornost **odgovornog lica u organu javne vlasti**, koje se novčano kažnjava ukoliko povredi propise o klasifikaciji, obeležavanju, čuvanju, korišćenju i zaštiti tajnih podataka. Odgovorno lice je definisano: to je rukovodilac organa ili drugo lice koje je ovlašćeno da organizuje, nadzire ili odlučuje o primeni sistema tajnosti u organu.

Prekršaji obuhvataju širok spektar radnji i propusta, a mogu se svrstati u četiri kategorije:

1. **Neosnovano ili nepravilno određivanje tajnosti,**
2. **Neizvršavanje obaveza u vezi sa trajanje i promenom klasifikacije,**
3. **Propusti u sprovođenju mera zaštite i kontrole,**
4. **Nepravilnosti u postupanju sa sertifikatima, evidencijama i pristupom tajnim podacima.**

Zakon sankcioniše kako aktivne zloupotrebe (npr. neopravdano označavanje podataka kao tajnih ili određivanje pogrešnog stepena tajnosti), tako i pasivne propuste (poput propuštanja da se izvrše periodične procene, sprovede unutrašnja kontrola ili čuva evidencija). Prekršaji obuhvataju i situacije kada odgovorno lice propusti da opozove tajnost po isteku roka, događaja ili po nalogu Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti (Poverenik) ili suda, kao i kada nepravilno dostavlja ili uskraćuje pristup tajnim podacima. Dodatno, kažnjivo je i nepravilno postupanje sa sertifikatima za pristup tajnim podacima, kao i neobezbeđivanje propisanih opštih i posebnih mera zaštite.

**Međutim, Zakon gotovo potpuno izostavlja drugi, savremeni i jednako ozbiljan rizik: namerno ili neosnovano označavanje podataka kao tajnih.** Iako ovakvo postupanje ne predstavlja otkrivanje tajnih podataka, njegova štetnost može biti jednaka ili čak veća, posebno u demokratskim društvima u kojima transparentnost predstavlja ključni mehanizam kontrole vlasti i sprečavanja korupcije.

Za razliku od krivičnih odredaba za otkrivanje tajnih podataka koje su visoke, sankcije za nezakonitu klasifikaciju svode se isključivo na prekršajnu odgovornost, i to u obliku novčane kazne od 5.000 do 50.000 dinara. Te kazne primenjuju se na odgovorno lice u organu javne vlasti koje označi podatke kao tajne kada za to ne postoje zakonski uslovi, odredi pogrešan stepen tajnosti, ne izvrši periodičnu reviziju tajnosti, ne opozove tajnost po isteku roka ili

događaja, ili na druge načine ne primeni zakonom propisane obaveze u vezi sa klasifikacijom i zaštitom podataka.

Ovakav pristup stvara ozbiljan normativni nesklad. Dok je otkrivanje zakonito klasifikovanog podatka strogo kažnjivo, zloupotreba klasifikacije, koja često predstavlja način skrivanja korupcije, nezakonitosti ili neefikasnosti u radu organa, sankcioniše se tek simboličnom kaznom. **Time zakon štiti samo jedan aspekt državnog interesa, dok drugi aspekt, interes javnosti da zna, interes države da spreči zloupotrebe koje mogu imati podjednako štetne posledice po „državne interese”, kao i interes celog sistema za očuvanjem poverenja građana, ostaje praktično nezaštićen.**

Neosnovana tajnost ima potencijal da ugrozi javni interes jednako kao i curenje legitimno tajnih podataka. Korišćenje oznake tajnosti kao sredstva prikrivanja nezakonitih radnji, zloupotreba javnih resursa, nepravilnosti u javnim nabavkama ili sporne političke odluke može dovesti do dugoročnog urušavanja institucija, izbegavanja odgovornosti i uništavanja mehanizama kontrole vlasti. U svim tim situacijama šteta po državne interese nije samo moguća, već realna i ozbiljna.

**Kada se ima u vidu struktura krivične norme iz člana 98, postaje jasno da zakon polazi od pretpostavke da je svaka klasifikacija zakonita i opravdana. Zakon kažnjava otkrivanje tajnog podatka, ali uopšte ne razmatra mogućnost da je neki podatak pogrešno ili zlonamerno označen kao tajan.** U praksi to znači da čak i ako organ nezakonito proglasi tajnim podatak koji je od visokog javnog interesa (npr. ugovor o javnoj nabavci, odluku o trošenju budžetskih sredstava, podatke o istragama korupcije ili o radu bezbednosnih službi), odgovorno lice rizikuje samo prekršajnu kaznu koja je u većini slučajeva zanemarljiva, i često manja od novčanih naknada koje organi plaćaju advokatima ili troškova zastupanja.

Još ozbiljniji problem predstavlja činjenica da ne postoje nikakve krivične sankcije za namerni ili sistemski motivisani čin nezakonite klasifikacije, iako ovakvo postupanje direktno podriva ustavni poredak zasnovan na transparentnosti i odgovornosti vlasti.

Pored toga, izostanak krivičnih sankcija dodatno je problematičan u kontekstu činjenice da Ministarstvo pravde već godinama ne vrši nadzor nad zakonitošću određivanja tajnosti. Time prekršajna odgovornost ostaje neaktivna, jer nema organa koji bi utvrdio da je prekršaj uopšte učinjen.

## Odnos Zakona o tajnosti podataka i Zakona o slobodnom pristupu informacijama od javnog značaja

Zakon o tajnosti podataka, tajni podatak definiše u odnosu na interes za slobodan pristup informacija od javnog značaja. U članu 8. se navodi:

*“Kao tajni podatak može se odrediti podatak od interesa za Republiku Srbiju čijim bi otkrivanjem neovlašćenom licu nastala šteta, ako je potreba zaštite interesa Republike Srbije pretežnija od interesa za slobodan pristup informacijama od javnog značaja.”*

Ovo je posledica toga što je Zakon o slobodnom pristupu informacijama od javnog značaja (ZoSPIJZ) donet pre Zakona o tajnosti podataka. Time je prvo došlo do definisanja toga šta jeste informacija od javnog značaja (čl 2. ZoSPIJZ):

*„Informacija od javnog značaja, u smislu ovog zakona, jeste informacija kojom raspolaže organ javne vlasti, nastala u radu ili u vezi sa radom organa javne vlasti, sadržana u određenom dokumentu, a odnosi se na sve ono o čemu javnost ima opravdan interes da zna.*

*Da bi se neka informacija smatrala informacijom od javnog značaja nije bitno da li je izvor informacije organ javne vlasti ili koje drugo, lice, nije bitan nosač informacija (papir, traka, film, elektronski mediji i sl.) na kome se nalazi dokument koji sadrži informaciju, datum nastanka informacije, način saznavanja informacije, niti su bitna druga slična svojstva informacije.”*

Dalje se u ZoSPIJZ propisuje da javnost uvek ima pravo na informacije o radu organa javne vlasti, a da se prava iz ovog zakona mogu izuzetno podvrći ograničenjima propisanim ovim zakonom ako je to neophodno u demokratskom društvu radi zaštite od ozbiljne povrede pretežnijeg interesa zasnovanog na Ustavu ili zakonu.

Iz ovoga se vidi, da su za zakonopisci načelo javnosti želeli da postave kao standard i pravilo u Srbiji koja je od 2000. krenula u demokratske promene, a da je tajnost podataka postavljena tako da predstavlja izuzetak, odnosno zahteva dokazivanje pretežnijeg interesa od prava javnosti da zna.

U savremenim demokratskim državama pravo javnosti da zna predstavlja jedan od temeljnih mehanizama kontrole vlasti i zaštite javnog interesa. Pristup informacijama od javnog

značaja podrazumeva da je transparentnost **pravilo**, a **ograničenja mogu biti uvedena samo izuzetno, strogo definisano i uz jasno opravdanje**. Nasuprot tome, zaštita podataka kao tajnih štiti legitimne državne interese, poput nacionalne bezbednosti, odbrane ili spoljne politike. Međutim, savremeni standardi zahtevaju da se ova dva interesa ne posmatraju kao suprotstavljena, već kao **uravnotežena**: tajnost je izuzetak koji mora biti precizno definisan, vremenski ograničen i podložan nadzoru, dok se svaka sumnja tumači u korist transparentnosti. Demokratske države insistiraju da se klasifikacija ne sme koristiti za prikrivanje nezakonitosti, zloupotreba ili neefikasnosti, jer je upravo otvorenost institucija ključna za očuvanje poverenja građana i funkcionalnost sistema vladavine prava.

### Trodelni test javnog interesa

Činjenica da je određeni podatak označen kao tajni ne znači da će on to nužno i ostati, ukoliko se utvrdi da je interes javnosti da zna pretežniji od interesa koji se štite tajnošću. U praksi je upravo primena testa javnog interesa jedini stvarni mehanizam kontrole nad neopravdano označenim tajnim podacima.

Kada organ javne vlasti odlučuje o zahtevu za pristup informacijama od javnog značaja, a tražena informacija je označena stepenom tajnosti, dužan je da sprovede trodelni test javnog interesa. Suština ovog testa je da se utvrdi da li u konkretnom slučaju postoji pretežniji javni interes za objavljivanje informacije u odnosu na interes koji se štiti ograničenjem pristupa.

Test se sastoji iz tri koraka:

1. **Provera osnova ograničenja**: da li se pristup uskraćuje radi zaštite nekog od zakonom predviđenih razloga (izuzeća iz članova 9, 13 i 14 Zakona o slobodnom pristupu informacijama od javnog značaja)?
2. **Procena ozbiljnosti štete**: da li bi omogućavanje pristupa konkretno i ozbiljno ugrozilo zaštićeni interes?
3. **Provera neophodnosti ograničenja u demokratskom društvu**: da li je uskraćivanje pristupa informacijama zaista nužno i srazmerno interesu koji se štiti?

U praksi se često dešava da organi javne vlasti test javnog interesa ne sprovedu, već se samo pozovu na činjenicu da je podatak označen kao tajni ili da „preteže drugi interes“. U takvim situacijama Poverenik u žalbenom postupku obično poništava rešenje organa, vraća predmet na ponovno odlučivanje uz nalog da se test sprovede, a povreda pretežnijeg interesa dokaže, a nakon izjašnjavanja prvostepenog organa može i sam izvršiti ocenu da li je interes javnosti pretežniji. Na taj način se omogućava pristup informacijama uprkos označavanju tajnosti.

Kako je već problematizovano u analizi, u Srbiji ne postoji funkcionalan nadzor nad određivanjem tajnosti podataka. Zbog toga test javnog interesa iz Zakona o slobodnom pristupu informacijama od javnog značaja trenutno predstavlja **jedini mehanizam kontrole nad neopravdano označenim tajnim informacijama**. Važno je naglasiti da je domet ovog mehanizma u smislu kontrole veoma skroman, jer se odnosi na pojedinačne slučajeve u kojima su se tražioci informacijama obratili žalbom Povereniku, kao i zbog drugih problema<sup>31</sup> u radu službe Poverenika koji utiču na efikasnost ovog žalbenog mehanizma.

Radi ilustracije odmeravanja pretežnijeg interesa u nastavku će biti predstavljena praksa Poverenika.

## Žalbe zbog tajnosti- pregled prakse Poverenika

Iz godišnjih izveštaja o radu Poverenika ne može se sa sigurnošću utvrditi koji broj podnetih žalbi i donetih rešenja se odnosi na tajnost podataka definisanu Zakonom o tajnosti podataka, jer su ovi slučajevi spojeni u godišnjoj statistici sa drugim vrstama tajnosti poput poslovne tajne koja se uređuje drugim zakonom. Zbog toga, za potrebe ovog istraživanja, Partneri Srbija uputili su Povereniku dva zahteva za pristup informacijama, tražeći kopije rešenja donetih tokom 2023. i 2024. godine u predmetima u kojima su organi javne vlasti odbili pristup informacijama pozivajući se na argument tajnosti u skladu sa Zakonom o tajnosti podataka.

Poverenik je dostavio kopije 29 rešenja donetih u 2024<sup>32</sup>, kao i 5 rešenja iz 2023. godine<sup>33</sup>. Ukupno, ovaj istraživački uzorak uključuje 34 rešenja Poverenika.

<sup>31</sup> Nedostatak kapaciteta usled masovnih zloupotreba prava (predstavljeno ranije u ovoj Analizi).

<sup>32</sup> U 2024, Poverenik je postupio po 49 predmeta, i doneo 29 rešenja. U nekim situacijama je Poverenik spojio više žalbi u jedan žalbeni postupak, u situacijama kada su se tražioci informacija žalili na isti organ vlasti, povodom istih ili sličnih vrsta informacija, otud razlika u broju predmeta i broju rešenja.

<sup>33</sup> Poverenik je u toku 2023. postupio po 6 predmeta u vezi sa tajnošću podataka, i doneo 5 rešenja, od čega je dva predmeta spojio u jedan postupak i doneo zajedničko rešenje.

## Ishod žalbenih postupaka

|                                                                               | 2023 | 2024 |
|-------------------------------------------------------------------------------|------|------|
| Poverenik vratio prvostepenom organu na ponovno odlučivanje                   | 1    | 9    |
| Poverenik odbio žalbu kao neosnovanu (zloupotreba prava tražioca informacija) | /    | 11   |
| Poverenik odbio žalbu kao neosnovanu ( drugi razlozi)                         | /    | 2    |
| Poverenik odbacio žalbu kao neurednu                                          | 1    | 1    |
| Poverenik odbacio žalbu kao nedopuštenu                                       | /    | 2    |
| Poverenik naložio dostavljanje informacija                                    | 2    | 4    |

U ukupno 10 slučajeva, Poverenik je poništio odluke prvostepenih organa i vratio predmete na ponovno odlučivanje, ukazujući da organi javne vlasti nisu obrazložili na koji način bi odavanje informacija izazvalo štetne posledice po zakonom zaštićene interese.

Ilustrativni primeri:

- ❖ **Dokumentacija o izvozu i uvozu naoružanja i vojne opreme**  
Ministarstvu unutrašnje i spoljne trgovine tražene su kopije zahteva za uvoz/izvoz naoružanja u periodu od 2018. do 1.8.2023. Poverenik je ocenio da organ nije dokazao postojanje konkretne štete i naložio je ponovno odlučivanje.
- ❖ **Nalaz i stručno mišljenje o eksploziji u fabrici „Sloboda“, Čačak**  
Uprkos pozivanju na tajnost, Poverenik je utvrdio da organ nije obrazložio kako bi objavljivanje izazvalo štetne posledice i vratio predmet na ponovno odlučivanje. Fabrika je donela novo rešenje o odbijanju, te je predmet još jednom vraćen na ponovno odlučivanje.
- ❖ **Predmet vanredne provere imovine funkcionera Nikole Kovačevića**  
Agencija za sprečavanje korupcije odbila je zahtev, pozivajući se na tajnost. Poverenik je utvrdio da nije sproveden test javnog interesa i da nije dokazano postojanje ozbiljnih posledica, te je predmet vraćen na ponovno odlučivanje.

U ukupno 6 rešenja, Poverenik je naložio organima javne vlasti da dostave tražene informacije, uprkos tome što su se prvostepeni organi pozivali na tajnost podataka.

*Ilustrativni primeri:*

**Kopije Pravilnika o sistematizaciji radnih mesta u MUP-u:** Relevantan primer je pre svega rešenje Poverenika 071-01-1571/2022-03, iz 2023, u kojem su dve žalbe izjavljene protiv MUP-a spojene u jedan postupak. Tražilac informacija je tražio kopije 11 Pravilnika o izmenama i dopunama Pravilnika o unutrašnjem uređenju i sistematizaciji radnih mesta u Ministarstvu unutrašnjih poslova (ukratko- sve izmene navedenog Pravilnika u periodu od 2019. do 2021). MUP je u rešenju odbio dostavljanje traženih informacija, pozivajući se na tajnost. Konkretno MUP je obrazložio da sve izmene pravilnika potpadaju pod oznaku tajnosti „INTERNO“ jer je Pravilnik kao takav odlukom iz 2018. godine označen oznakom „INTERNO“. MUP je u obrazloženju naveo i da bi se dostavljanjem traženih informacija mogao utvrditi način funkcionisanja MUP-a, „posebno u situacijama kada može doći do ugrožavanja bezbednosti građana Srbije“. Takođe je navedeno da odavanje podataka o operativnoj funkcionalnosti „može za posledicu imati ometanje sprovođenja policijskih mera i aktivnosti u borbi protiv svih vidova kriminala ...“.

Poverenik je žalbu dostavio MUP- u na izjašnjenje koji je u odgovoru ostao pri svojim navodima. Poverenik je nakon toga doneo rešenje u kojem je poništio prvostepenu odluku MUP-a i naložio ponovno postupanje MUP-u, te da obrazloži razloge za odbijanje zahteva, da dokaže koje štetne posledice bi nastale objavljivanjem informacija, kao i da proceni da li je moguće delimično dostavljanje traženih informacija (ukoliko ne svih).

Na ovo rešenje Poverenika, tražilac informacija je podneo tužbu Upravnom sudu, tvrdeći da je Poverenik propustio da (u skladu sa ZoSPIJZ) donese odluku u upravnoj stvari, već je predmet vratio na ponovno odlučivanje instituciji koja je već jednom donela odluku u istom predmetu. Upravni sud je doneo presudu kojom je poništio prvo rešenje Poverenika, i naložio mu da donese odluku u upravnoj stvari. U obrazloženju odluke Upravnog suda, navodi se da je Poverenik rešenjem povredio zakon na štetu tražioca informacija. U obrazloženju Upravni sud navodi da Poverenik, kada utvrdi, da je žalba osnovana treba prvostepenom organu da naloži dostavljanje traženih informacija. U presudi Upravnog suda se navodi i da je prvostepeni organ (MUP), imao priliku već dva puta da se izjasni (prvi put kad je doneo rešenje o odbijanju, drugi put kroz odgovor na žalbu), i da je oba puta ostao pri istim razlozima za odbijanje dostavljanja traženih informacija. Upravni sud je ocenio da je Poverenik trebalo da donese odluku u ovoj upravnoj stvari (u skladu ZoSPIJZ), a ne da predmet vrati na ponovno odlučivanje MUP-u (primenjujući supsidijarne pravne norme- Zakon o opštem upravnom postupku). Poverenik je postupio u skladu sa sudskom odlukom Upravnog suda, i u ponovljenom žalbenom postupku sproveo ocenu navoda žalioca i prvostepenog organa, i doneo rešenje u kojem je naloženo MUP-u da dostavi sve tražene informacije. Odluka je obrazložena ovako: da je MUP samo nabrojao razne hipotetičke posledice do kojih bi moglo doći, ne dokazujući ispunjenost uslova za uskraćivanje traženih informacijama iz člana 9. ZoSPIJZ. Poverenik je ukazao i da su mnoge informacije iz Pravilnika o sistematizaciji javno objavljene u Informatoru o radu Ministarstva, pravilnicima



o radu MUP, kao i u Akcionom planu za pregovaračko poglavlje 24, u kojem se navodi koliko zaposlenih imaju različite jedinice MUP, a koji je javno dostupan na sajtu Ministarstva za evropske integracije. Zbog svega navedenog, Poverenik je rešenju naložio MUP dostavljanje traženih informacija. Važno je napomenuti i da je MUP u poslednjem Nacrtu Zakona o unutrašnjim poslovima predvideo da Pravilnik o sistematizaciji radnih mesta bude označen kao tajni dokument.

**Statistički podaci o primeni posebnih dokaznih radnji:** MUP se pozvao na tajnost podataka, ali je Poverenik doneo rešenje kojim nalaže dostavljanje podataka. MUP je u obrazloženju odluke da ne dostavi informacije, između ostalog naveo da podaci predstavljaju tajne podatke u smislu Zakona o tajnosti podataka, kao i u skladu sa Zakonom o o krivičnom postupku, da bi dostavljanje traženih podataka predstavljalo nanošenje štete po interese države, da bi dostavljanje podataka o broju lica i broju primenjenih posebnih dokaznih radnji obesmisllilo primenu tih dokaznih radnji, i otkrilo kapacitete MUP-a u ovoj oblasti. Poverenik se u obrazloženju svoje odluke, pozvao i na prethodne odluke donete u vezi sa istim vrstama informacija traženim od BIA, kao i odluku Evropskog suda za ljudska prava u predstavi Inicijative mladih za ljudska prava (o kojoj će biti više reči kasnije). Poverenik je obrazložio da je sprovođenje posebnih dokaznih radnji dozvoljeno samo na određeno vreme i uz odluku suda, a u cilju zaštite Ustavnog prava iz člana 41 (nepovredivost pisma i komunikacije), da je kontrola nad primenom posebnih postupaka i dostupnost informacija podjednako važan i legitiman interes, kao da se objavljivanje podataka o broju preduzetih radnji i broju lica ne povređuje ni privatnost, niti postupci i načini rada organa koji takve mere preduzima.

**Kovački centar d.o.o. (troškovi reprezentacije):** Udruženje građana je tražilo kopije analitičkih kartica i računa za troškove reprezentacije za period 2014. do 2021. Organ je odbio zahtev pozivajući se na tajnost, navodeći da je reč o pravnom licu od posebnog značaja za odbranu Srbije. Poverenik je objedinio žalbe i naložio dostavljanje podataka. Iz obrazloženja rešenja Poverenika: „da bi organ uskratio pristup traženim informacijama dužan je da dokaže da je opravdano da to učini radi zaštite pretežnijeg interesa“. Poverenik je našao da prvostepeni organ nije pružio dokaz o opravdanosti isključenja pristupa traženim informacijama, odnosno nije dokazao da postoji uzročno- posledična veza između potencijalnog objavljivanja podataka i narušavanja javnog interesa. Ovo posebno zbog toga što su zahtevom tražene informacije koje se odnose na troškove ugostiteljskih usluga, koje su plaćene sredstvima organa javne vlasti, odnosno korišćenjem javnih resursa.

**Kovački centar d.o.o. (jubilarne nagrade):** Isto udruženje građana podnelo je i sedam zahteva za pristup informacijama o isplaćenim jubilarnim nagradama (sa imenima zaposlenih). Organ je odbio zahteve pozivajući se na tajnost i zaštitu podataka o ličnosti. Poverenik je spojio postupke i naložio dostavljanje informacija uz zaštitu ličnih podataka. Obrazloženje rešenja Poverenika bilo je veoma slično prethodnom.

Poverenik je u 11 slučajeva odbio žalbe kao neosnovane zbog zloupotrebe prava tražioca informacija. Ovo je dugogodišnji problem koji negativno utiče na kapacitete Poverenika i organa javne vlasti kojima se ovakvi zahtevi, odnosno žalbe upućuju, a u konačnici ima negativan efekat na savesne tražioca informacija, jer institucija Poverenika nema dovoljno kapaciteta da postupa po njihovim žalbama. Problem je nastao kao posledica brisanja instituta zloupotrebe prava iz ZoSPIJZ i promene dugogodišnjeg stava Upravnog suda u pogledu naknade troškova zastupanja u postupku po žalbi 2021. godine.<sup>34</sup> O ovom problemu se do sada mnogo pisalo, te stoga ovde neće biti detaljno predstavljen mehanizam zloupotrebe i posledice. Važno je naglasiti da je zbog ovog problema, ali i drugih problema koji postoje u primeni Zakona o slobodnom pristupu informacijama od javnog značaja neophodna hitna izmena ovog Zakona.

U dva slučaja iz uzorka, Poverenik je odbio žalbu kao neosnovanu. Jedna žalba je odbijena kao neosnovana jer je advokat lica iz sudskog postupka tražio podatke vezane za taj postupak. U drugom slučaju je Poverenik procenio da drugi interes preteže nad interesom prava javnosti da zna.

U jednom slučaju Poverenik je odbacio žalbu kao neurednu, jer tražilac informacija u ostavljenom roku nije dopunio žalbu potrebnim informacijama. Dve žalbe su odbačene kao nedopuštene, jer su žalbe bile podnete protiv Narodne banke Srbije, koja se nalazi na listi organa protiv kojih je moguće jedino podneti tužbu Upravnom sudu zbog kršenja prava iz ZoSPIJZ.

Pregled najnovijih rešenja pokazuje da je dominantan problem nedostatak obrazloženja prvostepenih organa o tome **kako bi objavljivanje informacija konkretno ugrozilo zakonom zaštićene interese**, što je zakonski uslov za opravdano pozivanje na tajnost.

Zbog toga se najveći broj predmeta vraća na ponovno odlučivanje, dok se u određenom broju slučajeva Poverenik upušta u meritorno odlučivanje, primenjuje test javnog interesa i nalaže dostavljanje informacija.

S obzirom na to da je tema ove analize posebno usmerena na institut tajnosti i sektor bezbednosti, u nastavku su izdvojeni i relevantni primeri iz ranije prakse Poverenika, koji su poslužili za formiranje standarda u primeni testa javnog interesa i kontrole opravdanosti pozivanja na tajnost.

<sup>34</sup> Za više pogledati godišnje izveštaje o radu Poverenika, primer: Godišnji izveštaj za 2024, od strane 27:

[https://www.poverenik.rs/images/stories/dokumentacija-nova/izvestajiPoverenika/2024/LATGodi%C5%A1nji%20izve%C5%A1taj%2024\\_002.pdf](https://www.poverenik.rs/images/stories/dokumentacija-nova/izvestajiPoverenika/2024/LATGodi%C5%A1nji%20izve%C5%A1taj%2024_002.pdf)

## Inicijativa mladih za ljudska prava protiv BIA (statistički podaci o merama tajnog nadzora, 2013.)<sup>35</sup>

Udruženje **Inicijativa mladih za ljudska prava** podnelo je zahtev Bezbednosno-informativnoj agenciji (BIA) za pristup informacijama o primeni posebnih mera kojima se odstupa od načela nepovredivosti tajnosti pisama i drugih sredstava opštenja u 2013. godini. Konkretno, tražene su:

1. **kopije dokumenata** iz kojih se može videti broj fizičkih i pravnih lica prema kojima su mere primenjene, i
2. **broj predloga** koje je direktor BIA uputio predsedniku Vrhovnog kasacionog suda radi odobravanja tih mera (posebno za fizička i posebno za pravna lica).

BIA je odbila zahtev, pozivajući se na član 9. tačka 5. Zakona o slobodnom pristupu informacijama i na odluku o klasifikaciji kojom su podaci označeni kao „**strogo poverljivo**“. BIA je tvrdila da bi objavljivanje čak i zbirnih statističkih podataka moglo da nanese štetu bezbednosnim interesima države, jer bi „analitički sposobna lica“ mogla da iz tih podataka zaključe koji su prioriteti i operativni kapaciteti Agencije.

Međutim, Poverenik je po žalbi poništio rešenje BIA i naložio dostavljanje traženih informacija (uz zaštitu ličnih podataka). Poverenik je ocenio da BIA **nije ispunila zakonsku obavezu dokazivanja** da bi dostupnost traženih podataka stvarno izazvala **ozbiljnu štetu** po pretežni interes koji se štiti tajnošću. Istakao je da se pravo na pristup može uskratiti samo ako su kumulativno ispunjena dva uslova:

1. **Formalni uslov**: da je informacija zakonito označena kao tajna.
2. **Materijalni uslov**: da bi objavljivanje **konkretno i stvarno** izazvalo teške pravne ili druge posledice po zaštićeni interes.

U ovom slučaju BIA je ispunila formalni uslov (postojanje odluke o klasifikaciji), ali **nije pružila nikakav dokaz** o tome da bi objavljivanje zbirnih statističkih podataka realno moglo ugroziti bezbednost države. BIA se oslanjala na pretpostavke („moguće je da neko izvuče zaključke“), ali nije pokazala **direktnu uzročno-posledičnu vezu** između objavljivanja podataka i tvrdene štete. Poverenik je naglasio da su traženi podaci **statističke prirode**, da ne otkrivaju pojedinačne postupke niti operativne metode BIA, te da organ nije dokazao nužnost ograničenja prava javnosti prema standardu „neophodno u demokratskom društvu“.

Kako udruženje nije dobilo informacije ni nakon žalbe Povereniku, ovaj slučaj je dospelo i do Evropskog suda za ljudska prava, koji je potvrdio odluku Poverenika. O ovoj presudi će biti

<sup>35</sup> Slobodan pristup informacijama: stavovi i mišljenja Poverenika, publikacija 3, str: 88-92:

<https://www.poverenik.rs/images/stories/dokumentacija-nova/prirucnik/3.publikacija/publikacijaiiii.pdf>

više napisano u odeljku analize „Praksa Evropskog suda za ljudska prava“. Ovde je važno naglasiti da značaj ove presude posebno u smislu da se njome naglašava da sektor bezbednosti ne može biti izuzet od prava na pristup informacijama i slobodu izražavanja. I da se bez obzira na potrebe službi bezbednosti da ograniče javnost svog rada, konkretno ograničenje slobode izražavanja mora biti u skladu sa principima ljudskih prava.

Mana ovog procesa je njegova dugotrajnost. Od podnošenja zahteva (2005) do konačne odluke Evropskog suda za ljudska prava donete 2013. prošlo skoro osam godina.

### **Dokument o obustavi krivičnog postupka protiv gradonačelnika Beograda<sup>36</sup>**

U ovom slučaju od tužilaštva je tražen dokument o obustavi krivičnog postupka protiv gradonačelnika Beograda. Tužilaštvo je odbilo zahtev pozivajući se na član 9. tačka 5. Zakona o slobodnom pristupu informacijama od javnog značaja i na činjenicu da je predmet vođen pod oznakom „strogo poverljivo“.

Istaknuto je da pravilnik Republičkog javnog tužilaštva zabranjuje dostavljanje takvih informacija i da bi objavljivanje dokumenta moglo naneti „tešku štetu“ interesima Republike Srbije, posebno interesima krivičnog gonjenja i funkcionisanja pravosuđa.

Zahtev je odbijen bez sprovođenja testa javnog interesa i bez razmatranja mogućnosti delimičnog dostavljanja informacije uz zaštitu poverljivih podataka.

Poverenik je uvažio žalbu, poništio rešenje tužilaštva i naložio da se tražene informacije dostave uz zaštitu podataka o ličnosti (osim imena gradonačelnika). U utvrđivanju činjenica, Poverenik je ocenio da tužilaštvo nije dokazalo nijedan od zakonskih uslova za uskraćivanje pristupa po članu 9. tačka 5. Zakona o slobodnom pristupu informacijama.

Najpre, organ nije dokazao da je dokument o obustavi postupka zaista klasifikovan kao „STROGO POVERLJIVO“ u skladu sa Zakonom o tajnosti podataka i relevantnim uredbama. Drugo, nije obrazloženo koje bi „teške pravne ili druge posledice“ nastale omogućavanjem pristupa informaciji, niti je predstavljen bilo kakav dokaz da bi objavljivanje dokumenta ugrozilo zakonom zaštićene interese.

Iz obrazloženje rešenja: „*Argumenti za uskraćivanje pristupa traženim informacijama se ne mogu zasnivati samo na pretpostavci o mogućoj povredi zakonom zaštićenih interesa. (...) prava iz ovog zakona mogu izuzetno podvrći ograničenjima propisanim zakonom samo ako je to neophodno u demokratskom društvu radi zaštite od ozbiljne povrede pretežnijeg interesa zasnovanog na ustavu ili zakonu, za šta u konkretnom slučaju po oceni Poverenika ne postoje razlozi, posebno imajući u vidu samu prirodu traženih informacija, odnosno da se*

<sup>36</sup> Slobodan pristup informacijama: stavovi i mišljenja Poverenika, publikacija 7, Str:72-75:  
<https://www.poverenik.rs/images/stories/dokumentacija-nova/Publikacije/7PoverenikPublikacija.pdf>

*radi o dokumentu koji sadrži razloge zbog kojih je tužilaštvo našlo da ne postoje osnovi sumnje da je prijavljeno lice izvršilo krivično delo koje mu se stavlja na teret, te se nastupanje posledica iz člana 9. tačka 5. Zakona, u konkretnom slučaju, po prirodi stvari realno ne bi moglo očekivati.*<sup>37</sup> Protiv ovog rešenja Republički javni tužilac je podneo tužbu Upravnom sudu traživši da se rešenje Poverenika poništi kao nezakonito, jer tražilac informacija kako je isticao prvostepeni organ, nije dovoljno precizirao svoj zahtev. Upravni sud je poništio prvo rešenje Poverenika, i vratio slučaj Povereniku na ponovno odlučivanje. U postupku ponovnog odlučivanja Poverenik je naložio prvostepenom organu da ponovo sprovede postupak odlučivanja po zahtevu, pri čemu će prvo uputiti zahtev tražiocu informacija da zahtev uredi radi preciznosti, a zatim i da postupi po uređenom zahtevu.

Polazeći od pretpostavke da organi javne vlasti ne promišljaju dovoljno prilikom sprovođenja testa javnog interesa u slučaju kada je suprotstavljeni interes tajnost podataka, a u cilju olakšavanja tog postupka ovde će biti navedena dodatna pitanja za sprovođenja testa javnog interesa koja mogu da budu od pomoći prilikom donošenja odluka, a koja je izradio prof. dr Goran D. Matić, u okviru zbornika radova Primena Zakona o tajnosti podataka, 10 najznačajnijih prepreka<sup>38</sup>:

- ❖ Da li je reč o tajnom podatku ili informaciji kojom raspolaže organ javne vlasti?
- ❖ Da li se utvrđivanjem tajnosti podataka prikriva postojanje teških povreda osnovnih prava čoveka?
- ❖ Da li se utvrđivanjem tajnosti podataka prikriva postojanje ugrožavanja ustavnog uređenja i bezbednosti Srbije?
- ❖ Da li se utvrđivanjem tajnosti podataka prikriva učinjeno krivično delo za koje se može izreći kazna zatvora u trajanju od 5 godina?
- ❖ Da li se utvrđivanjem tajnosti podataka prikriva postojanje krivičnog dela?
- ❖ Da li se utvrđivanjem tajnosti podataka prikriva prekoračenje ovlašćenja?
- ❖ Da li se utvrđivanjem tajnosti podataka prikriva zloupotreba službenog položaja?
- ❖ Da li se utvrđivanjem tajnosti podataka prikriva drugi nezakonit akt?
- ❖ Da li je potreba zaštite interesa R. Srbije pretežnija od interesa za slobodan pristup informacijama od javnog značaja?
- ❖ Da li je interes nabrojan u zakonu (čl. 9, 13. i 14. Zakona o slobodnom pristupu informacijama od javnog značaja) suprotstavljen interesu tražioca da zna? Da li bi pristupom ovoj informaciji suprotan interes bio ozbiljno povređen (pitanje procene posledica ili balansa prava)?

<sup>37</sup> Slobodan pristup informacijama: stavovi i mišljenja Poverenika, publikacija 7, Str:72-75:

<https://www.poverenik.rs/images/stories/dokumentacija-nova/Publikacije/7PoverenikPublikacija.pdf>

<sup>38</sup>prof. dr Goran D. Matić, Primena Zakona o tajnosti podataka, 10 najznačajnijih prepreka (zbornik radova), od str. 23

<http://repozitorijum.pravnifakultet.edu.rs/314/>

- ❖ Da li potreba zaštite suprotnog interesa preteže nad potrebom zaštite interesa tražioca da zna, prosuđujući neophodnost uskraćivanja pristupa po merilima demokratskog društva?

# Sankcionisanje povreda Zakona o tajnosti podataka

## Praksa prekršajnih sudova

Za potrebe ovog istraživanja formiran je reprezentativan uzorak koji obuhvata 60% svih prekršajnih sudova u Republici Srbiji. Tim sudovima upućen je identičan zahtev za dostavljanje kopija odluka donetih tokom 2023. i 2024. godine u postupcima vođenim zbog prekršaja iz Zakona o tajnosti podataka (čl. 99. i 100), kao i informacija o tome da li se takvi postupci trenutno vode.

Uzorak je koncipiran tako da obuhvati prekršajne sudove iz većih i manjih gradova i opština, uz ravnomernu geografsku raspodelu. Ukupno 27 prekršajnih sudova primilo je zahtev.

Svi sudovi su odgovorili u zakonskom roku. Iako je zbog izostanka institucionalnog nadzora bilo očekivano da praksa bude ograničena, neočekivani nalaz predstavlja činjenica da su svi sudovi izvestili da u navedenom periodu nije vođen niti okončan nijedan prekršajni postupak po Zakonu o tajnosti podataka, kao i da se takvi postupci trenutno ne vode.

## Krivični postupci

Partneri Srbija su i ranijih godina slali zahteve za pristup informacijama od javnog značaja kako bi utvrdili kakva je praksa sudova u pogledu krivične odgovornosti u oblasti tajnosti podataka. Praksa na godišnjem nivou je obično uključivala svega nekoliko okončanih sudskih postupaka.

Za potrebe ovog istraživanja poslali smo zahteve za pristup informacijama od javnog značaja svim višim sudovima u Srbiji (ukupno 20), sa pitanjima koliko se postupaka trenutno vodi u vezi sa krivičnim delima povezanim sa tajnošću (Zakon o tajnosti podataka čl.98 i Krivični zakonik članovi 316 i 369), kao i da dostave kopije sudskih odluka donete u 2024. u vezi sa ovim krivičnim delima.

Svi viši sudovi su odgovorili.

Dva suda su odgovorila da imaju postupke koji su u toku u vezi sa ovim krivičnim delima. Od toga jedan sud sedam postupaka, a drugi sud jedan postupak. 18 trenutno nema postupke.

13 sudova je odgovorilo da u toku 2024. nisu donosili sudske odluke po ovim krivičnim delima. Od preostalih sedam:

**Viši sud u Beogradu** dostavio je dve odluke: jednu kojom je zahtev odbijen zbog zastarelosti, i drugu kojom je izvršeno spajanje predmeta. Dakle, u oba slučaja radilo se o procesnim odlukama, bez vođenja klasičnog meritorno-sudskog postupka.

**Viši sud u Valjevu** doneo je jednu oslobađajuću presudu. Slučaj se odnosio na neovlašćeno činjenje dostupnim policijskih dokumenta koja predstavljaju tajne podatke sa oznakom tajnosti „poverljivo“ prema Zakonu o tajnosti podataka.

**Viši sud u Vranju** doneo je jedno rešenje kojim je odbio sporazum o priznanju krivičnog dela, ocenjujući da predložena kazna nije adekvatna, kao i da nisu posebno navedene niti obrazložene olakšavajuće okolnosti koje bi opravdale izricanje blaže sankcije. Istraživački tim je imao uvid isključivo u ovo procesno rešenje, u kojem se ne navode činjenice i okolnosti iz samog sporazuma o priznanju, zbog čega ovaj slučaj nije bilo moguće detaljnije predstaviti.

**Viši sud u Jagodini** doneo je jednu osuđujuću presudu. Slučaj se odnosio na nezakonito pribavljanje podataka označenih oznakom tajnosti „INTERNO“, koji se odnose na video snimke kretanja i oznaka vozila Vojske Srbije, koje je osuđeno lice nabavilo uz lažno predstavljanje. Viši sud je našao da je osuđeni učinio krivično delo iz člana 98. Zakona o tajnosti podataka, kao i krivična dela: lažno predstavljanje, falsifikovanje isprave, kao i krivično delo nedozvoljena proizvodnja, držanje, nošenje i promet oružja i eksplozivnih materija, zbog čega mu je izrečena zatvorska kazna u ukupnom trajanju od 2 godine, novčana kazna od 100,000,00 RSD kao i mera oduzimanja predmeta.

**Viši sud u Leskovcu** doneo je jednu osuđujuću presudu, zbog toga što je lice neovlašćeno pribavljalo podatke označene stepenom tajnosti „POVERLJIVO“ iz Jedinog informacionog sistema MUP-a koristeći svoju šifru i šifru drugog policijskog službenika. Lice je osuđeno na kaznu od 3 meseca zatvora, a presuda je potvrđena od strane Apelacionog suda u Nišu.

**Viši sud u Novom Pazaru** je doneo jednu osuđujuću presudu zbog toga što je policijska službenica učinila dostupnim neovlašćenom licu video snimke naplatne rampe koje je pribavila u sklopu istrage. Ovi podaci su bili označeni oznakama tajnosti „INTERNO“ i „POVERLJIVO“. Izrečena je uslovna osuda, odnosno kazna zatvora od 3 meseca ukoliko u roku od godinu dana okrivljena učini novo krivično delo.

**Viši sud u Novom Sadu** doneo je jednu presudu kojom se prihvata sporazum o priznanju krivičnog dela. Radi se o slučaju neovlašćenog pribavljanja podataka označenih stepenom „POVERLJIVO“ iz Jedinog informacionog sistema MUP-a, čime je izvršeno krivično delo iz člana 98. Zakona o tajnosti podataka. Okrivljena je sklopila sporazum o priznanju i



osuđena je uslovno, kao i u prethodnom primeru, odnosno kaznom zatvora od 3 meseca ukoliko u roku od godinu dana učini novo krivično delo.

Na osnovu prikupljenih podataka i odgovora viših sudova može se izvesti nekoliko jasnih zaključaka o primeni krivičnih odredaba Zakona o tajnosti podataka.

Prvo, **sudska praksa je izuzetno oskudna**. Većina sudova je izvestila da tokom 2024. godine nije donela nijednu odluku po krivičnim delima vezanim za tajnost podataka, dok samo dva suda trenutno vode postupke. **Ovakvo stanje snažno ukazuje na širi sistemski problem, nedostatak nadzora i kontrole, zbog čega slučajevi retko dospeju pred sud.**

Drugo, **u malom broju postupaka koji su sprovedeni, uočljivo je da se najveći broj slučajeva odnosi na neovlašćeno pribavljanje ili činjenje dostupnim tajnih podataka koji se nalaze u Jedinostvenom informacionom sistemu MUP-a**. Najčešće je reč o policijskim službenicima koji koriste sopstvene ili tuđe pristupne šifre kako bi pristupili poverljivim informacijama, **što ukazuje na slabosti u internim kontrolama i bezbednosnim procedurama u sektoru bezbednosti.**

Treće, **izrečene kazne su pretežno blage**, čak i u slučajevima koji se odnose na namerno odavanje podataka označenih stepenom „POVERLJIVO“ ili na pribavljanje informacija koje mogu imati bezbednosnu dimenziju. U nekoliko presuda izrečene su uslovne osude ili kratke zatvorske kazne od tri meseca, dok je samo u jednom predmetu (Viši sud u Jagodini) izrečena teža sankcija koja uključuje višegodišnji zatvor i novčanu kaznu.

**Ovakvi nalazi ukazuju da krivične odredbe Zakona o tajnosti podataka u praksi imaju ograničen domet, da se primenjuju retko i uz minimalne sankcije, što dodatno slabi preventivni efekat zakona i ostavlja prostor za zloupotrebe u radu državnih organa, naročito onih u sektoru bezbednosti.**

## Praksa Evropskog suda za ljudska prava

Praksa Evropskog suda za ljudska prava (ESLJP) treba da predstavlja orijentir državama u tumačenju i primeni ograničenja pristupa informacijama. Ona jasno pokazuje kako treba uspostaviti ravnotežu između zaštite tajnih podataka i prava javnosti da zna, naročito kada se radi o pitanjima od visokog javnog interesa ili potencijalnim povredama ljudskih prava. Organi vlasti bi trebalo da se rukovode ovim standardima kako bi njihovo postupanje bilo u skladu sa ljudskim pravima i obavezama koje proizlaze iz Evropske konvencije o ljudskim pravima.

ESLJP balansira tajnost i slobodu informisanja tako što priznaje da države imaju pravo da štite nacionalnu bezbednost, ali ne i do mere da potpuno sakriju informacije, naročito kada se one odnose na ozbiljna kršenja ljudskih prava ili postupanje državnih organa. Član 10. Evropske konvencije o ljudskim pravima ne garantuje neograničeno pravo na pristup informacijama, ali takvo pravo može nastati kada je pristup neophodan za ostvarivanje slobode prikupljanja i širenja informacija, posebno u vezi sa radom organa javne vlasti ili objavljivanjem zvaničnih dokumenata.

**Sud zahteva da svako ograničenje pristupa informacijama mora biti propisano zakonom, neophodno u demokratskom društvu i proporcionalno cilju koji se želi postići, kao što je zaštita nacionalne bezbednosti.**

### Balansiranje tajnosti i slobode informisanja

ESLJP ističe da potpuno uskraćivanje informacija u pravilu nije opravdano, čak ni radi nacionalne bezbednosti. Neophodna je mogućnost javnog nadzora nad radom vlasti, posebno u slučajevima gde postoji sumnja na kršenje ljudskih prava. Iako član 10. ne daje automatsko pravo na pristup svim informacijama, pravo pristupa može nastati kada su informacije ključne za ostvarenje slobode prikupljanja i širenja informacija. ESLJP u svojim odlukama takođe ističe da, svako ograničenje pristupa informacijama mora biti zakonito, neophodno i srazmerno legitimnom cilju, poput zaštite nacionalne bezbednosti. ESLJP priznaje državama određenu slobodu u proceni, ali ta procena mora biti uravnotežena sa značajem slobode informisanja.

U ovoj analizi je već pomenuta presuda<sup>39</sup> **Incijativa za ljudska prava (YIHR) protiv Srbije** (Application no. 48135/06)

Presuda Evropskog suda od višestrukog je značaja jer je bila i prva takva doneta u vezi sa kršenjem člana 10. Konvencije o zaštiti ljudskih prava protiv Srbije. Ona učvršćuje ranije

<sup>39</sup> <https://hudoc.echr.coe.int/eng#%7B%22appno%22:%5B%2248135/06%22%5D%22%7D>

utvrđen stav ESLJP da je pravo na pristup informacijama zaštićeno Evropskom konvencijom kao sastavni deo prava na slobodu izražavanja. **Presuda takođe ne pravi izuzetak u pogledu ostvarivanja tog prava kada je reč o nadležnosti organa vlasti, uključujući i sektor bezbednosti.** Ukazuje se i na to da, uprkos potrebama određenih službi da ograniče javnost svog rada, svako ograničenje slobode izražavanja mora biti u skladu sa principima ljudskih prava. U predmetnom slučaju, YIHR je podnela predstavku ESLJP-u, tvrdeći da im je Bezbednosno informativna agencija (BIA) uskraćivanjem pristupa informacijama o broju zahteva za prisluškivanje, onemogućila da ispune svoju ulogu kontrolora javnih institucija ('watchdog'). Sud je utvrdio da odbijanje BIA da postupi po nalogu Poverenika i dostavi tražene informacije predstavlja povredu člana 10 Evropske konvencije. Iako pravo na pristup informacijama može biti ograničeno, ESLJP nije našao nijedan osnov za ograničenje u ovom slučaju. Tvrdnja BIA da ne poseduje tražene podatke nije bila uverljiva, s obzirom na to da je prvobitno odbila pristup podacima pozivajući se na tajnost.

#### **Slučaj: GIRGINOVA protiv Bugarske (*Application no. 4326/18*)<sup>40</sup>**

Evropski sud za ljudska prava **presudio je 4. marta 2025. godine protiv Bugarske zbog povrede prava na slobodu izražavanja** (član 10) i prava na delotvorni pravni lek (član 13). Novinarka je tražila pristup obrazloženju oslobađajuće presude bivšem ministru unutrašnjih poslova u predmetu koji se odnosio na navodno nezakonito tajno nadziranje. Iako bugarski zakon uobičajeno zahteva objavljivanje sudskih obrazloženja, domaći sudovi su odbili njen zahtev pozivajući se na domaći zakon o zaštiti tajnih podataka. Novinarka je iskoristila sva dostupna pravna sredstva i potom se obratila ESLJP-u.

Evropski sud za ljudska prava je, razmatrajući dopuštenost predstavke, podsetio da član 10 Konvencije ne sadrži izričito pravo na pristup informacijama, ali da ovo pravo postoji kada je pristup informacijama **neophodan za ostvarivanje prava na slobodu izražavanja** (predmet *Magyar Helsinki Bizottság protiv Mađarske*<sup>41</sup>). Sud je zatim primenio četiri kriterijuma iz te presude na konkretan slučaj:

1. **Svrha zahteva za informacijama:** Postojao je legitiman novinarski interes, pristup informacijama bio je neophodan za pripremu izveštavanja o radu pravosuđa. Sud je istakao da novinari imaju dužnost da nadziru pravosudni sistem u ime javnosti.

<sup>40</sup> [https://hudoc.echr.coe.int/eng#{%22tabview%22:\[%22document%22\].%22itemid%22:\[%22001-242053%22\]}](https://hudoc.echr.coe.int/eng#{%22tabview%22:[%22document%22].%22itemid%22:[%22001-242053%22]})

<sup>41</sup> [https://hudoc.echr.coe.int/fre#{%22itemid%22:\[%22001-167828%22\]}](https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-167828%22]})

2. **Priroda traženih informacija:** Postojao je veoma snažan javni interes da se zna zbog čega je bivši ministar oslobođen optužbi povezanih sa nezakonitim tajnim nadzorom, kao i kako su tužilaštvo i sudovi postupali u tom predmetu.
3. **Uloga podnosioca zahteva:** Podnosilac je bio novinar, a mediji imaju ključnu ulogu u obezbeđivanju dostupnosti informacija o krivičnim postupcima javnosti.

U oceni povrede člana 10, Sud je prihvatio da je mešanje u pravo na slobodu izražavanja bilo zasnovano na zakonu jer se država pozivala na zaštitu nacionalne bezbednosti. Međutim, ključno pitanje bilo je da li je ovo ograničenje bilo **neophodno u demokratskom društvu**.

Sud je naglasio da postoji snažan javni interes za transparentnošću rada pravosuđa, da objavljivanje obrazloženih presuda jača poverenje javnosti u sudove i doprinosi pravičnom suđenju, kao i da obrazložene presude predstavljaju zaštitu od zloupotreba u pravosuđu.

U ovom slučaju, javni interes je bio posebno izražen jer se radilo o oslobađanju visokog državnog funkcionera za ozbiljne optužbe, u kontekstu šire zabrinutosti zbog zloupotrebe tajnog nadzora u zemlji. Sud je zaključio da potpuno uskraćivanje pristupa obrazloženju presude, nije bilo opravdano, čak ni pod izgovorom zaštite nacionalne bezbednosti. Postojale su manje restriktivne mere, poput delimičnog označavanja tajnosti ili objavljivanja redigovane ili anonimizovane verzije presude.

#### **Slučaj: GÎRLEANU protiv RUMUNIJE (*Application no. 50376/09*)<sup>42</sup>**

Slučaj se odnosio na novinara koji je istraživao rad oružanih snaga i policije. Protiv njega je pokrenut krivični postupak zbog navodnog prikupljanja i deljenja tajnih informacija u vezi sa vojnim operacijama rumunske vojske u Avganistanu.

Novinar je došao u posed kopije tajnih dokumenata koje je dobio od kolege, nakon čega je pokušao da proveriti njihovu autentičnost kod predstavnika vojske i obaveštajnih službi, a zatim ih je podelio sa nekoliko osoba za koje je smatrao da imaju stručno znanje o temi. U to vreme je u medijima objavljena informacija da je došlo do curenja podataka o vojnoj operaciji, ali dokumenta nisu javno objavljena. Protiv novinara je pokrenuta istraga, kuća mu je pretresena, kompjuter zaplenjen, telefoni prisluškivani, a sam novinar pritvoren, mada je ubrzo pušten. Kasnije je kažnjen novčanom kaznom od oko 240 evra, uz obrazloženje da je prekršio propise o nacionalnoj bezbednosti, iako je sa dokumenata u međuvremenu skinuta oznaka tajnosti. **Novinar je u predstavci ESLJP tvrdio da su sve njegove radnje bile deo legitimne novinarske istrage.**

<sup>42</sup> [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-184064%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-184064%22]})

ESLJP je utvrdio povredu člana 10 Evropske konvencije i naveo nekoliko ključnih razloga:

### **1. Novinar je delovao u okviru legitimne novinarske istrage**

Sud je naglasio da je novinar postupao kao istraživački novinar, da on nije nezakonito pribavio dokumenta, niti ih je objavio. Naglašeno je da je novinar prvo pokušao da potvrdi autentičnost dobijenih dokumenata kod nadležnih institucija. Zbog ovoga je ESLJP stao na stanovište da je ovim postupcima novinar pokazao profesionalizam.

### **2. Država nije dokazala da je postupanje novinara moglo da ozbiljno ugrozi nacionalnu bezbednost**

U obrazloženju, ESLJP je naglasio da su dokumenti u međuvremenu deklasifikovani, a sami organi su priznali da njihovo objavljivanje više ne bi moglo da šteti vojnim operacijama. Sud je zaključio da vlasti nisu pokazale da je ponašanje novinara moglo da nanese „značajnu štetu“ nacionalnoj bezbednosti.

### **3. Nacionalni sudovi nisu uradili potrebnu procenu javnog interesa**

ESLJP je posebno kritikovao da domaći sudovi nisu razmotrili da li je reč o pitanjima od značaja za javnost (curenje vojnih informacija, odgovornost institucija), kao i zbog toga što nisu uradili balansiranje između zaštite tajnosti i prava javnosti da zna. Takođe, ESLJP je smatrao da su domaći sudovi trebali da uzmu u obzir ulogu novinara i njegove motive (watch dog role).

Sud je naglasio da kada su u pitanju teme od javnog interesa, državne vlasti moraju izvršiti detaljnu i transparentnu analizu proporcionalnosti ograničenja.

### **4. Kažnjavanje novinara može imati širi „efekat zastrašivanja“ na profesiju**

Iako je kazna bila niska, ESLJP je ukazao da sama činjenica da je novinar osuđen, kao i prethodno hapšenje, pretres i prislušivanje, predstavljaju ozbiljan pritisak koji može obeshrabriti novinare da istražuju teme od javnog značaja.

### **Slučaj ŠEKS protiv HRVATSKE** (*Application no. 39325/20*)<sup>43</sup>

Podnosilac predstavke, bivši visoki hrvatski političar, tražio je pristup dokumentima iz arhive Kancelarije predsednika Republike Hrvatske radi pisanja knjige o stvaranju hrvatske države. Zahtev je upućen kao zahtev za pristup informacijama od javnog značaja.

<sup>43</sup> Za više pogledati: Vlada Republike Hrvatske Ured zastupnika Republike Hrvatske pred Europskim sudom za ljudska prava, Analiza presude Šeks protiv Hrvatske: <https://uredzastupnika.gov.hr/UserDocsImages/dokumenti/Analize%20presuda%20i%20odluka/%C5%A0eks%20-%20analiza%20presude.pdf>

Kako se radilo o dokumentima koji su bili označeni najvišim stepenom tajnosti („državna tajna- strogo poverljivo“) Hrvatski državni arhiv je zatražio mišljenje Kancelarije tadašnje predsednice države. Kancelarija predsednice je, nakon konsultacija sa Vijećem za nacionalnu sigurnost (VNS), skinula oznaku tajnosti sa dela dokumenata i dostavila ih tražiocu, dok je pristup ostalima dokumentima odbijen. Obrazloženje je bilo da bi objava dokumenata mogla naneti štetu nezavisnosti, bezbednosti i međunarodnim odnosima Hrvatske. Tražilac informacija je uložio žalbu Povjereniku za informiranje (Povjerenik), koji je izvršio uvid u tajna dokumenta i potvrdio odluku prvostepenog organa. Visoki upravni sud i Ustavni sud su takođe potvrdili ovu odluku i odbili njegove žalbe.

**Iako je Upravni sud doneo odluku da dokumenta ostanu tajna, važno je istaći i izdvojeno mišljenje jednog od sudija u postupku.<sup>44</sup> Izdvojeno mišljenje ukazuje na dilemu: da li je zaštita nacionalne bezbednosti u ovom slučaju zaista opravdavala tako široko ograničenje pristupa arhivskim dokumentima?**

Po njegovom mišljenju, odluka o uskraćivanju pristupa nije bila dovoljno obrazložena. Smatrao je da ni Povjerenik ni upravni sudovi nisu ispitali suštinsku opravdanost zadržavanja tajnosti (npr. konkretne rizike, vrstu štete, proporcionalnost). Smatrao je da je povređeno pravo na slobodu izražavanja, jer nije jasno utvrđeno da bi objava starih arhivskih dokumenata zaista mogla naneti štetu državi. Naveo je i da odluka predsednice države nije sadržala dovoljno konkretne razloge za odbijanje, te da su samo opšti interesi koji mogu biti povređeni navedeni u odgovoru u odbijanju (bezbednost, međunarodni odnosi), bez objašnjenja zašto bi konkretni dokumenti, stari više decenija, i dalje mogli predstavljati rizik. Sudija je ukazao i da nije sproveden pravi test proporcionalnosti (test javnog interesa), već je odluka zasnovana na apstraktnim pretpostavkama.

**ESLJP je doneo presudu i stao na stanoviše da nije bilo povrede člana 10 Evropske konvencije o ljudskim pravima.** Sud je smatrao da je uskraćivanje pristupa klasifikovanim dokumentima bilo nužno i proporcionalno cilju zaštite nacionalne bezbednosti. Sud je ocenio da je uskraćivanje informacija imalo **jasan zakonski osnov** (Zakon o tajnosti podataka) i da su informacije uskraćene radi zaštite **legitimnih interesa**: nezavisnosti, integriteta, nacionalne bezbednosti i međunarodnih odnosa države. ESLJP je ukazao da je odluka prošla kroz **više nivoa kontrole**, uključujući Kancelariju tadašnje predsednice države, Poverenika, Visoki upravni sud i Ustavni sud.

<sup>44</sup> Izdvojeno mišljenje sudije Ustavnog suda dostupno je u okviru presude Evropskog suda za ljudska prava: [https://hudoc.echr.coe.int/eng#{%22tabview%22:\[%22document%22\],%22itemid%22:\[%22001-215642%22\]}](https://hudoc.echr.coe.int/eng#{%22tabview%22:[%22document%22],%22itemid%22:[%22001-215642%22]})

## Perspektiva civilnog sektora i novinara

Za potrebe ovog istraživanja sprovedena su četiri intervjua sa predstavnicima organizacija civilnog društva i istraživačkim novinarima. Razgovori su obavljeni sa predstavnicima Beogradskog centra za bezbednosnu politiku (BCBP), Regulatornog instituta za obnovljivu energiju i životnu sredinu (RERI), Centra za istraživačko novinarstvo Srbije (CINS) i Mreže za istraživanje kriminala i korupcije (KRIK).

Organizacije i redakcije su odabrane na osnovu analize njihovog rada, kao i konsultativnog sastanka koji su Partneri Srbija organizovali radi prikupljanja uvida o izazovima sa kojima se civilno društvo suočava u pristupu informacijama od javnog značaja.

Intervjui su sprovedeni elektronski putem korišćenjem Zoom aplikacije i u proseku su trajali oko 30 minuta. Tematski su obuhvatali:

1. **Opšta iskustva u pristupu informacijama**, uključujući komunikaciju, saradnju i postupanje institucija po zahtevima za slobodan pristup informacijama od javnog značaja, sa posebnim fokusom na organe sektora bezbednosti.
2. **Odbijanje pristupa i pozivanje na tajnost**, kroz primere uskraćivanja informacija na osnovu Zakona o tajnosti podataka i diskusiju o opravdanosti takvih odluka.
3. **Postupanje po zahtevima za pristup informacijama**, posebno u pogledu rokova i kvaliteta dostavljenih odgovora.
4. **Pravnu zaštitu i postupanje institucija po rešenjima Poverenika**.
5. **Uticaj nedostupnosti informacija** na rad organizacija i novinara, posebno u kontekstu istraživačkog rada i izveštavanja.

U nastavku će biti sumirana iskustva i stavovi učesnika intervjua po gorenavedenim temama.

### Opšta iskustva u pristupu informacijama

Učesnici intervjua ukazuju da je komunikacija sa institucijama, posebno onima iz sektora bezbednosti, dugoročno otežana i da se njihova zatvorenost progresivno povećava još od 2016. godine. Prema oceni organizacija civilnog društva, nekadašnja saradnja bila je bolja dok su u institucijama radili „stariji kadrovi“ koji su poznavali rad civilnog sektora, redovno prisustvovali obukama i događajima i imali razumevanja za potrebe organizacija i novinara. Njihovim odlaskom nestao je i kontinuitet komunikacije, a novi kadrovi nisu uspostavili sličan model saradnje.

**Institucije u sektoru bezbednosti ocenjene su kao jedne od najzatvorenijih, sa minimalnim nivoom spremnosti za razgovor, pružanje informacija ili saradnju.** Organizacije navode da čak i osnovni upiti često ostaju bez odgovora.

**Iz perspektive novinara, situacija je donekle različita u zavisnosti od personalnih rešenja.** U pojedinim ministarstvima postoji komunikacija preko službi za odnose s javnošću, ali se ističe da su i PR službe često ograničene odlukama rukovodilaca, te u praksi mogu da pruže samo minimalne informacije ili formalne odgovore. Ističu da često šalju pitanja institucijama samo da bi zadovoljili novinarsku formu pisanja teksta, bez stvarnih očekivanja da će dobiti sagovornike i odgovore.

**Učesnici napominju da se kvalitet komunikacije „prelama“ preko pojedinaca i njihovog ličnog odnosa prema transparentnosti, što stvara visok stepen nepredvidivosti i neujednačenosti.**

Sveukupna ocena učesnika jeste da je saradnja sa institucijama danas slabija nego ranije, izrazito formalizovana i bez stvarne volje za transparentnošću.

### **Postupanje institucija po zahtevima za pristup informacijama**

Učesnici intervjuja ukazuju na niz ustaljenih problema u načinu na koji institucije postupaju po zahtevima za pristup informacijama od javnog značaja. Najčešće se izdvajaju sledeći trendovi:

- **Ćutanje uprave** predstavlja najrasprostranjeniji oblik uskraćivanja informacija. Institucije često uopšte ne odgovaraju na zahteve, svesne da su predviđene kazne niske i da ne predstavljaju stvarni podsticaj za zakonito postupanje.
- **Formalni odgovori bez suštine**, čak i kada institucije odgovore, često se dostavljaju nepotpuni, formalni ili irelevantni odgovori koji ne sadrže tražene informacije. Na taj način se „zadovoljava forma“, ali ne i suština prava na pristup informacijama.
- **Produžavanje rokova za dobijanje odgovora na 40 dana**, čak i u situacijama kada tražene informacije nisu velikog obima.
- **Odbijanje dostavljanja traženih informacija, uz pozivanje na razne osnove za ograničenje pristupa**, najčešće se koriste argumenti da je tražena informacija klasifikovana kao tajna, da predstavlja poslovnu tajnu ili da njeno dostavljanje može ugroziti zaštitu ličnih podataka, često i u situacijama kada takva pravna zaštita nije jasno opravdana.



## Odbijanje pristupa i pozivanje na tajnost

Imajući u vidu da je predmet ove analize primena Zakona o tajnosti podataka, tokom intervjua najveća pažnja je posvećena slučajevima u kojima je tajnost korišćena kao argument za odbijanje pristupa informacijama. Sagovornici su ukazali da se u praksi javlja zabrinjavajući trend **prekomernog označavanja podataka kao tajnih**, često u situacijama gde ne postoji jasna ili zakonski opravdana potreba za takvom vrstom ograničenja. Na ovo ukazuju i brojni primeri iz medija.

Jedan od ilustrativnih primera odnosi se na **slučaj renoviranja zdanja „Klub poslanika“**, za koje je država potrošila milionske iznose, da bi objekat potom bio dat na korišćenje biznismenu Aleksandru Kajmakoviću. Ugovori u vezi sa tim aranžmanom proglašeni su „tajnom“, iako se radi o očigledno javnim sredstvima i javnoj imovini, gde interes za transparentnost preteže.<sup>45</sup>

Slično tome, Vlada Srbije je odlukom označila kao **tajne dokumente koji se odnose na izgradnju spomenika Stefanu Nemanji**. Čak ni visina ukupnih troškova, što predstavlja tipičan primer informacije od nesumnjivog javnog interesa, nije dostupna javnosti. Iako je prema ranijim najavama oznaka tajnosti trebalo da bude skinuta 2023. godine<sup>46</sup>, do toga nije došlo, a podaci o troškovima ostaju nedostupni javnosti. Ovaj primer posebno ukazuje na nedostatak doslednosti u primeni zakona, kao i na problem izostanka jasnog obrazloženja zbog čega bi objavljivanje takve vrste informacija moglo da ugrozi bilo koji zakonom zaštićeni interes.

Upravo ovi slučajevi, široko poznati javnosti, potvrđuju ono što su sagovornici u istraživanju isticali: **institucije neretko koriste oznaku tajnosti na način koji prevazilazi njenu svrhu**, čime se smanjuje transparentnost, slabi poverenje javnosti i otežava demokratski nadzor nad radom organa vlasti.

## Imena poslanika koji poseduju sertifikate za pristup tajnim podacima

Za potrebe pripreme godišnjih izveštaja Koalicije prEUgovor, koja prati sprovođenje obaveza Srbije u procesu pristupanja EU u okviru klastera 1, 2023. upućen je zahtev Narodnoj skupštini sa pitanjem o broju i imenima narodnih poslanika koji poseduju sertifikate za pristup tajnim podacima. Ovi sertifikati su neophodni poslanicima kako bi mogli da

<sup>45</sup> N1, Država potrošila milione na "Klub poslanika" pa ga dala na korišćenje Aci Bosancu: Detalji iz ugovora proglašeni za "tajnu": <https://n1info.rs/vesti/drzava-potrosila-milione-na-klub-poslanika-pa-ga-dala-na-koriscenje-aci-bosancu-detalji-iz-ugovora-proglaseni-za-tajnu/>

<sup>46</sup> N1, Koliko košta spomenik Stefanu Nemanji i dalje tajna: U čijem je interesu da se cena krije: <https://n1info.rs/vesti/koliko-kosta-spomenik-stefanu-nemanji-i-dalje-tajna-u-cijem-je-interesu-da-se-cena-krije/>

razmatraju izveštaje bezbednosnih službi, nadziru trošenje budžeta i planiraju kontrolne posete, i neophodni su za rad članova skupštinskih odbora nadležnih za sektor bezbednosti.

U svom odgovoru, Narodna skupština je dostavila samo broj poslanika sa sertifikatima, ali ne i njihova imena.<sup>47</sup> Ovde je potrebno istaći i da je Kancelarija Saveta za nacionalnu bezbednost i zaštitu tajnih podataka na isti zahtev za pristup informacijama, odgovorila identično, odnosno nije dostavila informacije o imenima poslanika koji imaju sertifikat.<sup>48</sup>

Istovetni zahtev je, ranije 2019. uputila i organizacija Beogradski centar za bezbednosnu politiku (BCBP), koja je dobila isti odgovor. U obrazloženju odgovora iz 2019. godine<sup>49</sup>, Narodna skupština je navela:

*“Navodimo da je prema članu 35. stavu 1. i 2. Zakona o tajnosti podataka dostavljanje tajnih podataka moguće isključivo ovlašćenim licima koja poseduju sertifikat za pristup podacima označenim stepenom tajnosti kao i da spisak narodnih poslanika sa traženim podacima nismo u mogućnosti da dostavimo i na osnovu Zakona o zaštiti podataka o ličnosti.”*

Ukoliko ovaj odgovor razmotrimo, a na osnovu svega što je izneto u ovoj analizi može se zaključiti da Narodna skupština nije pravilno postupila po ovom zahtevu. Suprotno obavezama iz ZoSPIJZ, Skupština nije ukazala na konkretnu odluku o tajnosti ove evidencije, niti je obrazložila na koji način bi objavljivanje ovih informacija povredilo druge zaštićene interese (tajnost ili privatnost), a što je neophodno dokazati u slučaju da se pravo na pristup informacijama ograničava. Imajući u vidu ustavnu ulogu i nadležnosti narodnih poslanika u vršenju demokratskog nadzora, ove informacije moraju biti javne kako bi se osiguralo transparentno i odgovorno funkcionisanje parlamentarnog nadzora nad sektorom bezbednosti.

### Objavljivanje tajnih podataka u medijima od strane visokih funkcionera

Intervjuima je pokrenuto i pitanje šta se dešava kada visoki javnih funkcioneri iznose u javnost podatke koji su označeni nekim stepenom tajnosti. Takav slučaj je bio i kada je predsednik države prilikom gostovanja u emisiji „Novo jutro“ na TV Pink dana 1. 8. 2019.<sup>50</sup>

<sup>47</sup> Izveštaj koalicije prEUgovor o napretku Srbije u klasteru 1 - maj 2023, str 32: <https://www.preugovor.org/Alarm-izvestaji/1809/Izvestaj-koalicije-prEUgovor-o-napretku-Srbije-u.shtml>

<sup>48</sup> Izveštaj koalicije prEUgovor o napretku Srbije u klasteru 1 - maj 2023, str 32: <https://www.preugovor.org/Alarm-izvestaji/1809/Izvestaj-koalicije-prEUgovor-o-napretku-Srbije-u.shtml>

<sup>49</sup> Odgovor na zahtev za pristup informacijama od javnog značaja, Narodne skupštine br: 21 broj 9-447/19, od 21.03.2019.

<sup>50</sup> N1, Vučić prekršio zakon - još nema odgovora N1 o skidanju oznake "državna tajna", (u tekstu se nalazi sporno tv gostovanje): <https://n1info.rs/vesti/a523957-Vucic-prekrasio-zakon-jos-nema-odgovora-N1-o-skidanju-oznake-drzavna-tajna/>

godine javno izneo podatke o prisluškivanju, koji su se odnosili i na njega- dokument koji je nastao u radu BIA, odnosno resora Državne bezbednosti. Na televizijskom snimku se jasno videlo da dokumenta nose oznaku „DRŽAVNA TAJNA“. U kasnijem obraćanju javnosti, 03.8.2019. godine, predsednik je rekao „da je kao ovlašćeno lice skinuo oznaku tajnosti, jer su podaci u interesu javnosti“. U ovom slučaju jedna organizacija je podnela zahtev za pristup informacijama Bezbednosno- informativnoj agenciji kako bi utvrdila da li je postupak skidanja tajnosti sproveden u skladu sa Zakon o tajnosti podataka, ali BIA nije odgovorila na zahtev.

U poglavlju o praksi Poverenika već je pomenut slučaj u kojem je MUP odbio da dostavi sistematizaciju radnih mesta, pozivajući se na tajnost. Veoma sličan odgovor dobili su i novinari u martu 2023, koji su od Ministarstva odbrane tražili podatke o isplatama i imenima savetnika u Ministarstvu odbrane. U odgovoru<sup>51</sup> kojim se odbija pristup traženim informacijama, Ministarstvo je navelo da je Pravilnik o uređenju i sistematizaciji radnih mesta u Ministarstvu odbrane označen određenim stepenom tajnosti, budući da njegov sastavni deo čine podaci o formacijama i profesionalnim pripadnicima Vojske Srbije. U odgovoru je takođe navedeno da Ministarstvo redovno ažurira Informator o radu.

Međutim, kako su potvrdili sami novinari, ali i kako je utvrđeno tokom ovog istraživanja, podaci koji su traženi se ne nalaze u Informatoru o radu. Posebno je značajno istaći da su i Partneri Srbija dobili gotovo identičan odgovor na zahtev za pristup informacijama kojim je tražena informacija o broju zaposlenih u Ministarstvu odbrane, u martu 2025.<sup>52</sup> Uporednom analizom ova dva odgovora ustanovljeno je da se organ u oba slučaja koristio gotovo istim formulacijama: pozivanje na tajnost Pravilnika o sistematizaciji radnih mesta i upućivanje na Informator o radu. Ministarstvo odbrane je u oba slučaju propustilo da donese obrazloženo rešenje o odbijanju zahteva. U oba odgovora izostalo je bilo kakvo obrazloženje o tome kako bi dostavljanje traženih informacija moglo da ugrozi interese zaštićene oznakom tajnosti. Ministarstvo je u oba slučaju odbilo i da primeni načelo razdvajanja podataka, odnosno obavezu da se iz dokumenta izdvoje informacije koje same po sebi ne mogu da proizvedu štetu po zaštićeni interes, dok preostali sadržaj nastavlja da uživa odgovarajuću zaštitu.

Na osnovu ova dva odgovora može se zaključiti da Ministarstvo odbrane primenjuje iste nezakonite prakse pri odgovaranju na zahteve za pristup informacijama od javnog značaja.

<sup>51</sup> Ministarstvo odbrane, dopis br. 128-9/23, od 30.03.2023.

<sup>52</sup> Ministarstvo odbrane, dopis br. 199-4/25, od 15.04.2025.

Povodom ovog odgovora Partneri Srbija su izjavili žalbu Povereniku, a postupak je i dalje u toku,

Takvo postupanje direktno dovodi do umanjenja transparentnosti i predstavlja nesrazmerno ograničenje prava javnosti da zna.

### Pravna zaštita i postupanje institucija po rešenjima Poverenika

Sagovornici su ukazali da je pravna zaštita u oblasti pristupa informacijama o radu institucija **formalno postojeća, ali u praksi često ne obezbeđuje efikasnu i blagovremenu zaštitu prava tražilaca informacija**. Svedočenja ispitanika ukazuju da postupci po žalbama neretko traju mesecima, pa čak i više godina, što bitno umanjuje svrhu ovog mehanizma i obeshrabruje tražioce informacija da izjave žalbe naročito kada se radi o podacima koji su vremenski osetljivi.

Značajan broj sagovornika skrenuo je pažnju na to da Poverenik, umesto da meritorno odluči o zahtevu, što mu ZoSPIJZ omogućava, često donosi rešenja kojima vraća predmet organu vlasti na ponovno odlučivanje. U mnogim slučajevima organ potom ponavlja identičan odgovor, pa sledi novo ulaganje žalbe i novi postupak pred Poverenikom. Postoje slučajevi u kojima je Poverenik dva puta uzastopno vraćao predmet istom organu na ponovno odlučivanje, iako je iz okolnosti predmeta bilo jasno da organ neće postupiti u skladu sa zakonom i da bi meritorno odlučivanje bilo jedino delotvorno rešenje.

Ovakva praksa stvara **začarani krug neefikasnosti** i dodatno otežava ostvarivanje prava na pristup informacijama, jer institucije faktički ne snose posledice nezakonitog postupanja, a tražene informacije gube relevantnost. Sagovornici su ocenili da takav pristup obeshrabruje građane, novinare i organizacije civilnog društva da koriste mehanizme za zaštitu prava na pristup informacijama, jer se postupak može pretvoriti u dugotrajnu i iscrpljujuću proceduru bez jasnog ishoda.

### Uticaj nedostupnosti informacija na rad organizacija i novinara

Sagovornici su istakli da nedostupnost informacija i praksa prekomernog označavanja podataka kao tajnih imaju **direktan i veoma negativan uticaj** na rad organizacija civilnog društva i novinara. U istraživačkom radu, pravovremeni pristup informacijama predstavlja osnovni preduslov za kvalitetno izveštavanje, kontrolu rada institucija i otkrivanje nepravilnosti. Kada institucije uskraćuju pristup informacijama ili odugovlače odlučivanje, posledice su višestruke: smanjuje se transparentnost javnih politika, otežava otkrivanje nepravilnosti i korupcije i slabi poverenje građana u institucije.

## Zaključak

Analiza normativnog okvira, institucionalne prakse i iskustava civilnog sektora i novinara pokazuje da Zakon o tajnosti podataka, iako je formalno zasnovan na savremenim standardima zaštite tajnih podataka, u praksi ne obezbeđuje uravnotežen sistem koji jednako štiti legitimne bezbednosne interese države i pravo javnosti da zna. **Umesto da tajnost bude usko definisan, strogo ograničen izuzetak, ona je u Srbiji slabo kontrolisano sredstvo ograničavanja pristupa informacijama od javnog značaja.**

Normativno, **ključni problemi su neprecizno i preširoko definisanje pojma tajnih podataka, kriterijuma za klasifikaciju i nepostojanje nadzora nad primenom Zakona o tajnosti podataka.** Problem predstavljaju i kaznene odredbe, koje **ne prepoznaju nezakonito označavanje podataka kao tajnih** niti zloupotrebe u postupku klasifikacije kao radnje jednako ozbiljne onima koje se odnose na neovlašćeno odavanje tajnih podataka. U važećem okviru **u potpunosti izostaju krivične ili bilo kakve ozbiljnije pravne posledice** za organ ili pojedinca koji nezakonito, neopravdano ili zloupotrebljavajući ovlašćenja proglase podatke tajnim. Time se zanemaruje činjenica da **neosnovana klasifikacija može proizvesti jednako teške posledice po javni interes.**

**Dodatan nedostatak Zakona je i prepuštanje da se materija zakona u velikom delu uredi podzakonskim aktima.** Prekomerna razuđenost normativnih akata dovodi do pravne nesigurnosti i otežava doslednu primenu zakona, jer se ključni elementi zakona uključujući kriterijume za klasifikaciju, postupke procene i zaštite tajnih podataka, postupci interne kontrole, i dr. izmeštaju u uredbe i pravilnike. Time se omogućava da se kroz podzakonske akte uređuje materija koja bi morala biti u domenu zakonodavne vlasti. Ovo ujedno podriva demokratski i participativni proces izrade javnih politika, jer donošenje i izmena podzakonskih akata ne zahtevaju javnu raspravu, uključivanje javnosti niti parlamentarnu raspravu, već se sprovode isključivo voljom izvršne vlasti.

Definicije i kriterijumi za klasifikaciju poput „podatak od interesa za Republiku Srbiju“, kao i opšti pojmovi „štete“ i „ugrožavanja interesa“, ostavljaju širok prostor za arbitrarno tumačenje. Posebno problematična je kategorija „INTERNO“, koja je u praksi često mesto „parkiranja“ informacija koje po međunarodnim standardima ne bi trebalo da budu tajne, već samo administrativno ograničene, ako uopšte.

**Nadzor nad primenom Zakona pokazao se kao najslabija karika sistema. Ministarstvo pravde, koje je zakonom određeno kao ključni nadzorni organ, u praksi već godinama faktički ne vrši nadzor.** Zbog toga u praksi niko ne kontroliše postupanje institucija u ovoj oblasti. Istovremeno, Kancelarija Saveta za nacionalnu bezbednost i zaštitu tajnih podataka,

koja ima najbolji pregled nad sistemom i najveće kapacitete (iako nedovoljne), nema formalnu nadležnost da utiče i bude korektiv organa javne vlasti u ovoj oblasti. Imajući u vidu da je ona osmišljena kao tehnička i operativna kancelarija Vlade Srbije, odnosno Saveta bezbednosti, možda treba razmotriti u budućim reformama njeno izdvajanje iz izvršne vlasti i dobijanje većih ovlašćenja u ovoj oblasti.

**Sudska i prekršajna praksa u oblasti tajnosti gotovo da ne postoji. Podaci prikupljeni od prekršajnih sudova pokazuju da se prekršajni postupci po Zakonu o tajnosti podataka ne vode, iako zakon propisuje širok spektar povreda koje bi mogle biti sankcionisane. Krivični postupci su retki, a izrečene kazne pretežno blage.**

U takvom kontekstu, jedini stvarni mehanizam kontrole nad prekomernom tajnošću ostaje žalbeni postupak pred Poverenikom. Međutim, **praksa Poverenika ne obezbeđuje uvek delotvornu i blagovremenu zaštitu. Žalbeni postupci često traju mesecima, pa i godinama. Dodatno, Poverenik neretko vraća predmete organima na ponovno odlučivanje umesto da meritorno odluči i naloži dostavljanje informacija.** Ovakvo postupanje obesmišljava pravo na pristup informacijama, posebno kada je reč o temama koje su vremenski osetljive.

**Dodatan problem predstavlja uvođenje režima tajnosti kroz zakone iz oblasti sektora bezbednosti.** Ovo je sistemski problem jer se time zaobilaze opšti zakonski kriterijumi za klasifikaciju podataka, podaci određuju unapred tajni prema vrsti podataka, a ne prema stvarnoj šteti koja može da nastane njihovim otkrivanjem, omogućava proizvoljno i prekomerno uskraćivanje informacija i ozbiljno ugrožavaju principi transparentnosti, pravne sigurnosti i demokratskog nadzora nad sektorom bezbednosti.

Polazeći od svega navedenog, može se zaključiti da postojeći režim tajnosti podataka u Srbiji normativno i institucionalno ne funkcioniše: fokusiran je gotovo isključivo na zaštitu „državnih interesa“ u uskom, tradicionalnom smislu, dok istovremeno zanemaruje zaštitu javnog interesa, ustavno načelo transparentnosti i međunarodne standarde koji zahtevaju strogo ograničen, precizno definisan i nadzirani režim tajnosti. Umesto da tajnost bude izuzetak, u praksi ona postaje sredstvo prikrivanja informacija o trošenju javnih sredstava, odgovornosti nosilaca javnih funkcija i radu bezbednosnog sektora.

Zbog toga je neophodna temeljna reforma Zakona o tajnosti podataka i pratećih mehanizama, koja bi obuhvatila najmanje sledeće pravce:

- ❖ **preciznije definisanje pojma tajnog podatka i kriterijuma za klasifikaciju**, uz usklađivanje sa evropskim standardima i jasnim insistiranjem na tome da se tajnost

ne može odnositi na informacije o kršenju ljudskih prava, korupciji, zloupotrebi ovlašćenja i trošenju javnih sredstava;

- ❖ **uspostavljanje funkcionalnog, nezavisnog i stručnog nadzornog mehanizma;**
- ❖ **reformu kaznenih odredbi** u pravcu uvođenja ozbiljnijih sankcija, uključujući i krivičnu odgovornost za namerno ili sistemsko nezakonito označavanje podataka kao tajnih;
- ❖ **jačanje uloge Poverenika** kroz podsticanje meritornog odluka, i kraće rokove za postupanje po žalbama;
- ❖ **obustavljanje prakse uvođenja tajnosti kroz sektorske zakone**
- ❖ **normativno i praktično jačanje načela „transparentnost je pravilo, tajnost izuzetak“**, uz obavezu redovne revizije klasifikacije, proaktivno objavljivanje što šireg spektra informacija i ograničavanje trajanja tajnosti.

## Aneks 1: Metodologija istraživanja

Istraživanje je sprovedeno primenom kombinovanog kvalitativnog metodološkog pristupa, koji obuhvata analizu pravnog okvira, prakse institucija i sudova, kao i prikupljanje podataka od relevantnih aktera kroz intervju i konsultativne procese. Cilj primenjene metodologije bio je da omogući sveobuhvatno sagledavanje primene Zakona o tajnosti podataka i povezanih propisa, kao i uočavanje ključnih izazova u praksi.

### 1. Analiza domaćeg pravnog okvira

Sprovedena je detaljna analiza važećeg domaćeg zakonodavstva i podzakonskih akata koji se odnose na oblast tajnosti podataka i transparentnosti rada institucija. Analizirani su, Zakon o tajnosti podataka, Zakon o inspeksijskom nadzoru, zakoni koji uređuju rad i nadležnosti organa sektora bezbednosti (Zakon o VBA i VOA, BIA, i drugi), Zakon o policiji, Zakon o slobodnom pristupu informacijama od javnog značaja, drugi relevantni zakoni, uredbe i pravilnici, a koji se odnose na oblast tajnosti podataka.

### 2. Analiza sudske prakse, nadzora i prakse nezavisnih institucija

Za prikupljanje podataka o postupanju organa javne vlasti u vezi sa ovom oblašću poslati upućeni su i zahtevi za pristup informacijama od javnog značaja, sledećim institucijama:

- ❖ Svim višim sudovima u Srbiji (20 sudova);
- ❖ prekršajnim sudovima, na uzorku koji obuhvata oko 60% ukupnog broja sudova (27 sudova);
- ❖ Povereniku za informacije od javnog značaja i zaštitu podataka o ličnosti (2 zahteva);
- ❖ Ministarstvu pravde (2 zahteva).

Cilj ove aktivnosti bio je da se utvrdi kako organi vlasti u praksi postupaju u slučajevima koji se odnose na tajne podatke, posebno u delu kontrole, nadzora i sudske zaštite.

### 3. Analiza sekundarnih izvora i međunarodnog normativnog okvira

Istraživanje je uključilo pregled postojećih analiza i izveštaja međunarodnih organizacija, akademske zajednice, civilnog sektora i stručne literature. Posebna pažnja posvećena je:

- ❖ praksi Evropskog suda za ljudska prava u predmetima koji se odnose na slobodu izražavanja, pristup informacijama i ograničenja zasnovana na tajnosti podataka i zaštiti nacionalne bezbednosti;



- ❖ relevantnim standardima i dokumentima EU.

#### **4. Prikupljanje informacija od organizacija civilnog društva i novinara**

U okviru istraživanja organizovan je zatvoreni konsultativni sastanak sa članicama Koalicije za slobodan pristup informacijama, na kojem se diskutovalo o izazovima u oblasti pristupa informacijama od javnog značaja, i slučajevima u kojima su organi vlasti odbijali pristup informacijama pozivajući se na tajnost.

Pored toga, sprovedena su i četiri intervjua sa predstavnicima organizacija civilnog društva i istraživačkim novinarima koji se u svom radu suočavaju sa ograničenjima pristupa informacijama.

Za potrebe istraživanja pokušano je i organizovanje intervjua sa predstavnicima Kancelarije saveta za nacionalnu bezbednost i zaštitu tajnih podataka. Uprkos tome što je poziv upućen tri puta, odgovor nije dobijen.

