



БЕЗБЕДНОСТ

ЧАСОПИС
МИНИСТАРСТВА
УНУТРАШЊИХ ПОСЛОВА
РЕПУБЛИКЕ СРБИЈЕ

БЕОГРАД, година LXVII 3/2025

„БЕЗБЕДНОСТ“
Часопис Министарства унутрашњих послова Републике Србије
УРЕДНИШТВО

Проф. др Божидар Ойашевић, Криминалистичко-полицијски универзитет
Проф. др Миливој Дойсај, Факултет спорта и физичког васпитања Универзитета у Београду
Проф. др Ивана Богрожић, Криминалистичко-полицијски универзитет
Проф. др Тијана Шурлан, судија Уставног суда Републике Србије
Проф. др Бојан Милисављевић, Правни факултет Универзитета у Београду
Проф. др Миле Шикман, Правни факултет Универзитета у Бања Луци,
начелник Управе за полицијску обуку, Министарство унутрашњих послова Републике Српске
Проф. др Младен Милошевић, Факултет безбедности Универзитета у Београду
Др Жељко Бркић, Министарство унутрашњих послова Републике Србије
Доц. др Данило Сивевандић, Министарство унутрашњих послова Републике Србије
Др Кайарина Живановић, Министарство унутрашњих послова Републике Србије
Др Најша Рагосављевић-Сивевановић, Министарство унутрашњих послова Републике Србије
Доц. др Владимир Шебек, Министарство унутрашњих послова Републике Србије
Др Илија Раџић, Министарство унутрашњих послова Републике Србије
Марина Васић Мрдак, Министарство унутрашњих послова Републике Србије
Ивана Мишић, Министарство унутрашњих послова Републике Србије

ГЛАВНИ И ОДГОВОРНИ УРЕДНИК

Проф. др Божидар Ойашевић

УРЕДНИК II

Јасмина Владисављевић

ЛЕКТУРА И КОРЕКТУРА

Јасмина Милејић

ЛЕКТОР ЗА ЕНГЛЕСКИ ЈЕЗИК

Весна Анђелић-Николенџић

АДРЕСА УРЕДНИШТВА: Булевар Зорана Ћинђића 104, Београд
011/3148-734, 3148-739, имејл: upobr@mup.gov.rs

ЧАСОПИС ИЗЛАЗИ ТРИ ПУТА ГОДИШЊЕ (тираж: 800 примерака)
ПДФ верзија часописа доступна је на адреси: <http://www.mup.gov.rs> у поднаслову Публикације

Штампа: www.grafikcentar.com

САДРЖАЈ

ОРИГИНАЛНИ НАУЧНИ РАДОВИ

Проф. др Саша М. МАРКОВИЋ	5	ПРЕВЕНЦИЈА ИНТИМНО-ПАРТНЕРСКОГ ФЕМИЦИДА У РЕПУБЛИЦИ СРБИЈИ
---------------------------	---	------------------------------------------------------------

ПРЕГЛЕДНИ НАУЧНИ РАДОВИ

Zsolt, LIPPAI Béla, ÁRPÁS Pál, KARDOS	59	ПРИВАТНЕ ИСТРАГЕ У РЕПУБЛИЦИ МАЂАРСКОЈ
Доц. др Марија ПОПОВИЋ МАНЧЕВИЋ	61	ПОЛИЦИЈСКА ДИПЛОМАТИЈА У БОРБИ ПРОТИВ ГЛОБАЛНОГ ТЕРОРИЗМА: ИЗАЗОВИ И ПЕРСПЕКТИВЕ
Проф. др Дарко Т. ДИМОВСКИ	101	КРИМИНОЛОГИЈА СВЕМИРСКОГ ПРОСТОРА – ФЕНОМЕН ЈЕДНЕ УТОПИЈЕ ИЛИ РЕАЛНОСТ АПСУРДА
Проф. др Горан МАТИЋ	141	АНАЛИЗА ТРЕНДОВА У БЕЗБЕДНОСНИМ ПРОВЕРАМА ПРИПАДНИКА МИНИСТАРСТВА УНУТРАШЊИХ ПОСЛОВА У КОНТЕКСТУ СПРОВОЂЕЊА ЗАКОНА О ТАЈНИМ ПОДАЦИМА (2019–2024)
Санела Д. АНДРИЋ Ана С. МУТАВЏИЋ Весела М. МИЛОВАНОВИЋ	143	ЕТИЧКИ И БЕЗБЕДНОСНИ АСПЕКТИ УПОТРЕБЕ ОТИСАКА ПАПИЛАРНИХ ЛИНИЈА КАО БИОМЕТРИЈСКЕ ИДЕНТИФИКАЦИЈЕ
Ненад Н. КОВАЧЕВИЋ Немања Р. СТЕВАНОВИЋ	163	ДРУШТВЕНО-ПРАВНА ОГРАНИЧЕЊА У ПРИМЕНИ ЗАКОНА О СЛОБОДНОМ ПРИСТУПУ ИНФОРМАЦИЈАМА ОД ЈАВНОГ ЗНАЧАЈА
	189	УПУТСТВО АУТОРИМА

CONTENTS

ORIGINAL SCIENTIFIC PAPERS

- Prof Saša M. MARKOVIĆ, PhD **29** PREVENTION OF INTIMATE PARTNER FEMICIDE IN THE REPUBLIC OF SERBIA

REVIEW PAPERS

- Zsolt, LIPPAI
Béla, ÁRPÁS
Pál, KARDOS **31** PRIVATE INVESTIGATION IN THE REPUBLIC OF HUNGARY
- Marija POPOVIĆ MANČEVIĆ, PhD **98** POLICE DIPLOMACY AND GLOBAL COUNTERTERRORISM EFFORTS: CHALLENGES AND PERSPECTIVES
- Prof Darko T. DIMOVSKI, PhD **121** SPACE CRIMINOLOGY – A UTOPIAN PHENOMENON OR AN ABSURD REALITY
- Prof Goran MATIĆ, PhD **123** ANALYSIS OF TRENDS IN SECURITY VETTING OF MINISTRY OF INTERNAL AFFAIRS PERSONNEL IN THE CONTEXT OF THE IMPLEMENTATION OF THE LAW ON CLASSIFIED INFORMATION (2019–2024)
- Sanela D. ANDRIĆ
Ana S. MUTAVDŽIĆ
Vesela M. MILOVANOVIĆ **162** ETHICAL AND SECURITY ASPECTS OF THE USE OF PAPILLARY LINE IMPRINTS AS BIOMETRIC IDENTIFICATION
- Nenad N. KOVAČEVIĆ
Nemanja R. STEVANOVIĆ **187** SOCIO-LEGAL CONSTRAINTS IN THE IMPLEMENTATION OF THE LAW ON FREE ACCESS TO INFORMATION OF PUBLIC IMPORTANCE
- 189** INSTRUCTIONS FOR AUTHORS

Проф. др Саша М. МАРКОВИЋ¹
Криминалистичко-полицијски универзитет, Београд

ДОИ: 10.5937/bezbednost2503005M
УДК: 343.85:343.61-055.2(497.11)“2018/2024“

Оригинални научни рад
Примљен: 10. 10. 2025. године
Ревизија: 1. 11. 2025. године
Датум прихватања: 24. 11. 2025. године

Превенција интимно-партнерског фемицида у Републици Србији

Апстракт: Предмет овог рада је анализа деловорности мера које надлежне институције Републике Србије предузимају с циљем превенције убиства жена од стране мушкараца приликом вршења насиља у интимно-партнерским односима. Фемицид је најчешћи облик родно заснованог насиља, а број убијених жена од стране партнера у току или након завршетка брачног, ванбрачног или другог интимно-партнерског односа представља глобалан друштвени проблем који постоји већину држава у свету. Савет Европе је с циљем превенције насиља у породици на подручју европских држава усвојио 2011. године Истанбулску конвенцију. Мада се текстови Конвенције односе на превенцију и заштити свих жртва насиља у породици, главни циљ њеног доношења била је превенција родно заснованог насиља над женама и њихова заштита. Србија је, након ратификовања Конвенције, 2016. године усвојила посебан закон који је разрадио њене одредбе и прописао проактиван начин рада надлежних органа заснован на процени и управљању ризиком од насиља у породици од првог сазнања о учињеном насиљу, као и након сазнања да до насиља

¹ sasamarkovic975@gmail.com, ORCID 0000-0003-1025-7961

може доћи уколико насиље није вршено у прошлости. Главне циљеве истраживања надлежних органа моћи бисмо дефинисати на следећи начин: оснаживање жртва како бисмо их подстигли да пријаве насиље, а то подразумева повећање поверење жртва у полицију и друге надлежне институције с циљем смањивања тамне бројке; заштитна жртва од поновљеног насиља и сарађивање истраживања најтежих последица, насиља телесних повреда и лишење живота жртве; решавање проблема уклањањем узрока насиља, што подразумева и забрану приласка учиниоца жртви и забрану контаката. У раду су приказани резултати истраживања које је обухватило све евиденциране догађаје интимно-партнерског насиља у Србији у којима је извршен фемцид након почетка примене Закона о сарађивању насиља у породици, у седмогодишњем периоду од 2018. до 2024. године. Детаљно је анализирано седам случајева убиства жена у којима је полиција имала сазнања о учињеном насиљу у породици пре извршења убиства.

Кључне речи: фемцид, насиље у породици, интимно-партнерски однос, превенција, жртва.

Увод

Убиство је кривично дело које подразумева лишење живота другог лица и сврстано је у област кривичних дела против живота и тела. Инкриминацијом убиства штити се право на живот човека које, како је једнодушно прихваћено, представља врховно људско право које се налази испред сваког другог права (Коларић, 2015: 146). Многа истраживања спроведена у Србији и свету показују да су учиниоци убиства у преко 85% случајева мушкарци и да убиство најчешће врше употребом ватреног оружја или оштрог предмета (ножа, секире, итд.) (Константиновић Вилић, Петрушић, Бекер, 2019: 19–21). Фемцид представља најтежи облик насиља над женама (Лубура, 2017: 117). То је, пре свега, криминолошки појам, а мали број држава, углавном латиноамеричких, инкриминисао је кривично дело са тим називом. Тако је, на пример Боливија

2013. инкриминисала кривично дело под овим називом (Батричевић, 2016: 438–439). У Бразилу, Чилеу, Колумбији, Костарики, Еквадору, Ел Салвадору, Гватемали, Хондурасу, Мексику, Никарагви, Панами, Перуу и Доминиканској Републици такође постоји кривично дело са овим називом, али дефиниције варирају и само у неколико држава је прописано да је учинилац искључиво мушкарац (Константиновић Вилић, Петрушић, Бекер, 2019: 90). У литератури се као главни разлог за неинкриминисање фемцида у кривичним законодавствима европских држава наводи то да су мушкараци и жене изједначени пред законом па би се, евентуално, могло поставити питање дискриминације једног пола у односу на други. У појединим кривичним законодавствима (на пример Шпаније и Швајцарске) жртве које спадају у посебно рањиве групе лица (жене, стара лица, деца и немоћна лица) посебно су заштићене када су оштећене кривичним делом са елементима насиља и за учиниоца је предвиђена строжа санкција (Марковић, Достић, 2025: 60). Хрватска је 2024. године инкриминисала кривично дело под називом „тешко убиство женске особе”. Основни облик подразумева чињење родно заснованог убиства женске особе. Запрећена је затворска казна од најмање десет година или казна дуготрајног затвора² (Казнени закон Републике Хрватске, члан 111а). Северна Македонија је 2023. године, чланом 6 Закона о изменама и допунама Кривичног законика, инкриминисала нови квалификовани облик кривичног дела „убиство” који подразумева лишење живота женске особе или девојчице млађе од 18 године приликом вршења родно заснованог насиља (КЗ, члан 123, став 2, тач. 2а). Запрећена је затворска казна од најмање десет година или казна доживотног затвора.

У српском кривичном законодавству инкриминисано је кривично дело „насиље у породици” (Кривични законик, члан 194). Уколико услед чињења основног и првог квалификованог облика наступи смрт лица, предвиђен је најтежи квалификовани облик овог кривичног дела и казна од пет до петнаест година затвора, с тим да је предвиђена још строжа санкција уколико је лишено живота малолетно лице. Предвиђена је казна затвора од најмање

² Казна дуготрајног затвора дефинисана је чланом 46 КЗРХ.

десет година. Међутим, наступање смртне последице мора да буде обухваћено нехатом учиниоца. Од 9. септембра 2025. године траје јавна расправа о Нацрту Закона о изменама и допунама КЗ којим је, између осталог, предвиђено поштравање казне за све облике кривичног дела „насиље у породици”, осим за овај најтежи облик. Предлагач закона, Министарство правде, у образложењу измена и допуна, у делу који се односи на поштравање казни за ово кривично дело наводи да се очекује да би усвајање предлога значајно охрабрило све жене и остале жртве да не трпе насиље и да сваки облик насиља без страха пријаве и да буду уверени да ће их држава заштитити (Министарство правде, 2025). Такође, Кривични законик одредбама члана 54а предвиђа могућност примене посебне околности за одмеравање казне за кривично дело учињено из мржње, између осталог, због пола другог лица. Осим тога, уколико су испуњени услови, могуће је дело квалификовати као тешко убиство члана своје породице који је претходно злостављан (члан 114, став 1, тач. 10 КЗ).

Иако јединствена дефиниција појма „фемцид” до данас није установљена, у литератури се најчешће помиње да је највећи допринос у утврђивању значења овог криминолошког појма дала Дајана Расел (*Diana Russell*) која је у својој књизи „Силовање у браку” фемцид означила као „убиство жене зато што је жена” (Russell, 2008: 26). Затим је 1990. године са коауторком Џејн Капути (*Jane Caputi*) фемцид одредила као „убијање жена од стране мушкараца мотивисано мржњом, презиром, задовољством или осећањем власништва и надмоћи над женама” и на крају је 2001. године, заједно са Робертом Хармс (*Roberta Harmes*) дала верзију термина фемцид која покрива све манифестације мушког сексизма, а не само мржњу: „убиство женских особа од стране мушких особа зато што су женског пола”. Такође, користила је термин „женске особе” уместо „жене” како би укључила девојчице и женске бебе које су често жртве фемцида. По истом принципу, користила је и термин „мушке особе” јер су и дечаци и младићи често учиниоци фемцида (Russell, 2008: 27). Приликом дефинисања овог појма, Раселова је истицала да пол жртве мора бити разлог чињења убиства, јер ако мушка особа убије женску особу из неког другог разлога, односно убиство није мотивисано полом жртве, не ради се о фемциду.

Статистички оквир за мерење родно заснованог убијања жена и девојчица (такође називан „фемцид/феминцид“), који су заједнички развили Канцеларија УН за борбу против дроге и криминала (UNODC) и УН Жене (UN Women), а који је у марту 2022. године одобрила Статистичка комисија УН, идентификује три типа фемцида који подразумевају умишљајно убиство особа женског пола (жена и девојчица) од стране: 1. интимних партнера; 2. других чланова породице; 3. особа које нису интимни партнери или чланови породице, а које испуњавају бар један од осам критеријума утврђених у Статистичком оквиру (UNODC, UN WOMEN, 2024: 10; UNODC, UN WOMAN, CEGS, 2022: 11, 12).

Истраживање спроведено у 12 градова у САД од 1994. до 2000. године показало је да је интимно-партнерски фемцид најчешћа врста фемцида, и чини између 40% и 50% фемцида у САД. Лишењу живота жена од стране мушкараца као примарни фактори ризика претходе физичко насиље, доступност ватреног оружја и претња употребе ватреног оружја и убиством. Незапосленост учиниоца и коришћење опојних дрога такође су чести фактори ризика који претходе овој врсти фемцида, док факултетско образовање учиниоца и физичка одвојеност жртве од партнера смањују ризик од фемцида (Campbell, 2008, 58, 59). Истраживање спроведено у Великој Британији на подручју Енглеске, Шкотске и Велса показало је да интимно-партнерском фемциду претходе снажна емотивна веза између партнера, напуштање партнера од стране жртве и раздвојеност у време чињења убиства, посесивност и изражена контрола жртве. У многим случајевима утврђено је да је дошло до вршење сексуалног насиља током убиства (Dobash, Dobash, 2008, 69–71). Актуелни Нацрт Закона о изменама и допунама КЗ Србије предвиђа поштравање казне и за силовање и увођења могућности изрицања доживотног затвора за ово кривично дело (Министарство правде, 2025). Резултати једног истраживања спроведеног у пет држава насталих распадом СФРЈ за период од 2014. до 2024. године (истраживање није обухватило Црну Гору) показало је да је стопа фемцида највиша у Србији, а најнижа у Хрватској (Врућинић, 2025: 321).

Предмет и циљ истраживања

Предмет спроведеног истраживања јесте анализа практичног поступања надлежних органа (полиције, јавног тужилаштва и суда) у превенцији фемцида у интимно-партнерским односима и заштити жена жртава насиља у породици у Србији. Циљ истраживања је утврђивање да ли су проактиван начин поступања полиције и примена *pre-crime* концепта довели до смањења броја жена које су лишене живота од стране партнера и боље координације надлежних органа у превенцији интимно-партнерског фемцида. Резултати истраживања треба да нам дају одговоре на питања: Који су најчешћи начини извршења убистава жена при интимно-партнерском насиљу? Која су средства извршења коришћена? Да ли је насиље у породици претходно пријављивано полицији? Колико ученилаца убистава је извршило самоубиство?

Методe и хипотетички оквир

Истраживање је засновано на примени нормативне и статистичке методе, анализе садржаја и компаративне и формално-логичке анализе. Резултати добијени истраживањем обрађени су статистички, уз одговарајући избор статистичких метода.

У раду су применом методе анализе садржаја анализирани законски прописи који се односе на насиље у породици и кривична дела против живота, а применом статистичке методе обрађени су подаци Министарства унутрашњих послова Републике Србије (МУП-а) који се односе се на интимно-партнерски фемцид за период 2018–2024. године. Анализирани су и списи правосудних органа који се односе на седам случајева у којима је дошло до убистава жене од стране интимног партнера, а претходно је пријављивано насиље и као мере заштите жртве изрицане су хитне мере.

Главна хипотеза од које аутор полази јесте да је примена Закона о спречавању насиља у породици и *pre-crime* концепта довела до повећања ефикасности и ефективности надлежних органа и

елиминисања главних узрока који доводе до најтежих случајева насиља у породици – оних који су праћени лишењем живота жртава насиља од стране интимног партнера.

Просторни и временски рок истраживања и опис узорка

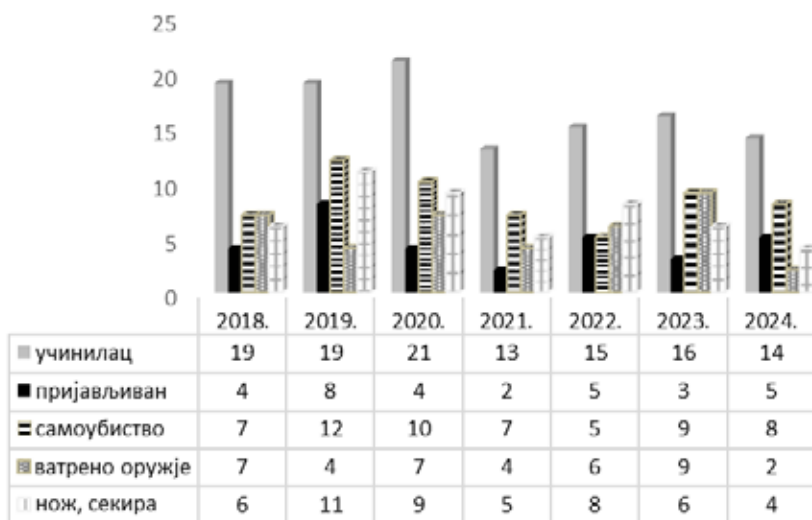
Временски оквир спроведеног истраживања био је период од 2018. до 2024. године, а просторни територија Републике Србије. Узорак су чинили сви евидентирани догађаји у којима је дошло до чињења интимно-партнерског фемицида. Узорак обухвата податке о: полу и старости учиниоца и жртава, средствима извршења, да ли је насиље у породици пријављивано у ранијем периоду, да ли су учиниоцу изрицане хитне мере, да ли је учинилац након убиства извршио самоубиство.

Резултати истраживања и дискусија

Циљ примене pre-crime концепта у борби против насиља у породици јесте пре свега смањење наступања најтежих последица и обезбеђење поштовања права човека на живот, јер је оно универзално признато као највише људско право које је изнад сваког другог права (Марковић, Коларић, 2023: 54). Закон о спречавању насиља у породици (ЗСНП) као резултат ратификовања Истанбулске конвенције усвојен је у новембру 2016. године са одложеном применом од 1. 6. 2017. године. У том периоду, од доношења до примене закона, у организацији Правосудне академије и Криминалистичко-полицијског универзитета спроведен је први циклус обуке полицијских службеника, јавних тужилаца и судија с циљем оспособљавања за примену закона. Пред надлежне органе су стављени задаци који су подразумевали подизање нивоа ефикасности и бољу заштиту жртава насиља у породици. Полиција је добила надлежност и обавезу да предузима конкретне мере превенције одмах по добијању првог сазнања да до насиља у породици може доћи, или да је оно већ учињено. У првих шест месеци при-

мене закона полиција је изрекла 11.533 хитне мере, а суд је продужио 87% (Коларић, Марковић, 2018: 57). Предузимањем благовремених мера требало је отклонити услове и узроке који могу довести до наступања најтежих последица по жртву. Координирано мултисекторско поступање надлежних органа и установа, преточено у рад група за координацију и сарадњу (ГКС) које су основане на подручју сваког основног јавног тужилаштва (укупно 63) и доношење конкретних мера заштите у плановима индивидуалне заштите жртве, имало је за циљ повећање безбедности жртава насиља у породици. Пре примене ЗСНП, у периоду од 2011. до 2016. године, при вршењу интимно-партнерског насиља убијено је 238 жена (Николић-Ристановић, Константиновић-Вилић, 2018: 120), па је требало предузети делотворне мере да се такве последице насиља у породици избегну. Одредбе ЗСНП дале су добру основу за подизање ефикасности и ефективности полиције и других надлежних органа.

На основу доступних података од почетка примене ЗСНП па до 2024. године може се закључити да је примена ЗСНП дала очекиване резултате. О томе сведоче подаци садржани у следећем графикону.



Графикон 1. Учиниоци мушкој пола и средство извршења убиства интимне партнерке у периоду 2018–2024. године

У анализираном седмогодишњем периоду у Србији је од стране интимних партнера лишено живота укупно 117 жена, што је за 50% мање у односу на шестогодишњи период од 2011. до 2016. године. Ово значајно смањење можемо приписати повећању ефикасности надлежних органа од почетка примене ЗСНП. Додатно охрабрују подаци да је у последње четири године од стране интимних партнера убијено мање жена него у три године које су им претходиле, што указује да тренд смањења убистава жена има континуитет. Наиме, од 2018. до 2020. године живота је лишено 59 жена, а од 2021. до 2024. године 58.

Забрињавајуће делује податак да је 31 (или 26,5%) мушки учинилац у периоду који је претходио убиству пријављиван за насиље у породици од стране своје интимне партнерке или трећих лица. То показује да надлежни органи нису предузели адекватне мере заштите жртава. На пример, од укупно 14 убистава у 2024. години, пет (или 36%) жртава је учиниоца претходно пријављивало за насиље у породици. У тој години полиција је евидентирала 33 догађаја у којима је дошло до убиства члана породице од стране другог члана. Само у ових пет случајева учиниоци су претходно евидентирани као могући учиниоци насиља у породици, док се у преосталих 28 случајева убистава чланова породице од стране сродника или интимне партнерке жртве претходно нису обраћале за помоћ надлежним институцијама. То нам показује да се жене жртве интимно-партнерског насиља чешће одлучују да пријаве учиниоце и да се обрате за помоћ због изложености насиљу у породици.

Подаци показују да у многим случајевима жртве не добијају делотворну заштиту. Главни циљ постојања ГКС јесте обезбеђивање заштите жртвама насиља у породици. Тамна бројка криминалитета се повећава најчешће због тога што жртве немају поверења у надлежне органе. Не верују да ће они предузети делотворне мере с циљем санкционисања учиниоца, превенције насиља и њихове заштите након обраћања за помоћ. Резултати једног истраживања за период 2018–2023. показују нам да се у Србији годишње евидентира просечно око 28.600 догађаја са елементима насиља у породици, око 30.000 могућих учинилаца и око 32.600 жр-

тава (Марковић, 2024: 214). Поставља се питање да ли, ако је само четвртина жртва лишених живота од стране интимних партнера претходно пријавила учиниоца за насиље у породици, то значи да се таква тамна бројка може преликати и на укупну бројку непријављених догађаја са обележјима насиља у породици. То би значило да се у Србији годишње просечно изврши између 75.000 и 100.000 догађаја са обележјима насиља у породици. Примаран циљ надлежних органа након добијања сазнања да је насиље у породици учињено, односно, након добијања сазнања да прети опасност да насиље буде извршено у непосредној будућности, треба да буде потпуна заштита безбедности жртве. То подразумева хитну реакцију полиције, центара за социјални рад (ЦСР) и правосудних органа и предузимање адекватних мера које ће омогућити делотворну заштиту жртве и неутралисање ризика од свих облика насиља који могу угрозити њену безбедност.

Како бисмо утврдили због чега мере које надлежни органи предузимају након добијања сазнања о учињеном насиљу у породици у одређеном броју случајева нису делотворне и из којих разлога у одређеном броју случајева долази до наступања најтежих последица по жртву која се обратила надлежним органима за помоћ, заштиту и подршку, анализирали смо седам предмета изабраних по методи случајног узорка од укупно 31 евидентираног у којем су жене лишене живота од интимних партнера, а претходно су пријавиле насиље у породици.³

Први предмет који смо анализирали је из Вишег суда у Брању (пресуда К26/22 од 10. 3. 2023). Учиницац је осуђен на казну доживотног затвора због тешког убиства⁴ и насиља у породици⁵ јер је 23. марта 2022. године у алкохолисаном стању, у присуству своје две ћерке, употребом ножа нанео тешке телесне повреде својој супрузи, након чега је она наредног дана преминула у здравственој

³ На основу захтева за приступ информацијама од јавног значаја добијени су списи предмета од стране суда и јавног тужилаштва. Четири предмета се односе на убиства учињена 2019, а по један на убиства из 2021, 2022 и 2023. године.

⁴ Кривични законик, члан 110, став 1, тач. 10.

⁵ Кривични законик, члан 194, став 3, у вези са ст. 2 и 1 и чланом 194, став 2.

установи, а малолетној ћерки, која је са сестром покушавала да га спречи у извршењу дела, нанео је тешке телесне повреде у виду прелома ручне кости петог малог прста шаке са дислокацијом и отоком. Из пресуде се може закључити да је насиље у породици постојало све време трајања брака. По изјавама деце, учинилац је тукао жртву (своју супругу а њихову мајку) од њиховог раног детињства, а ћерки је жртвина мајка причала да је отац тукао мајку и пре брака, у време док су се забављали. Учинилац је конзумирао алкохолна пића у већим количинама, а у алкохолисаном стању био је агресиван и насилан. Континуирано је вршио физичко и психичко насиље над својом супругом и ћеркама. Супруга га није пријављивала због насиља, али старија ћерка и његови родитељи (отац и мајка) јесу. Тако је 20. јуна 2021. године у породичној кући вређао супругу и задао јој више удараца у пределу главе, а вређао је и претио својој мајци која је са оцем становала на првом спрату исте куће. Наређењем надлежног полицијског службеника (НПС) истог дана изречене су му обе хитне мере. Суд их је на предлог јавног тужилаштва продужио. Учинилац је хитне мере прекршио тако што је 17. јула 2021. године путем телефона назвао своју супругу, вређао је и претио јој убиством.

Основни суд у Врању, по тужби центра за социјални рад, изрекао му је породично-правне мере заштите (решење П2. бр. 173/21 од 6. 10. 2021. и 10. 12. 2021), и то: забрану приближавања супрузи, ћеркама, сину и родитељима на удаљеност од сто метара, забрану приступа у простор око места становања и места рада члана породице, односно образовне установе у којој деца похађају наставу на удаљеност од сто метара, забрану даљег узнемиравања и издавања налога за исељење из породичне куће. Требало је да мере заштите трају шест месеци. У време трајања породично-правних мера заштите, учинилац је учинио ново физичко насиље према жртви 28. децембра 2021. године. Полиција је изрекла хитне мере наредног дана, а суд их је продужио. Изречене хитне мере учинилац је прекршио истог дана када су му изречене, због чега је осуђен на казну затвора од осам дана (Прекршајни суд у Врању, 6Пр. бр. 6306/21 од 30. 12. 2021).

Учишилац је осуђен за кривично дело „насиље у породици” које је учинио 20. јуна 2021. године према супрузи, али тек седам месеци након што је жртва лишена живота. Оптужни предлог је поднет 12. априла 2022. године, 19 дана након што је учинилац убио своју супругу над којом је претходно вршио насиље (Основни суд у Врању, К. бр. 97/22 од 20. 10. 2022). Истом пресудом осуђен је и зато што је 28. децембра 2021. године прекршио мере породично-правне заштите доласком у породичну кућу за време њиховог трајања, а и зато што је наредног дана, 29. децембра 2021. године, гурао и ударио супругу, вређао мајку и старијој ћерки претио убиством. Овом пресудом, у време док се налазио у притвору због постојања основане сумње да је учинио кривично дело тешког убиства, изречена му је јединствена казна затвора од 15 месеци и новчана казна од 40.000 динара. Евидентно прекасно. Списи предмета показују да је ГКС 16. августа 2021. године на унапред припремљеном обрасцу израдила план заштите и подршке жртве (супруге), којим су наложене следеће мере: за ОЈТ Врање – саслушање осумњиченог, испитивање оштећене и психијатријско вештачење осумњиченог; за ЦСР Врање – оснаживање жртве да сведочи; за Полицијску управу Врање – поступање по захтевима ОЈТ и ЦСР. Закључујемо да наложене мере нису биле довољне и адекватне, а да надлежни органи нису предузели делотворне мере с циљем заштите безбедности жртве.

Други случај убиства који ћемо приказати десио се у Ваљеву (вид. Марковић, 2024а: 386–390). Учишилац је 17. маја 2021. године лиши живота бившу интимну партнерку. Она га је претходно, у периоду од око годину и по дана, више пута пријављивала због физичког насиља, прогањања, малтретирања и претњи убиством и самоубиством. Два пута му је изрицана и продужавана хитна мера забране приласка и контактирања жртве и два пута је хапшен; једна кривична пријава је одбачена применом института опортунитета, а на основу друге су му изречене условна осуда и мера безбедности забране приласка оштећеној на удаљеност од сто метара (ОЈТ у Ваљеву, ПИ бр. 28/23 од 20. 7. 2023). ГКС је проценила висок ризик од понављања насиља „и донета је одлука да полиција учестало надзире кретање жртве с циљем њене заштите, као и да доставља извештај

ГКС на сваких седам дана” (Марковић, 2024а: 388). Два месеца након доношења ове одлуке жртва насиља је убијена испред улаза зграде где је становала, у раним јутарњим сатима, када је кретала на посао, а учинилац је недалеко одатле извршио самоубиство (ВЈТ у Ваљеву, ПИ бр. 16/23 од 21. 7. 2023). Закључујемо да надлежни органи нису заштитили жртву која им се безуспешно више пута обраћала за помоћ.

Трећи и четврти случај односе се на убиства у Новом Саду. Прво убиство је извршено 24. маја 2019. године, 14 дана након што је жртва пријавила полицији насиље у породици. Учиниоца је извршио троструко убиство у време тајања хитних мера. Мере су му изречене и продужене након учињеног физичког и психичког насиља према супрузи. Жртва је приликом пријаве насиља у породици обавестила полицију да јој је супруг упутио квалификовану претњу – да ће је лишити живота ако пријави насиље полицији. Убиство је извршено у породичној кући родитеља жртве, у којој је она боравила након напуштања супруга, са двоје малолетне деце. Учиниоца је лишио живота таста, ташту и супругу. Малолетна деца су била присутна у кући за време извршења тешког убиства. Без обзира што је жртва пријавила полицији да јој је супруг упутио озбиљне претње да ће је убити, он није ухапшен, а по налогу јавног тужиоца против учиниоца поднета је кривична пријава у редовној процедури. На овом месту подсетићемо на одредбе чланова 211 и 291 Законика о кривичном поступку.⁶

Група за координацију и сарадњу није поступала у овом случају. У допису ОЈТ у Новом Саду наведено је да ГКС поступа два пута месечно, а да околности случаја пријављеног 10. 5. 2019. године нису биле такве природе да је постојао разлог за ванредни састанак (ОЈТ у Новом Саду, ПИ 57/23 од 26. 7. 2023). Неколико дана након извршеног тешког убиства учинилац је ухапшен, а у при-

⁶ Између осталог, „притвор се може одредити против лица за које постоји основана сумња да је учинило кривично дело ако особите околности указују да ће у кратком временском периоду поновити кривично дело или довршити покушано кривично дело или учинити кривично дело којим прети”, а „полиција може неко лице ухапсити ако постоји разлог за одређивање притвора”.

твору за време трајања кривичног поступка извршио је самоубиство (Коларић, Марковић, 2024: 556). Друго убиство учињено је 10. маја 2023. године, за време трајања хитних мера, које су биле изречене и продужене, а 15 дана након што је жртва пријавила да јој је интимни партнер претио убиством и самоубиством када му је саопштила да жели да раскине интимно-партнерски однос са њим. Убиство је извршено тако што је учинилац у поподневним сатима дошао до козметичког салона који је био у власништву жртве и у којем се она налазила, насилно ушао у њега и употребом ватреног оружја извршио убиство и самоубиство. На месту догађаја пронађена су два пиштоља која је учинилац узео из продавнице оружја у којој је био запослен. Без обзира на околност да је могући учинилац запослен у продавници оружја и да је жртва изјавила да јој је претио убиством и самоубиством, у обрасцу процене ризика коју је 25. априла 2023. године сачинио НПС, а која се налази у списима судског предмета, за фактор ризика под редним бројем 5 „постоји сумња да поседује оружје у илегалном поседу или да му оружје може бити доступно” наведено је „НЕ” (Основни суд у Новом Саду, Решење НП 418/23 од 25. 4. 2023). ГКС није разматрала овај случај⁷ (ОЈТ у Новом Саду, ПИ 57/23 од 26. 7. 2023).

Пети и шести случај односе се на убиства на подручју Полицијске управе у Ужицу 2019. године. Прво је извршено 2. априла у Ужицу. Мушкарац стар 57 година убодима ножем у пределу леве поткључне артерије лишио је живота пет година млађу бившу супругу, након чега је извршио самоубиство вешањем. Жртва је пријавила супруга за насиље у породици 19. фебруара исте године и поднела кривичну пријаву за насиље у породици. Учиниоца јој је претио самоубиством и тешким последицама по њу јер је покренула поступак за развод брака, који је након тога окончан почетком марта. НПС је изрекао хитне мере и оне су продужене. Од учиниоца је одузета ловачка пушка коју је имао у легалном поседу. ГКС је разматрала овај случај на састанцима три пута, и то 28.

⁷ У допису ОЈТ у Новом Саду који је добијен по захтеву за слободан приступ информацијама од јавног значаја наведен је разлог због којег предмет није разматран – „састанци ГКС одржавају се два пута месечно тако да се убиство десило пре заказивања истог”.

фебруара, 14. марта и 27. марта. У свим извештајима је констатовано да ризик од насиља у породици постоји. Индивидуални план заштите жртве је био израђен, међутим, конкретне мере заштите безбедности жртве нису одређене. На последњем састанку који је одржан пре убиства жртве наводи се да су све мере које се односе на поступања полиције и јавног тужилаштва извршене, а да ЦСР није доставио извештај по захтеву ОЈТ. ГКС је предмет архивирала 11. априла, девет дана након учињеног убиства и самоубиства. Други случај се десио у Чајетини, 13. новембра 2019. године. Учинио је лишио живота супругу употребом кухињског ножа. У извештају ГКС од 4. јула 2019. године, када је овај случај први пут разматран, наведено је да је 26. јуна 2019. године НН лице пријавило насиље у наведеној породици – да супруг вербално вређа своју супругу. Жртва је полицији саопштила да дужи период трпи насиље у породици од свог супруга и да јој је он више пута претио убиством. Полиција је учиниоца превезла до здравствене установе где је задржан на психијатријском лечењу. Процењено је да постоји ризик од насиља у породици, а након изласка из психијатријске болнице супругу жртве су изречене и продужене обе хитне мере (5. јула). ГКС се састајала четири пута по овом случају и то 4. јула, 18. јула и 1. августа, док је 15. августа, након добијања сазнања да је кривична пријава одбачена 6. августа 2019. године, донета одлука да се предмет архивира. Пријава је одбачена јер је осумњичени негирао насиље, а жртва ускратила своје сведочење. Из оптужнице Вишег јавног тужилаштва види се да је учинилац више година вршио физичко насиље над својом супругом, а наводе се и лични подаци НН лица које је пријавило насиље 26. јуна. Ради се о колеги са посла жртве који је изјавио „да је у последњих 7–8 година лично видео, сигурно педесет пута оштећену сву у модрицама, убијену од батина, да зна да је трпела насиље мужа, да је пре две-три године телефонским путем и сам пријављивао Полицијској станици у Чајетини насиље у породици над оштећеном, као и да је у лето 2019. године оштећена пребијена од стране свог супруга и да је тражила од њега да догађај пријави полицији, што је и урадио. Да је том приликом видео оштећену која је била сва у модрицама жуте боје по телу, леђима и по лицу” (ВЈТ Ужице, КТО број 10/20 од 14. 4. 2020).

Седми случај се односи на убиство у Панчеву које је учињено 12. 7. 2019. године. Мушкарац стар 64 године на јавном месту лишио је живота бившу супругу стару 60 година, тако што јој је нанео више убода ножем, у пределу врата, грудног и трбушног дела тела. Осуђен је на казну затвора од тридесет година (Виши суд у Панчеву, Пресуда 48/19 од 12. 5. 2020). Он је вршио насиље према жртви од почетка трајања брака. Наносио јој је телесне повреде, вређао је и претио убиством више од четрдесет година. Жртва се иселила из породичне куће у фебруару 2019. године и покренула бракоразводни поступак, а од краја јуна била је смештена у сигурну кућу јер је страховала за свој живот. Након што је пријавила насиље у породици, учиниоцу је 25. јуна 2019. изречена хитна мера привремене забране контакта и приласка жртви, а суд ју је продужио. Након судског рочишта у поступку развода брака 27. јуна 2019. године, за време трајања хитне мере, учинилац је дошао до врата сигурне куће, изјавио да има сазнања да је унутра његова жена и тражио је да је види. Радница сигурне куће му то није дозволила. О догађају је обавештена полиција, али није поднета пријава за прекршај кршења хитних мера⁸. ГКС је разматрала случај 28. јуна 2019. године, донет је индивидуални план заштите жртве, процењен је средњи ниво ризика од насиља у породици, а полицији је наложено чешће обилажење жртве за време трајања хитне мере с циљем провере да ли се мере заштите спроводе (ОЈТ у Панчеву, ПИ 6/23 од 17. 7. 2023). На основу исхода случаја можемо закључити да надлежни органи нису спровели адекватне и делотворне мере заштите жртве.

На основу приказаних случајева можемо закључити да постоје одређени пропусти и неправилности у поступању надлежних органа и установа које предузимају мере с циљем спречавања насиља у породици и заштите безбедности жртава. Полиција је у свим случајевима проценила ризик од насиља у породици и изрекла хитне мере које је суд продужио. У једном случају, по тужби ЦСР

⁸ У допису ОЈТ у Панчеву ПИ бр. 6/23 од 17. 7. 2023. наведено је да је по мишљењу јавног тужилаштва том приликом дошло до кршења хитних мера и да је полиција била у обавези да о томе обавести прекршајни суд.

одређене су и породично-правне мере заштите. Против учинилаца су благовремено подношене кривичне пријаве јавном тужилаштву. Међутим, у пет анализираних предмета осумњичени за насиље у породици нису ухапшени без обзира на то што су жртви претили убиством (случајеву у Новом Саду, Панчеву, Врању и Ужицу), а у Ваљеву је учинилац ухапшен, али му суд није одредио притвор. Европска конвенција за заштиту људских права и основних слобода не предвиђа експлицитно право на заштиту од насиља у породици, али Европски суд за људска права у својим одлукама наводи, када је реч о кршењу права на живот, односно члана 2 Конвенције: немогућност државе да ефикасно спречи насиље засновано на полу представља облик дискриминације жена (видети: Бранко Томашић и други против Хрватске); држава својом неактивношћу, потцењујући озбиљност насиља, у суштини одобрава насиље (видети: Талпис против Италије); постоји позитивна обавеза државе да предузме превентивне оперативне мере ради заштите појединца чији је живот угрожен кривичним делом другог појединца (видети: Осман против Велике Британије, став 115; Опуз против Турске, став 128) (Марковић, Коларић, 2024: 227–229).

У већини случајева жртва је желела да напусти учиниоца, а учинилац јој је упућивао претње убиством непосредно пре његовог извршења. У три случаја учинилац је извршио убиство за време трајања хитних мера, у једном случају и за време трајања мера породично-правне заштите, а у једном за време трајања мере безбедности забране приближавања и комуникације са оштећеним. Закључујемо да хитне мере и друге мере заштите саме по себи нису довољне да спрече насиље и заштите жртву. У неколико случајева убиство је учињено пре него што је случај разматран на састанку ГКС, а хитне мере су донете. Разлог који се наводи јесте да ГКС није стигла да разматра случај јер се по одредбама ЗСНП састанак групе заказује на 15 дана. Мада резултати једног истраживања показују да се та законска одредба поштује и да ГКС заказује састанке у том року (Чворовић, Оташевић, Вранешевић, 2021: 1147), сматрамо да је нужно да надлежни полицијски службеник након изрицања хитних мера ургентно иницира састанак ГКС у свим случајевима

у којима процени да могу наступити тешке последице по жртву. Затим, приликом доношења индивидуалног плана заштите жртве ГКС треба да одреди конкретне мере заштите, које ће у неким случајевима обухватити и физичку заштиту жртве и места где жртва борави. Залажемо се и за увођење мера електронског надзора у наш правни систем. Мере би се примењивале као начин заштите жртве када ГКС процени висок ризик од насиља у породици, а за кршење мере, *de lege ferenda* требало би предвидети затворску казну (Марковић, 2024а: 395–396).

У три случаја насиље је трајало више година, односно од почетка интимно-партнерског односа, а у пет од седам случајева учинилац је извршио самоубиство. Графикон 1 нам показује и да је чак 58 или 50% учинилаца убиства покушало или извршило самоубиство. За разлику од истраживања спроведеног у Црној Гори у периоду 2001–2010, којим је утврђено да сваки десети фемицид прати самоубиство учиниоца (Пижурица, Шоћ, Абрамовић, 2013: 12), резултати нашег истраживања потврђују резултате многих других истраживања која показују да је интимно-партнерски фемицид доста чешће праћен самоубиством учиниоца (Павлов, Лацмановић, 2023: 11).

У два од седам анализираних случајева убиство је учињено употребом ватреног оружја, а у осталих пет употребом оштрог предмета, најчешће ножа. Графикон 1 нам показује да је укупно 39 или 33% жена лишено живота употребом ватреног оружја, а 49 или 42% употребом ножа, секире или другог оштрог предмета. Можемо закључити да мушкарци за убиство своје интимне партнерке најчешће користе оштар предмет или ватрено оружје. Ако узмемо у обзир чињеницу да ватрено оружје (у легалном или илегалном власништву) није доступно сваком учиниоцу, можемо са сигурношћу изнети претпоставку да убица најчешће користи ватрено оружје, ако му је оно доступно, а оштар предмет ако му оно није доступно.

Закључак

Фемицид је превасходно криминолошки а не кривично-правни појам. У Србији је интимно-партнерски фемицид након доношења Закона о спречавању насиља у породици у значајном паду. Мада је број жена лишених живота од стране њихових интимних партнера смањен, сматрамо да је он и даље висок. У раду смо приказали резултате истраживања који показују да се мултисекторска сарадња надлежних органа за спречавање насиља у породици, а самим тим и насиља према женама од стране њихових интимних партнера, може значајно унапредити. Ту првенствено мислимо на поступање ГКС, која треба да предузме делотворне мере заштите жртава. Индивидуални план заштите жртве треба да садржи конкретне мере заштите, начин њиховог спровођења, рокове и начин праћења. На крају се морају извршити евалуација и анализа учинка сваке надлежне институције у спровођењу наложених мера. ГКС не сме примењивати формалистички приступ приликом предузимања заштите жртве, већ у сваком конкретном случају треба да изабере најбоље, адекватне мере заштите, ако је могуће уз укључивање саме жртве у изради индивидуалног плана заштите. Сваки случај има одређене специфичности на основу којих се мора усмерити поступање надлежних органа. Дугорочни циљ треба да подразумева одсуство жртава лишених живота од стране интимних партнера у оним случајевима када су се обратиле за помоћ надлежним органима. На тај начин ће се многобројне жртве насиља у породици, које трпе насиље а нису га пријавиле због неповерења у институције, охрабрити да се обрате надлежним органима за помоћ. Неопходно је смањити високу тамну бројку у овој области како би се смањио укупан број жртава изложених тешким последицама насиља у породици. Сматрамо да је Србија на добром путу да постигне тај циљ, али је неопходно предузети још низ мера које, између осталог, обухватају већу специјализацију и бољу обученост особља у институцијама надлежним за супротстављање насиљу у породици и заштиту жртава.

Литература

1. Батричевић, А. (2016). Кривичноправна реакција на фемицид, *Темуга*, 19 (3–4): 431–451. DOI: 10.2298/ТЕМ1604431В
2. Врућинић, Ж. (2025). (Не)видљиве жртве фемицида у Босни и Херцеговини, Србији, Словенији, Северној Македонији и Хрватској (2014–2024) – с посебним освртом на Босну и Херцеговину, У Зборнику радова: Жене у модерном друштву: изазови и могућности, Бања Лука, стр. 314–325. DOI:10.7251/ZCMZ0125314V
3. Dobash, R. E., Dobash, R. P. (2008). *Murder in Britain Study: The Murder of Women, Strengthening Understanding of Femicide*, Washington, pp. 66–72.
4. Коларић, Д. (2015). *Кривична дела убиства – de lege lata i de lege ferenda*, НБП, 20(2): 145–165.
5. Коларић, Д., Марковић, С. (2024). Убиства при извршењу насиља у породици у Републици Србији – узроци и појавни облици, *Социолошки ирепед*, 58(2): 548–572. <https://dx.doi.org/10.5937%2Fsocpreg58-49145>
6. Коларић, Д. Марковић, С. (2018). Поједине недоумице у примени Закона о спречавању насиља у породици, *Анали Правној факултету у Београду*, 66(1): 45–71. DOI: 10.5937/AnaliPFB1801045K
7. Лубура, М. (2017). Појам фемицида и значај његовог правног регулисања, *Страни правни живот*, 61(3): 115–130. DOI: <https://doi.org/10.56461/spz17308L>
8. Марковић, С. (2024). Анализа практичне примене Закона о спречавању насиља у породици од стране надлежних органа Републике Србије, *Баштина, Приштина – Лепосавић*, св. 63: 209–224. DOI: <https://doi.org/10.5937/bastina34-51714>
9. Марковић, С. (2024а). Убиства у контексту интимног партнерског насиља у Србији: Појавни облици и заштита жртава, *Темуга*, 27(3): 375–400. DOI: <https://doi.org/10.2298/ТЕМ2403375М>

10. Marković, S. Dostić, S. (2025). The role of the police and the public prosecutor's office in the prevention of domestic violence in Serbia, *SCIENCE IJ Journal*, Vol. 4(2): 59–66. DOI: <https://doi.org/10.35120/sciencej0402059m>
11. Marković, S. Kolarić, D. (2024). Possibilities and limitations of preventive measures as a form of combating the most severe forms of domestic violence, *Теме*, 48(1): 223–241. doi.org/10.22190/ТЕМЕ230707012М
12. Marković, S. Kolarić, D. (2023). Some effects of 'pre-crime' concept in combating domestic violence, *Наука, безбедност, полиција*, 28(1): 40–57. DOI: 10.5937/nabepo28-42953
13. Николић-Ристановић, В., Константиновић-Вилић, С. (2018). *Криминологија*. Београд, Прометеј.
14. Павлов, Т., Лацмановић В. (2023). *Карактеристике и превенција случајева феминицида-суицида починених вајреним оружјем у интимном партнерском односу*. Истраживачки извештај. Београд: Програм Уједињених нација за развој.
15. Pižurica A. Šoć, M. Abramović, M. (2013). Sudskomedicinske karakteristike ubistava žena u Crnoj Gori u XXI vijeku, *Medical Journal of Montenegro*, 1(2): 1–12, DOI: <https://doi.org/10.5937/cma1-2856>
16. Russell, D. (2008). Femicide: Politicizing the Killing of Females, *Strengthening Understanding of Femicide*, Washington, pp. 26–31.
17. Campbell, J. (2008). Risk Factors for Femicide and Femicide-Suicide: A Multisite Case Control Study, *Strengthening Understanding of Femicide*, Washington, pp. 57–65.
18. Чворовић, Д. С., Оташевић, Б. Б., Вранешевић, М. М. (2021). Мултисекторска сарадња у случајевима насиља у породици из угла центра за социјални рад. *Социолошки преглед*, бр. 55(3): 1138–1164. DOI: 10.5937/socpreg55-32012

Правосудна пракса

1. Виши суд у Врању, Пресуда К26/22 од 10. 3. 2023.
2. Виши суд у Панчеву, Пресуда 48/19 од 12. 5. 2020.
3. Више јавно тужилаштво у Ваљево, Одговор на захтев за приступ информацијама од јавног значаја, ПИ бр. 16/23 од 21. 7. 2023.
4. Више јавно тужилаштво у Ужицу, Одговор на захтев за приступ информацијама од јавног значаја, ПИ бр. 7/23 од 21. 7. 2023.
5. Више јавно тужилаштво у Ужицу, Оптужница, КТО број 10/20 од 14. априла 2020.
6. Основни суд у Новом Саду, Решење, НП бр. 418/23 од 25. 4. 2023.
7. Основни суд у Врању, Пресуда, К. бр. 97/22 од 20. 10. 2022.
8. Основни суд у Врању, Решење, П2. бр. 173/21 од 6. 10. 2021. и 10. 12. 2021.
9. Основно јавно тужилаштво у Ваљево, Одговор на захтев за приступ информацијама од јавног значаја, ПИ бр. 28/23 од 20. 7. 2023.
10. Основно јавно тужилаштво у Панчеву, Одговор на захтев за приступ информацијама од јавног значаја, ПИ бр. 6/23 од 17. 7. 2023.
11. Основно јавно тужилаштво у Новом Саду, Одговор на захтев за приступ информацијама од јавног значаја, ПИ бр. 57/23 од 26. 7. 2023.
12. Основно јавно тужилаштво у Ужицу, Одговор на захтев за приступ информацијама од јавног значаја, ПИ бр. 6/23 од 26. 7. 2023.
13. Case of Talpis v. Italy (app. no. 41237/14), Judgment of 21. March 2017.
14. Case of Opuz v. Turkey (app. no. 33401/02), Judgment of 9 June 2009.
15. Case of Branko Tomašić and Others v. Croatia (app. no. 46598/06) Judgment of 15 January 2009.
16. Case of Osman v. The United Kingdom (app. no. 87/1997/871/1083), 28 October 1998.

Општи правни акти

1. *Законои за изменување и дојолнување на Кривичниот законик*, Указ за прогласување на Законот за изменување и дополнување на Кривичниот законик број 08 – 789/1 13 февруари 2023. година, Скопје.
2. *Законик о кривичном постојуку*, Службени гласник Републике Србије, бр. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014, 35/2019, 27/2021 (Одлука Уставног суда), 62/2021 (Одлука Уставног суда).
3. *Закон о сиречавању насиља у породици*, Службени гласник РС, бр. 94 од 24. новембра 2016, 10 од 9. фебруара 2023 – др. закон.
4. *Конвенција о сиречавању и борби против насиља над женама и насиља у породици (Истанбулска конвенција)*, Савет Европе, Истанбул, 11. 5. 2011.
5. *Кривични законик*, Службени гласник Републике Србије, бр. 85/2005, 88/2005, 107/2005, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016, 35/2019, 94/2024.
6. *Казнени закон*, Народне новине РХ, бр. 125/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/19, 84/21, 114/22, 114/23, 36/24.
7. *Council of Europe Convention on preventing and combating violence against women and domestic violence*, 11 May 2011, in Istanbul. *Закон о потврђивању Конвенције Савета Европе о спречавању и борби против насиља над женама и насиља у породици*, Службени гласник РС – Меѓународни уговори, бр. 12/2013, 4/2014.
8. *Convention for the Protection of Human Rights and Fundamental Freedoms*, Rome, 4.XI.1950, *Закон о ратификацији Европске конвенције за заштиту људских права и основних слобода*, Службени лист СГ – Меѓународни уговори, бр. 9/2003, 5/2005, 7/2005 (исправка), Службени гласник РС – Меѓународни уговори, бр. 12/2010, 10/2015.

Остали материјали

1. Министарство правде (2025) Нацрт Закона о изменама и допунама КЗ, <https://www.mpravde.gov.rs/sr/obavestenje/14262/javna-rasprava-o-nacrtu-zakona-o-izmenama-i-dopunama-krivicnog-zakonika-.php>, доступан 19. 9. 2025.
2. Министарство унутрашњих послова (2025) Допис са статистичким подацима Одељења за статистичку аналитику и ОКЕ, бр. 141/1, од 10. 2. 2025. и број 1810/23 од 8. 2. 2024.
3. UNODC, UN WOMEN (2024) Femicides in 2023: Global Estimates of Intimate Partner/Family Member Femicides, United Nations publication.
4. UNODC, UN WOMAN, CEGS (2022) Statistical framework for measuring the gender-related killing of women and girls (also referred to as “femicide/feminicide”), Prepared by the United Nations Office on Drugs and Crime and the United Nations Entity for Gender Equality and the Empowerment of Women Endorsed by the United Nations Statistical Commission at its 53rd Session on 28th February-2nd March and 4th March 2022.

Prevention of Intimate Partner Femicide in the Republic of Serbia

Abstract: *This paper analyses the effectiveness of measures taken by the competent institutions of the Republic of Serbia to prevent the killing of women by men in the context of intimate partner violence. Femicide is the most severe form of gender-based violence, and the number of women killed by their partners during or after the end of a marital, non-marital, or other intimate relationship is a global social problem affecting most countries. In 2011, the Council of Europe adopted the Istanbul Convention to prevent domestic violence in European countries. Although the Convention addresses the prevention and protection of all victims of domestic violence, its main objective is to prevent gender-based violence against women and ensure their protection. After ratifying the Convention, Serbia adopted a special law in 2016 that elaborated on its provisions and introduced a proactive approach for competent authorities, based on risk assessment and risk management of domestic violence from the moment of first awareness of violence, as well as in cases where there is a risk of future violence, even if it has not occurred previously. The main objectives of the competent authorities' actions can be defined as follows: empowering victims and encouraging them to report violence, which includes increasing the victims' trust in the police and other institutions to reduce the dark figure of crime; protecting the victims from repeated violence and preventing the most severe outcomes, such as bodily harm and loss of life; and addressing the root causes of violence, including restraining orders and no-contact orders against perpetrators. The paper presents the results of a study that covered all recorded cases of intimate partner femicide in Serbia during the seven-year period following the implementation of the Law on Prevention of Domestic Violence, from 2018 to 2024. A random sample of seven cases in which women were killed by their intimate partners was selected and thoroughly analysed. These women had previously reported violence to the police, which resulted in emergency measures taken against the perpetrators. The results showed a significant decline in intimate partner femicide in Serbia after the adoption of the Law on Prevention of Domestic Violence. However, the analysed femicide cases revealed certain shortcomings in the work of competent authorities,*

indicating that multisectoral cooperation in preventing domestic violence—and thus violence against women by intimate partners—can be significantly improved in the future. The author concludes that the functioning of coordination and cooperation groups can be considerably enhanced to better protect victims.

Keywords: *femicide, domestic violence, intimate partner relationship, prevention, victim.*

Zsolt, LIPPAI¹
Béla, ÁRPÁS²
Pál, KARDOS³

DOI: 10.5937/bezbednost2503059L
UDK: 343.123.12(439)
Pregledni naučni rad
Primljen: 7. 10. 2025. godine
Revizija: 13. 10. 2025. godine
Datum prihvatanja: 24. 11. 2025. godine

Private investigation in the Republic of Hungary

Abstract: *In our study, as practicing law enforcement professionals, we examine the historical development, legal regulation and forensic characteristics of private detective activity in Hungary, which is little known by many. We examine the normative regulation of private detective activity, which is difficult to interpret and leaves many questions open, as well as its lack of regulation, with which we wish to contribute to the comprehensive scientific research and mapping of private security. Nowadays, it has become a priority to make a well-founded and responsible choice of which tasks the police will focus its forces on and which they can hand over to the private security sector. As a result, the question arises in which areas it will strengthen their cooperation with the private security sector, thus ensuring the rationalization of state tasks and more efficient and cost-saving organizational operation. In this paper, by analysing the theoretical*

¹ pol. lieutenant colonel, assistant professor, Ludovica University of Public Service, Faculty of Law, Department of Private Security and Municipal Policing, <https://orcid.org/0000-0003-4211-2249>, lippai.zsolt@uni-nke.hu

² pol. lieutenant colonel, master lecturer, Ludovica University of Public Service Faculty of Law, Department of Criminal Intelligence and Economic Protection, <https://orcid.org/0009-0004-5169-613X>, arpas.bela@uni-nke.hu

³ master lecturer, Ludovica University of Public Service, Faculty of Law, Department of Private Security and Municipal Policing, <https://orcid.org/0000-0002-4965-035X>, kardos.pal@uni-nke.hu

and practical background related to private investigation, we try to provide interesting impulses for future researchers interested in the field.

Keywords: *Hungary, private investigation, history, legal regulation, forensics*

On the margins of the blurring borders

Based on the provisions of Article 46 of the Basic Law of Hungary, the basic task of the police is to prevent and detect crimes, protect public safety, public order and the order of the state border. In our country, pivotal laws determine the operation of the police and national security services, and the duties of law enforcement agencies related to public safety.

In order to enforce its powers related to public safety, the state, starting from the fact that public order is a basic value for the rise of the nation, declared that cooperation with the persons (bodies) performing law enforcement duties, regulated by law, is essential for the maintenance of public order and public safety (CXX of 2012 law). Within the framework of this regulation, the legislator provides for armed security guards, personal and property guards (meaning: personal and property guards, private investigators, property protection system designers and installers, property protection system installers), nature conservation guards, members of the forestry authority performing law enforcement duties, the activities of mountain rangers, professional hunters, forestry personnel performing law enforcement duties, state and professional fish rangers, public land inspectors, municipal nature conservation rangers, and field rangers. The state development of the conditions and frameworks of the mentioned activities serves to ensure the constitutional protection of property. The legislator creates the legal framework for the protection of private and public property by using means of personal and property protection.

A few years ago, the European Union published a study volume examining the private security market of the member states (the so-called White Book), in which the possible reasons for the rise of private security included the blurring of the boundaries between public and

private areas, the overburdening of the police and various fiscal reasons (Finzter, 2009; 66-83). The study came to the conclusion that the financial resources cannot be provided to maintain public safety as a full-scale state monopoly (URL1). Based on this, of course, it would be easy to immediately say that a significant part of the performance of law enforcement tasks will be transferred to private security service providers and businesses. However, the overall picture is much more complex than this, given that the boundaries between private and public safety of the already mentioned collective work, and therefore the creation of public safety as a cooperative product, seem to be blurred. This is especially the case in the areas of policing, in which state control is not significantly impaired even if market players are involved in the creation of the public good. A good example of this is personal protection, in which, in addition to maintaining its own exclusivity (protection of particularly important persons), the state recognizes the need for individual security (or the need for it) and enables the provision of the service on a market basis (Nagy & Lukács, 2019; 168–169).

The apparent blurring of borders and the complexity of the phenomenon are exemplified by the fact that there are a number of police functions that the state police reserve for themselves, but at the same time, even in their case, some privatization can be observed in part, but not exclusively; a good example of this is the outsourcing of the safeguarding of state assets to private companies. At the same time, a very interesting issue can be classified here, the relative legal regulation of private detective activity – which is difficult to interpret and leaves many questions open (Mészáros, 2010; 285–294) – or its lack of regulation, one of the basic questions of which is the legality and objectivity of the information-gathering activity carried out in the framework of financial compensation, along with the question of legislative trust, the materially motivated interest of possibly covering up the truth; asking the question whether what is legal is effective, and whether what is effective is legal. In our study, we examine the historical development, legal regulation and forensic characteristics of the private detective activity in Hungary, which is little known by many, and in many cases accompanied by legends, supposed and real stories.

Excerpts from the legal background of the private investigation systems in the United Kingdom, Germany, Austria, Slovakia, Slovenia, and the Czech Republic

Before we move on to analyse private investigation activities in Hungary, we would like to take a look at the legal background of the private investigation systems in a few countries that we consider relevant. This highlights the fact that private investigation operates under different legal frameworks in the Member States of the European Union, reflecting the historical, legal and social characteristics of each country. Below, we present the regulation and institutional background of private investigation in six countries.

In the United Kingdom, private investigation is not subject to a license, but it is subject to strict data protection and ethical standards. Private investigators do not have police powers and must comply with human rights and data protection regulations in their activities (URL2). The activity is primarily regulated by the Data Protection Act and the Regulation of Investigatory Powers Act. It should be emphasized that *"Private investigators cannot tap phones, track people with GPS without permission, or obtain information through deception."* (URL3)

In Germany, private investigation is subject to legal licensing and strict data protection rules. The admissibility of evidence gathered by private investigators in court is often disputed, especially if it violates data protection laws (Heinze, 2021). The German legal system distinguishes between investigations conducted by private individuals and authorities, and private investigators are not authorized to conduct covert surveillance or wiretapping.

In Austria, the legal framework for private investigation is regulated by the Gewerbeordnung (Commercial Code), which stipulates licensing conditions and professional requirements. The seizure and examination of data from mobile phones and digital devices was given a new legal framework in 2024, which tightened data processing procedures (URL4). Private investigators often collaborate with law firms and corporate compliance departments (Knoetzl, 2019).

In Slovakia, the legal regulation of private investigation is relatively new and the activity is subject to licensing. The role of private investigators is becoming increasingly important in corporate and family matters, but the legal framework is still under development. The role and impact of private investigation in the security sector is being examined in a growing number of studies (Boroš et al., 2022).

In Slovenia, private investigation is regulated by law and operates independently of the police. The legal framework for these activities is defined by the Private Detective Act, which regulates licensing, data management, and ethical standards in detail (Britovšek et al., 2018). The role of private investigation has also appeared in the security policy discourse, particularly in connection with the fight against terrorism.

In the Czech Republic, the legal framework for private investigation is defined by commercial law and data protection regulations. The role of the private sector in investigative activities is growing, especially in the detection of corporate abuse and fraud (URL5). The legal environment allows private investigators to gather information within certain limits, but its admissibility in court is subject to strict conditions.

As the examples of the countries we analysed show, there is a definite social demand for the services of private investigators, which in most cases is accompanied by strict legal regulations, while a scientific examination of the activity and a detailed elaboration of its scientific foundations are still pending.

The history and regulation of private investigation offices in Hungary

Examining the history of domestic policing, the operation of private investigative (private detective) offices claimed an indisputable part in it, in connection with which the first legislation was issued in 1913, 135.585/1913. B.M no. m. out. circular decree of the Minister of the Interior on the regulation of the operation of private investigative (private detective) offices. According to the introduction of the decree that entered into force on February 1, 1914, "in recent times, there has been an increase in the number of companies that, under various names, such as private

research (private detective) offices, in a business-like occupation that is not covered by the industrial law, obtain information of a confidential nature through observations and research undertake - by deceiving the public, often extending their operations to the performance of tasks that are reserved for public authorities or their circles". The purpose of creating a decree prohibiting the use of the name "detective" for the owner and employees of a private research firm is to "prevent abuses that may be harmful to public order and the interests of the public" (Circular Decree of the Minister of the Interior No. 135.585/1913. B.M.), under the supervision of the police was the normative regulation of the authorization and continuation of listed private investigative activities.

As a negative effect of the changed living conditions following the First World War, some of the offices ceased their activities. Furthermore, 1 October 1919 on the nationalization of the police, 5047/M. The decree issued under the letter E created new conditions in certain issues of administrative policing, so the regulation - issued for the regulation of the operation of private investigative (private detective) offices m. out. Minister of the Interior 99.546/IV. Based on Circular Decree No. 1921 - amended. As the 1926 issue of "A Rend", the first newspaper of the Hungarian police at the time, emphasized: "the private detective is an indispensable supplement to the official police in the broader protection of the individual" (A Rend, 1926; 4).

After the Second World War, however, in 1949, due to the classification of the Hungarian state as a Soviet type of state, the activity of private detectives was prohibited by Law 458700/1949. (X.16.) Banned by BM decree. The decree - § 1 of which stated that "It is forbidden to maintain a private investigator (private investigator) office⁴, and to deal with private investigator activities, research, confidential observations and the performance of related data services as a business" (BM Decree

⁴ The number of private research offices in Hungary rose to 20 by 1916. There were 12 offices with 16 employees in Budapest in 1918, and 27 offices in the 1920s. From the end of the 19th century until 1945, 200-250 people nationwide could engage in private investigation, and then in the period between the two world wars, approximately 50 people could continuously carry out private investigation activities. After the Second World War, a total of 15 private investigation offices operated in Sopron, Szombathely, Székesfehérvár, Pécs and Kaposvár.

458700/1949. (X.16.) § 1.) - declared it to be a violation and ordered the violator to be punished with a fine and imprisonment, and at the same time, Article 45800/1923, which provided the legal basis for private detective activity until then, was also out of force. no. BM decree (Mészáros, 2010; 286). All this was confirmed by 6/1982. (VIII.1.) MT decree, as well as 24/1987. (VII.22) MT. the entry into force of the decree, which already specifically prohibited the conduct of private detective activities.

In the ministerial decree issued in 1987 – equivalent to a government decree in today's Hungarian legal hierarchy – private investigation was still interpreted as a prohibited activity, while, even if in a narrow circle, the performance of asset protection activities has already been permitted (Decree 24/1987. (VII. 22.) MT). After that, we can even consider it a revolutionary step forward the adoption of Act No. 87/1995 on the personal and property protection carried out in the framework of the enterprise, as well as on the transitional rules of private investigative activities. (VII. 14.) The government decree, in addition to repealing the previous ban by the Council of Ministers, legalized and regulated the activity of private detectives for the first time after almost half a century. The government decree describing the activity of private investigators, IV of 1998, was superseded by law, specifically Act CXXXIII of 2005 which remains in force (hereinafter: SzVMt.) (Mészáros, 2010, p. 286). Marked as a sad fact and characteristic of all three pieces of legislation, in addition to the personal and property protection provisions, the creation of detailed rules for private detective activity was neglected; they contained only difficult-to-interpret, vague and contradictory provisions regarding private investigation.

Legal regulation of private investigation

Based on the unanimous opinion of experts and law enforcement researchers, it would be necessary to amend the legislation, or even to create an independent norm separate from asset protection activities (Mészáros, 2010; 285–294). In recent years, there have been several initiatives and even draft legislation for this, but no change has been achieved.

In this part of our study, we scrutinize the normative elements of the already mentioned law on the protection of persons and property, as well as the rules of private investigative activity, regarding private investigation, as the elements of the legal regulation of the activity. Also pointing out that with respect to private investigations, for example, the provisions on data protection, the regulator dealing with civil legal relations and the sanctioning standards for violations and non-compliance with the laws must be taken into account, since the complexity of the laws and regulations provides the legal framework along which private detectives can legally carry out their assignments.

Examining the SzVMt from the point of view of the subject conditions necessary for the performance of private investigator activities, for the private investigator and the private investigator company, it can be seen that a certificate issued by the police at the request of the private investigator is required for the organization, management, and direct execution of the activity. This ID card can be obtained by a Hungarian citizen of legal age, with no criminal record, or a person with the right to free movement and residence, who has at least a secondary education and a required professional qualification (Section 6 of Act CXXXIII of 2005).

In possession of the operating license, the private investigator conducts his activities in all cases on the basis of an assignment (business) contract drawn up in accordance with the rules of Act V of 2013 on the Civil Code (hereinafter: Civil Code), as well as a valid compensation for damages caused during the performance of the assignment, as well as the damages fee it can be carried out in possession of liability insurance and a certificate of payment (Law CXXXIII of 2005 §§ 5–6). Based on the conflict of interest rule appearing in the law, a senior official of a private investigative company cannot be a senior official of a private investigative company or a professional staff member of the police (Act CXXXIII of 2005 § 3.).

According to the SzVMt, the private investigator or private investigation company (contract register) must keep a diary of the contracts. It must record the time of the conclusion of the contract and its termination, the name and address of the client(s) - in the case of a company, its headquarters - and the scope of the person(s), involved business(es)

and other contributor(s) actually participating in the fulfilment of the assignment.

The effective Civil Code states that a contract with an illegal purpose or content, or that conflicts with good morals, is null and void (Law V of 2013 §§ 6:95–6:96), and this also applies to the commission of a private investigator. It follows that the private investigator's task can only serve to enforce the client's legal rights - or at least those believed to be so in good faith - and to protect their legitimate interests, and in no case can it be self-serving or based on illegal interests.

We consider it essential to mention that the legitimate interest of a private individual authorizes and makes it legal for the private investigator to process personal data⁵ without the consent of the affected person (GDPR Article 6 (1) points c) and d)). At the same time, the moral responsibility of the private investigator is also significant, since private detectives often work with personal and, in most cases, sensitive information. Moral responsibility lies mostly in respecting people's privacy as much as possible, even in the case of data collection within the framework of the law. In addition, the client's trust in the private investigator is important; both the performance of the work at an appropriate professional level and the determination of the remuneration for the activity. Abuse of trust can have serious consequences due to the nature of the work, therefore it is extremely important to select and commission a morally impeccable private investigator or private investigation agency. As the Hungarian Detective Association points out on its website, *"We have to admit that, due to the above, the selection and commission of a private investigator can involve significant risks for the principals. In the absence of an authoritative and public register, it is not easy to identify companies and entrepreneurs*

⁵ Personal data: any information relating to an identified or identifiable natural person ("data subject"); a natural person can be identified directly or indirectly, in particular on the basis of an identifier such as name, number, location data, online identifier or one or more factors relating to the physical, physiological, genetic, mental, economic, cultural or social identity of the natural person can be identified. Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free flow of such data, and on the repeal of Directive 95/46/EC (General Data Protection Regulation) (hereinafter GDPR) According to Article 4, Clause 1.

operating in the grey zone - hiding behind the guise of security consulting, without official authorization - operating in the black economy and without any license yet claiming to be private investigators. Due to the confidentiality obligation of the private investigator, he cannot present references to his future client, so it is a serious difficulty for every investigator to prove his professional preparation, even more so, his credibility" (URL6). Private investigators must therefore find a balance between the client's interests and ethically and morally correct actions. Transparency, integrity and objectivity are fundamental ethical guidelines in this profession in order to avoid incorrect methods of obtaining information and violations of law.

Given the relationship of trust between the private investigator and the principal, as well as the personal data that can be obtained during the data collection, the private investigator is bound by an obligation of confidentiality during the period of activity according to the contract, as well as after it, with regard to all facts and data of which he became aware during the performance of the contract and in connection with it (Act CXXXIII of 2005, Section 22, Paragraph (1)). The private investigator can only inform the principal about the obtained data, except in the case of being questioned as a witness in official proceedings (Article 22 (3) of Act CXXXIII of 2005).

According to the rules of the SzVMt, private investigative activities may not be directed at the activities of diplomatic or consular missions, international organizations under the same jurisdiction as these, as well as their members, or official bodies, national and foreign specified in Act C of 2012 on the Criminal Code (hereinafter: Penal Code) for a person's official activities (Article 35 of Act CXXXIII of 2005). Even here, the question arises as to what exactly can be considered to constitute the official activities of such persons.

In addition to the conditions described so far, the private investigator, in order to fulfil his lawful assignment arising from the contract, exercises the rights of the principal based on his professional training and abilities, with the specifics and limitations of forensic tools set out in the SzVMt. Examining the actual activity, we can say that the apostrophized activity of a private investigator is nothing more than a complex data collection operation with many possibilities.

According to the wording of the SzVMt, during the performance of an assignment, the private investigator may collect data and request clarification (Article 34 of Act CXXXIII of 2005). For the conceptual definition of data collection, it is necessary to look beyond the SzVMt. In terms of the conceptual definition of data collection, it is "a process in which the desired data is obtained from the stakeholders with the help of selected methods and techniques, or from the respondents. In the sense of private security, it is the method of obtaining information provided by law for the private investigator, in order to fulfil the assignment contract for the given case, based on the current legislation" (Boda, 2019; 16).

According to the law on criminal procedure, "the prosecutor's office, the investigative authority, the internal crime prevention and detection body of the police, and the anti-terrorism body of the police may collect data for the purpose of establishing the suspicion of a crime, and in order to clarify whether there are any means of proof and where they are located" (Section 267 (1) of Act XC of 2017). In doing so, the authorities may collect data from registries defined by law, public or lawfully disclosed data files or sources, request information from anyone, select and identify a person or object by presenting images, sounds, or images and sound recordings, and examine the scene of a crime. The acting member of the authority prepares a record of all such data collection activities (Article 267 (3) of Act XC of 2017). Data collection (information acquisition) – not necessarily the most effective, most expedient, but undoubtedly the simplest method – is the identification, search and interview of the person or persons who have relevant information regarding the event or the person that is the subject of the assignment.

One of perhaps the simplest, completely open and legal methods of data collection includes, in addition to listening to the persons concerned, the analysis of various press materials and announcements, the collection of data on the Internet, and in today's popular, but somewhat incorrect term, OSINT (open source intelligence). Open source data collection does not run into legal obstacles, since the person affected by the data collection is the one who publishes their data, thereby quasi contributing to the management of their personal data.

Covert data collection is more difficult, requiring greater preparation and deeper professional preparation, but in many cases the only method that provides results. The difference between the two execution methods of data collection is that during covert data collection, softening - or even more complex environmental studies - a so-called legend is used, which is the "fictitious identity or cover story used by the private investigator when collecting data on behalf of the private investigator" (Boda, 2019; 364-365). The legend can be completely fictitious, but it can also be a fictional identity or event based on an actual one, which is suitable for the successful execution of the data collection, aimed at obtaining the data necessary to fulfil the private investigator's assignment contract.

A member of the authorities acting in criminal cases authorized to use covert devices when such devices are not subject to a judge's or prosecutor's license, can collect and check information about the crime while keeping the true purpose of the procedure secret (Act XC of 2017, paragraph 214 (4) point a) and 215 §. (2); however, covert data collection carried out without a legal basis may result in criminal prosecution (Article 305 of Act C of 2012).

During the data collection activity carried out with the legend, the private investigator may not enter or remain in the private apartment, other premises or fenced area of the other person against the will of the resident or the person who owns it, or by deception, because in that case he commits an offense of trespassing (II of 2012 § 166 of the Act). If the created legend is based on an official procedure (for example, the private investigator acts as a local government official, or as a statistician acting on behalf of the Central Statistical Office, etc.), then the private investigator can no longer be held responsible for the violation of the law of private residence, but for its criminal nature (221 of Act C of 2012). §.).

The situation-based, purely private investigator competence is the choice of whether the private investigator conducts open or covert data collection. The answer to making a decision will mostly be provided by the experience of practicing the profession.

Another special and extremely effective method of covert data collection, and - as a result - the most frequently used one and the most prominent segment of the activity is tracking and monitoring, which is

"getting to know the activities of persons, as well as events and happenings, while staying outside a private residence" (Boda, 2019; 382). If the observed person resides in a private apartment or a place with the same status, the private investigator's observation using only his own senses - even through a window - is legal, because the person concerned must ensure the protection of his private sphere. From a criminal law point of view, this is the only exception to the prohibition of data collection concerning private residences.

While the conceptual definition only emphasizes the inviolability of the private home, the SzVMt, for reasons that do not require any particular explanation, expressly prohibits the making of video and audio recordings in places where surveillance may violate human dignity, such as in dressing rooms, fitting rooms, washrooms, toilets, hospital rooms and in the residential premises of a social institution (Article 34 (2) of Act CXXXIII of 2005).

An extremely important rule is that a private investigator may make and use video and audio recordings in the course of his data collection activities within the framework of the commission contract, in compliance with the rules on the protection of personal data and privacy rights (Section 34 of Act CXXXIII of 2005. (1) point c).

Practice shows that in many cases, the effective implementation of surveillance requires an advanced technical device that meets the standards of the age, which is indispensable for the unquestionable substantiation of what has been observed. During surveillance carried out with the help of a technical device, special attention must be paid to the location of the observed person, the locality of the surveillance, because this determines the legal framework. If the observed person is in a public place or a place open to the public, or on a means of public transport, the private investigator may, in addition to observing with one's senses, make and use video and audio recordings within the framework of the assignment contract. At the same time, the situation of absolute prohibition exists if the target person, object, event, or relationship of the surveillance resides in a private residence or in a place of the same nature (for example, in a private vehicle), and the private investigator wishes to document this with a technical device (either from an external location

or by bringing in a device). It is also prohibited to observe events inside a private residence or a property under the same legal protection using an unmanned aerial vehicle (commonly known as a drone).

Finally, in connection with surveillance using technical devices, it should also be mentioned that - on the basis of other legal regulations - the private investigator may not use dual-use or military equipment⁶ (Government Decree 156/2017 (VI. 16.)).

The experience of observation and the information obtained are recorded in sufficient detail by the specialist performing the private investigation in the so-called observation report. Relevant photographs taken during the observation, according to the legal framework, can be embedded in the report, but photo, video, audio and audiovisual recordings can also be attached to the report. Precise documentation is extremely important, not only from the point of view of the effectiveness of the assignment, but also for correct accounting to the client.

The provision of data can be requested from anybody, a legal person or organization without legal personality for the bodies authorized to carry out formal investigations, i.e. to continue criminal proceedings, although a public prosecutor's license is required for special data - electronic communications, postal, banking or health data - that deeply affects the private sector. (Law C of 2012 §§ 261–262). Pursuant to the Act on Criminal Procedure, the requested person is obliged to provide free information within the deadline specified by the authority (Article 264 of Act C of 2012, paragraphs (1) and (2)).

Based on a comparison of the itemized list of the SzVMt and the rules defined in the criminal procedure law, it is clear that the access of private investigators to the official databases is much narrower - certainly due to

⁶ According to Regulation (EU) 2021/821 of the European Parliament and of the Council on the establishment of an EU control system for the export of dual-use products, their brokerage activities, related technical assistance, and their transit and transfer Dual-use products: those products, including software and technology that can be used for both civilian and military purposes, including products that can be used for the design, development, manufacture or use of nuclear, chemical or biological weapons or their means of delivery, including products that can be used for explosive purposes and for any form of contribution to the production of nuclear weapons or other nuclear explosive devices.

the protection of personal data already discussed - so the data collection possibilities in this direction are more limited.

In connection with the private investigator activity, the SzVMt also mentions that the private investigator can check the contents of a sealed shipment addressed to another party only with the prior consent of the recipient or the sender. The protection of the confidentiality of correspondence is also an emphasized fundamental right, therefore there is no possibility of voluntary knowledge of sealed correspondence sent to others.

The Forensics of Private Investigation

Forensic science is "a multidisciplinary criminal science that develops scientifically based tools, methods and procedures in accordance with current legal regulations for the purpose of detection and proof, as well as the prevention of crimes" (Boda, 2019; 355). Forensics is the science of investigating crimes, and the principles, tactical recommendations and procedural methods that form part of the discipline are of decisive importance during the investigation of individual crimes; thinking, for example, when facts need to be established, data obtained and evaluated, versions set up or possible explanations of an event/phenomenon defined (Mészáros, 2015; 133). By criminal investigation, we mean intellectual and practical activities aimed at learning about an event or phenomenon that happened in the past, carried out with data and the versions based on them, while private investigation refers to the multifaceted collection of data aimed at learning about the past, present and future.

The toolkit of private investigation, which shows similar features to criminal investigation but is characterized by different characteristics and specific data collection methods, as a multifaceted data collection activity, is fundamentally based on the science of forensics, keeping in mind its main questions (What? Where? When? Who with? How? Why?). We mention the following as perhaps the most relevant elements of forensic thinking, also used during private investigations:

- setting up and checking versions (its necessity and process are equally important in criminal and private investigations) (Sasvári, 2011; 44–47),
- reverse causality (during the investigation of events that happened in the past, the private investigator deduces the cause based on the principle of reverse causality) (Sasvári, 2008; 14)
- planning and organization of an investigation (similar to a criminal investigation, a private investigation cannot be ad hoc, the individual steps, the entire data collection process must be consciously planned in advance),
- compliance with tactical recommendations (it is also advisable to comply with tactical recommendations developed by forensics during a private investigation; for example, the use of listening, tracking, evidence, etc. techniques)
- evaluation and analysis work (evaluation and analysis of acquired data),
- application of methodological elements (professional/procedural protocols developed for certain types of crimes) (Sasvári; 2008; 79-81) (Mészáros, 2015; 135).

We point out that there are interesting similarities between the professions of private investigator and lawyer since both activities assume a relationship of trust between the client and the service provider, during which the basic requirement of discretion and the obligation of professional secrecy are involved. Like the lawyer, the private investigator acts on behalf of the principal, exercises his rights and represents his interests, and the purpose of both professions is to assert the principal's rights, fulfil his obligations or protect his interests. It should be pointed out that nowadays private investigation is "a service provided within the framework of an enterprise (individual enterprise or individual company or business association), which is performed by the private investigator on the basis of an assignment contract concluded under the rules of civil law, naturally in exchange for compensation" (Mészáros, 2015; 134).

In the case of providing security as a service - under free and fair market conditions - within the framework of a business, only the business

that is able and capable of providing a marketable service of an appropriate level and value for money, based on legal foundations, remains "alive". And this brings us to one of the most interesting questions in private investigation: "Why do people turn to private investigators?" Many people then think of investigating the reliability of the unfaithful spouse, for which the client often only pays several million forints (the hourly rate of a private investigation company in Budapest is around HUF 20,000 plus VAT; and for the monitoring, at least three vehicles, 6-7 professionals and technical means are needed, sometimes for months; not to mention the cost of obtaining information in other ways) and gets an answer after paying. At the same time, in Hungarian civil law (unless the marriage or other contract expressly states this) the proof of infidelity in any direction has no relevance. Based on this, it is easy to understand that the so-called "panty cases" are present only with a smaller weight in domestic private investigations.

Why do they turn to a private investigator?

People turn to a private investigator if the procedure of the police or other authority did not bring the result they expected, or if the procedure did not lead to a result; if for some reason they cannot or do not want to turn to the authorities, or the matter in question does not fall under the jurisdiction of the authorities. The following can be considered traditional private detective services:

- searching for stolen or lost things,
- examining and testing the loyalty of a partner or spouse,
- collection of data related to personal relationships,
- examining and testing the honesty of a friend or business partner,
- searching for a missing relative,
- searching for persons who have disappeared or are staying or hiding in an unknown place,
- finding the perpetrator of an unsolved criminal case,

- checking of future or current employees within the company,
- security checks of senior officials and employees of business companies and other organizations,
- obtaining various economic and criminal information and evidence,
- preparing an environmental study,
- examination of insurance events,
- acquiring company information, writing company histories, mapping company networks,
- preparing (and possibly conducting) legal debt management and asset protection procedures,
- checking the reliability of future and current business partners,
- loss prevention in a multinational, wholesale environment, internal company investigations,
- expert investigations in economic matters,
- searching for and interviewing witnesses in civil and criminal cases, as well as obtaining other additional evidence, etc.

The above list, which is not exhaustive, can be expanded with an almost infinite number of elements, especially with regard to the dynamically changing living conditions of today. The individual principals:

- can specifically employ companies specializing in private investigations,
- can create security departments within their own organization dealing with business intelligence, prevention, and loss prevention (for example, the official name of the person performing security activities of the Marriott International hotel chain is "loss prevention manager", or
- in the case of certain matters of a sensitive nature, they may use covert companies to obtain internal or external information related to the company's operations (for example, there is a company that issues an invoice to another market service for its information-gathering activities).

Some thoughts on the activities of a legitimate private investigator

If we are talking about a private investigator (enterprise) that operates legally in all respects under clean market conditions, then before accepting the assignment, the case must always be discussed with the client and the legal and ethical solutions necessary for its solution must be considered; in justified cases, it is recommended to contact the authorities (for example: in the case of a missing person, object, private life, insurance event, internal investigation of companies, other crimes, etc.). In the case of taking on the case, it is reasonable to prepare a preliminary estimate of the budget (by phasing the case), indicating the delivery and cost of the expected result product(s) (the client must be continuously informed during the procedure; give and receive feedback on whether we are moving in the right direction during the private investigation).

The investigation must be conducted in a legal manner, so that the collected evidence can also be used in court. The same applies to the acquisition, storage and analysis of the collected documents and evidence, and the preparation of the private investigator report concluding the assignment, with particular regard to its future uses.

During the legal procedure, we must not forget that the private investigator:

- does not have authority, cannot obstruct the procedure of the authority,
- may not wear a name or uniform that refers to authority, or any other sign or address or rank insignia that suggests an official character, suitable for deception,
- must keep his ID card with him when carrying out his activities and present it during the official inspection (the administrative and criminal service branch of the police is entitled to inspect it),
- may act in the interest of several principals only if their interests do not conflict,
- can perform an assignment that may harm the interests of the previous client only if three years have already passed from the termination of the previous contract,

- the contract created between the agent and the principal, between equal parties, is realized on the basis of mutual agreement in the field of civil law, so the assignment must be recorded in writing (there is a legal obligation to keep a contract registry diary, the retention period of which is five years).

According to the legal provisions on the continuation of the activity, the private investigator is not entitled to more rights than the principal; its activity can also be evaluated as an extended hand of the principal based on the *nemo plus iuris*⁷ principle. *In relation to his work regulated by legal restrictions, he is obliged to maintain confidentiality, but during his hearing as a witness, he is under the obligation to tell the truth (he can ask for/ receive an exemption from the contractual confidentiality from the client). We mentioned it in the previous part of our article, but the extremely large numbers of moral and legal questions that test all private investigators that arise in connection with private investigations also require analysis from a forensic perspective. Some of these include the following:*

- Is what is effective legal, or is what is legal effective?
- Moral questions, based on when, how and why I can reject a case?
- How important is profit orientation and focus on results?
- Is the customer's will holy?
- "I want the result by yesterday!" How important is the time factor?
- Does the principal "want to drink blood" or does he just want to get his valuables back?
- Is it necessary to go as far as criminal proof, or is persuasion enough?
- Is what the client says true? How deeply should the principal be checked, and his motivation investigated?
- Which of the obtained information do we consider relevant, which of these do we want to share with the client, why and how? Do you have to share everything with the client at all?
- The issue of assignments of a sensitive nature affecting political interests.

⁷ It is a basic principle known from Roman law and linked to real property law, according to which no one can transfer more rights than he already has.

- The scope of assignments related to organized crime.
- Regarding the use (usability) of the results, their possible consequences, the issue of moral responsibility related to the use.

In the course of his activities, the private investigator cannot carry out formal investigative acts, but at the same time he can rely on a number of forensic and evidentiary sources (for example: testimony, incriminated testimony, physical evidence, expert opinion, document, etc., as well as the possibility to conduct an inspection, presentation for identification, proof test, on-site hearing). In the course of his work, he can use experts and consultants (for example: a polygraph examiner, a linguist, an expert on voice, writing, document, genetics, etc.). As we explained in the legal framework, he can also use hidden data collection tools (tracking, monitoring, and use of legends) within strict legal limits.

Importance of open source information acquisition in private investigation

Nowadays, the already mentioned OSINT, open source information acquisition, is present with the highest degree of effectiveness in the activities of a private investigator. A large number of domestic and international literature deals with OSINT, so in our article we examine the procedural elements that we consider important from the point of view of private investigation.

Emphasizing cost-effective and effective business operations, "20% of usable information can be obtained from qualified sources, for which 95% of the costs must be sacrificed [...] 80% of usable information comes from open sources, for which 5% of the costs must be used" (Kenedli, 2013; 172). As a result, the importance of open-source resources that can be researched in a targeted manner and are accessible to anyone with appropriate expertise is enhanced, highlighting the following:

- traditional media (newspaper, radio, TV programs),
- grey literature (work and discussion documents, brush prints, research and market research, economic and other reports, stan-

- dards travel reports, minutes, studies, dissertations, theses, conference materials, theses, etc.),
- personal experiences of experts and observers,
 - recordings of commercial satellites,
 - commercial online information providers,
 - the internet, highlighting social networks (based on estimates, there are between 15 billion and 1 trillion pages on the world wide web),
 - other sources (language schools, scientific organizations, universities, libraries, business journalists, civil organizations, etc.),
 - personal experiences.

Among the applicable OSINT tools, emphasis is on the following methods:

- innovative data mining and data analysis,
- search based on intelligent linguistic foundations,
- intelligent search engines,
- thematic sorting system (for example, automating the monitoring of RSS channels),
- social media monitoring (for example, immediate risk assessment of flash mobs),
- evaluating the source code of websites, displaying hidden content,
- domain search, whois tools (extracting data that can be linked to the website's domain subscriber),
- Hungarian and international press monitoring (Nyeste & Szendrei, 2019; 56).

Openly available domestic databases that are most often used during the work of private investigators in Hungary include:

1. E-company register: (www.ecegjegyzek.hu):
 - the paid business directory services are a much more complete, versatile and usable database, which, in addition to the contact diagrams, also contain data on individual entrepreneurs, and it is also possible to search by person,

- an additional option is the closed system company register available at the company courts, which is less easily searchable than the paid registers, but contains scanned and electronic versions of the companies' data related to the company procedure, thus containing a lot of useful information that the online registers do not.
- 2. Electronic report, portal (www.e-beszamolo.im.gov.hu);
- 3. Magyarország.hu property and vehicle search functions (www.mo.hu);
- 4. National legislation repository (www.njt.hu);
- 5. Records of searches of persons and objects (www.police.hu);
- 6. National Tax and Customs Office databases (www.nav.gov.hu):
 - inquiry of taxpayers (this is an important register because it may also include locations in relation to companies that were not only reported to the NAV register at the company court),
 - registration of tax arrears,
 - employees, employers without notification,
 - reliable taxpayers, etc.
- 7. National Data Protection and Freedom of Information Office databases (www.naih.hu):
 - resolutions.
- 8. Court databases (civil organizations, court decisions), (www.birosag.hu);
- 9. Google: (www.google.com) (in addition to the basic search, various sub-services are also important):
 - Street View,
 - Google image-based search.
- 10. Social media (Facebook, snapchat, YouTube, tinder, Instagram, etc.);
- 11. Databases of the National Intellectual Property Office (trademark protection, patent protection), (www.sztnh.gov.hu);
- 12. Agricultural Parcel Identification System (geographic number search outside) (www.mepar.hu):

- related to this, the settlement plans of the local governments, which are usually available on the websites of the individual local governments.
- 13. Arcanum digital science library. Press products in digital format (www.arcanum.com);
- 14. Electronic Archive Portal (www.eleveltar.hu);
- 15. Public procurement database: (<https://kozbeszerzes.hu/adatbazisok>);
- 16. Government tender portal (https://archive.palyazat.gov.hu/tamogatott_projektkereso);
- 17. Register of primary producers (<https://portal.nebih.gov.hu/oftermelo-kereso>).

In the case of the OSINT methodology and the processes it involves, the first phase is the collection of data, the second is data processing, the third is the analysis of the information, while the fourth and final phase is the sharing of the OSINT product. Methodologically, we emphasize the importance of lexical, social network and geospatial analysis, as well as their combinations. Furthermore, we should mention the prohibitions of the GDPR rules that are organically related to OSINT, the prohibitions related to the active and passive research of certain contents (for example: terrorism, child pornography, etc.), even in addition to criminal prosecutions due to research carried out by illegal means.

Conclusion

In our study, we wanted to provide an insight into the history of the development of the private detective activity in Hungary, which is little known to many, as well as the legal regulation and forensic characteristics of the activity. Examining the existing domestic literature on private security, which can be said to be relatively meagre, we can see that it is a rather controversial legal field that has not been worked out with scientific thoroughness. It is controversial because there are many questions regarding the place, role and importance of private security, since it is a

relatively young field that has been developed in our country since the regime change; perhaps because of this, the precise theoretical foundations have not been developed so far. We would like to contribute with this paper to the exploration of this little-researched area, therefore, within the framework of this study, our efforts can only be limited to raising some of the questions we consider controversial here and now, and as a result of this confrontation, by recording the legislative and theoretical problems of the subject area, to further research and the development of solution alternatives - with sufficient professional humility – let us encourage those who are open to the development of the nascent law enforcement science (Balla, 2020; 26).

List of used literature

1. Balla, Z. (2020). Ockham's razor and policing. *Hungarian Police*, 23(3): 15–26. <https://doi.org/10.32577/mr.2020.3.1>
2. Boda, J. at al. (ed.): *Law Enforcement Encyclopedia*. Budapest, Dialogue Campus, 16. 2019, 355, 364–365, 382.
3. Boroš, M., Zvaková, Z., Šoltés, V., & Veľas, A. (2022). What is the role of private intelligence in the Slovak Republic? *Security Journal*, 35, 649–675. <https://doi.org/10.1057/s41284-021-00294-2>
4. Britovšek, J., Tičar, B., & Sotlar, A. (2018). Private intelligence in the Republic of Slovenia. *Security Journal*, 31, 410–427. <https://doi.org/10.1057/s41284-017-0107-0>
5. Finszter, G. (2009). Public safety and the rule of law. *Law, state, politics*, 3. 66–83.
6. Heinze, A. (2021). Evidence illegally obtained by private investigators. *New Criminal Law Review*, 24(2): 212–253. <https://doi.org/10.1525/nclr.2021.24.2.212>
7. Kenedli, T. (2013). The general theory of national security. University note. National University of Public Service Institute of National Security. 172.
8. Knoetzl, B. (2019). Global investigations around the world: Austria. <https://www.lexology.com>

9. Mészáros, B. (2010). Current issues in the regulation of private detective activity. In: Gaál, Gy. & Hautzinger, Z. (eds.) Pécs Border Guard Scientific Publications XI. Studies in "Quo vadis policing? From the scientific conference "Freedom rights, social obligations and security". Hungarian Military Science Society Border Guard Section Pécs Special Group, Pécs, 285–294.
10. Mészáros, B. (2015). The relationship between forensics and private investigation. In: Gaál, Gy. & Hautzinger, Z. (eds.) Law enforcement aspects of modern threats. Pécs, Hungary. Hungarian Military Science Society Border Guard Section Pécs Special Group, 133–135.
11. Nagy, T. & Lukács, Zs. (2019). Law enforcement characteristics and private security role of personal protection. In: Christian, L. at al. (ed.): Safety Manager's Handbook. Ludovika University Publishing House, Budapest, 168–169.
12. Nyeste, P. & Szendrei, F. (2019). Open source information acquisition in law enforcement. National Security Review. 7(2) 56. <https://doi.org/10.32561/nsz.2019.2.5>
13. Sasvári, R. (2008). Professional knowledge. In: Szabó, L. (ed.): Handbook of private investigators. SzVMSzK, Budapest, 14., 79–81.
14. Sasvári, R. (2011). The criminalistic mindset. Detector Plus 4. 44–47.
15. The Order (1926). The glorification of the private detective as clever advertising. no. July 17, 1926. 4

Legislation used

1. 135.585/1913. B.M no. m. out. circular decree of the Minister of the Interior regulating the operation of private investigative (private detective) offices.
2. 458700/1949. (X. 16.) BM decree on the termination of private investigative agencies and the prohibition of the continuation of private investigative activities (Administrative registration number: 5.661.), § 1.

3. 6/1982. (VIII. 1.) BM decree on the prohibition of private detective activity.
4. 24/1987. (VII. 22.) MT decree on asset protection activities and the prohibition of private investigations.
5. CXXXIII of 2005 Act on the protection of persons and property, as well as the rules of private detective activity § 3. 5–6. §, § 22 (1)-(3), § 34-35.
6. CXX of 2012. Act on the activities of persons performing certain law enforcement duties, as well as on the amendment of certain laws to ensure action against school truancy.
7. Act V of 2013 on the Civil Code 6:95 – 6:96. §.
8. II of 2012 law On violations, the violation procedure and the violation registration system § 166.
9. Act C of 2012 on the Criminal Code.
10. Regulation (EU) 2016/679 of the European Parliament and of the Council (April 27, 2016) on the protection of natural persons with regard to the processing of personal data and on the free flow of such data, and on the repeal of Regulation 95/46/EC (general data protection decree) Article 4, point 1, Article 6, paragraph (1) c) and d)
11. 156/2017. (VI. 16.) Government decree on the detailed rules for the licensing of military technical activities and the certification of enterprises.
12. 2017 XC. Act on criminal procedure 214 (4) point a) and § 215 (2), § 221, § 261 - 262, § 264. Paragraphs (1) and (2), § 267 § (3), § 267 § (1), § 305.
13. 2021/821. Regulation of the European Parliament and of the Council (EU) No. on the establishment of an EU control system for the export of dual-use products, their brokerage activities, related technical assistance, and their transit and transfer.

Internet links

1. URL1: CoESS and INHES White Paper, Private security and its role in European security, 15/12/2008 <https://www.coess.org/newsroom.php?page=white-papers>
2. URL2: Clifford Chance LLP. (2024). The private investigations legal framework. <https://www.cliffordchance.com>
3. URL3: Tremark. (2025). What Can Private Investigators In the UK Legally Do? <https://www.tremark.co.uk>
4. URL4: Schönherr Rechtsanwälte. (2024). Mobile data examination in Austria. <https://www.schoenherr.eu>
5. URL4: Gray, C. W. (2021). The Legal Framework for Private Sector Activity in the Czech Republic. *Vanderbilt Journal of Transnational Law*, 26(2), 271. <https://scholarship.law.vanderbilt.edu/vjtl/vol26/iss2/3/>
6. URL6: The requirements for membership are the strictest in the profession <https://detektivszovetseg.hu/>

Приватне истраге у Републици Мађарској

Апстракт: Као професионалци у области примене закона, у овој студији истражујемо историјски развој, правну регулацију и форензичке особености везане за активност приватних дејствија у Мађарској, о којој се мало зна. Бавимо се нормативним уређењем дејствијске делатности које је тешко проумачити и у вези са којим многа питања остају отворена, а иако ће се бавимо и одсуством адекватне регулације. Жеља нам је да дамо допринос једном свеобухватном научном истраживању и мишљењу приватног сектора безбедности. У данашње време полиција мора да одређује приоритете у погледу тога на које задатке ће фокусирати своје снаге, а које може да препусти приватном сектору. Одатле проистиче и питање: у којим областима ће полиција најчешће сарађу са приватним сектором безбедности како би обезбедила рационализацију задатака на нивоу државе и ефикасније и штедљивије функционисање организације. У овом раду, анализом теоретских и практичних основа везаних за приватне истраге настојимо да подстиакнемо будуће истраживаче који су заинтересовани за рад на овом пољу.

Кључне речи: Мађарска, приватне истраге, историја, правни процеси, форензика.

Доц. др Марија ПОПОВИЋ МАНЧЕВИЋ¹

Криминалистичко-полицијски универзитет, Београд

ДОИ: 10.5937/bezbednost2503061P

УДК: 351.746:323.28(100)

341.456:316.776

Прегледни научни рад

Примљен: 14. 10. 2025. године

Датум прихватања: 24. 11. 2025. године

Полицијска дипломатија у борби против глобалног тероризма: изазови и перспективе

Апстракт: Глобални тероризам је водећа претња националној и међународној безбедности. Чак и терористичке групе које делују унутар националних граница најчешће имају неки глобални елемент, било да је то идеолошка везница са неком другом групом, финансирање или интернет пројекат. Стога је међународни контратероризам један од главних задатака држава удружених у заједничкој борби против ове претње, и он захтева координирано и уједињено деловање различитих држава на националном и међународном нивоу. Да би се ово постигло, међународна полицијска и обавештајна сарадња нужни је елемент контратероризма, а она укључује размену информација и заједничке акције уз истовремено превазилажење равних и организационих ограничења која представљају изазов за ту сарадњу. Предмет овог рада је полицијска дипломатија, као алат превазилажења изазова и претрека у међународној сарадњи у области контратероризма, а истраживачко питање којим се рад бави јесте на који начин стратешке активности полицијске дипломатије могу олакшати и поједноставити оперативну сарадњу. Кроз студију случаја анализирани су активности полицијске дипломатије и резултати који су постигнути у сарадњи Европола и ФБИ-ја (САД и Европ-

¹ marija.popovic@kpu.edu.rs

ске уније) у борби против глобалног тероризма. Закључци показују да се активност полицијске дипломатије, оперативне праксе орјана за спровођење закона и правни оквир сарадње међусобно констатуишу и надограђују, а да је полицијска дипломатија одиграла кључну улогу у унапређењу сарадње Европола и ФБИ-ја, од терористичких напада 11. септембра до данас.

Кључне речи: безбедност, контртероризам, полицијска дипломатија.

Увод

Упркос усложњавању претњи безбедности у комплексном међународном окружењу данашњице, тероризам и даље представља једну од највећих претњи на свим нивоима, а борба против тероризма једна је од осам приоритетних области Секретаријата Уједињених нација (Report of the Secretary-General on the Work of the Organization, 2024). Тероризам је друштвени феномен ширег обима, па борба против тероризма укључује мноштво актера који једнички доприносе њеним различитим аспектима. Свакако, централно место у одговору на тероризам имају службе безбедности и полиција. Како се *modus operandi* терористичког деловања последњих деценија драстично променио, полиција као орган заштите јавне безбедности добија све истакнутију улогу у контртерористичком деловању јер су мете напада све чешће цивили, а места напада јавни простори и места масовног окупљања. Контртерористички напори на међународном нивоу све више зависе од успешне међународне полицијске сарадње, посебно у областима као што су размена обавештајних података, борба против финансирања тероризма и праћење транснационалних екстремистичких мрежа. С друге стране, међународна сарадња суочена је са правним, политичким и културолошким баријерама, те израженим неповерењем држава, нарочито у области сарадње у безбедносним стварима.

Циљ овог рада је да истражи улогу полицијске дипломатије у контртерористичким напорима на глобалном нивоу, с обзиром

на велики потенцијал, али и бројне изазове који постоје на плану међународне сарадње у области контратерористичког деловања. Улога полицијске дипломатије истражиће се кроз призму активности које се предузимају пре свега на нивоу полицијских аташеа и официра за везу, с циљем унапређења безбедносних политика, превазилажења политичких разлика и унапређења ефикасности глобалних контратерористичких мера. Кроз примену метода студије случаја, у раду ће бити приказане и контекстуализоване мере и активности полицијске дипломатије на примеру сарадње Европола и ФБИ-ја у борби против ИСИС-а. Резултати истраживања помоћи ће бољем разумевању свих препрека за успешну међународну полицијску сарадњу у области борбе против тероризма, и понудити детаљније увиде у могућности унапређења будућих иницијатива, како на глобалном нивоу, тако и на нивоу билатералне сарадње између држава које деле заједнички интерес у борби против тероризма. Такође, рад ће допринети научној литератури која се бави полицијском дипломатијом, као специфичним типом дипломатске комуникације између држава, и тако што ће истражити њен стратешки значај у обликовању и операционализацији полицијске сарадње.

Полицијска дипломатија – концепт и кључни актери

Људи су још од античког доба покушавали да унапреде могућности преговарања, побољшају услове преговарања и на тај начин обезбеде боље исходе у остваривању интереса својих заједница. Иако етимолошки корени дипломатије и њене рудиментарне практичне форме сежу далеко у прошлост, концептуализација дипломатије је релативно нова и дефинише се кроз сет пракси комуникације, представљања и преговарања (Leira, 2016: 36). Дипломатија се данас првенствено бави односима између држава, међувладиних организација, односно релевантних територијално-политичких ентитета, и значајан је инструмент спољнополитичког деловања. Као најважнији циљеви дипломатије и даље се издвајају промовисање спољнополитичких циљева појединачних актера, али

и тежња ка остваривању међудржавних циљева, глобалних циљева, унапређење односа између држава и омогућавање мирних односа између актера, решавање сукоба и спречавање ратова (Hart, Siniver, 2020: 171).

Како би најважнији циљеви дипломатије били остварени, дипломатија се реализује кроз различите дипломатске форме, а свака од њих фокусирана је на позитивне исходе у специфичној области. Тако постоје јавна дипломатија, дигитална дипломатија, економска дипломатија, спортска дипломатија, научна дипломатија, градска дипломатија, пословна дипломатија, војна дипломатија (видети: Constantinou, Kerr, Sharp, 2016). Тиме се ова класификација не завршава, а посебно важном чини се идеја о коришћењу полицијске дипломатије, нарочито узимајући у обзир обим међународне сарадње и комуникације држава у области борбе против прекограничних претњи безбедности. Иако идеја о полицијској дипломатији постоји извесно време и иако се праксе које се концептуално сврставају у праксе полицијске дипломатије већ спроводе, о самом концепту и даље постоји ограничен обим литературе. Потреба за полицијском дипломатијом јавила се са модерним безбедносним изазовима и претњама, а сам термин „полицијска дипломатија” често је поистовећиван са термином „међународна полицијска сарадња”. Ипак, треба истаћи да је полицијска дипломатија стратешки концепт који се и развио управо из потребе да се међународна полицијска сарадња, као оперативна активност, додатно унапреди и олакша. Полицијска дипломатија је новији концепт од међународне полицијске сарадње, и резултат је све веће институционализације те сарадње и померања од једноставнијих форми билатералне размене ка мултилатералном систему са стандардизованим оквирима заснованим на међународном праву (<https://neweralive.na/opinion-police-diplomacys-role-in-fighting-transnational-crime>, доступан 14. 3. 2025). Стога се полицијска дипломатија може одредити и као инструмент за унапређење комуникације држава и међународних организација, како би оперативне и тактичке активности борбе против криминала на међународном плану биле ефикасније и успешније. Та комуникација данас нужно

захтева и поседовање дигиталне писмености и знања о употреби дигиталних и интернет технологија, као и развијене вештине дигиталног комуницирања (Голубовић, 2023: 156).

Под полицијском дипломатијом подразумева се стратешко практиковање међународне сарадње између агенција за спровођење закона с циљем неговања партнерстава, размене обавештајних података, координације операција и стварања јединственог фронта против злочина који се протежу преко граница (<https://neweralive.na/opinion-police-diplomacys-role-in-fighting-transnational-crime>, доступан 14. 3. 2025). Конкретније, она укључује „ланац мера и поступака у упућивању полицијских службеника и органа из једног међународно признатог субјекта (међународно призната држава, званична међународна организација) у други, у службеном својству, који, притом, поседују одређене имунитете и привилегије у међународном субјекту у оквиру којег се акредитују, при чему извршавају задатке од важности за супротстављање, спречавање и борбу против међународних изазова, ризика и претњи безбедности” (Кекић, Субошић, 2009: 147).

Полицијска дипломатија је, самим тим, и део спољне политике, и као таква има утицај на спољне односе са другим актерима и успешније остваривање спољнополитичких циљева. Поред тога што полицијска дипломатија представља стратешку активност унапређења међународне полицијске сарадње у борби против регионалног и међународног криминала, њен допринос се огледа и у подршци изградњи државе у постконфликтним ситуацијама кроз обезбеђивање експертизе у области јачања капацитета за спровођење закона (Greener, 2011: 232). На овај начин државе се умрежавају, било билатерално, било кроз мултилатералне ангажмане, и остварују тежње да безбедност својих држава и грађана подигну на виши ниво кроз унапређење и ширење стабилности. Зато се полицијска дипломатија сматра каменом темељцем мировних мисија ОУН, а Интерпол је најбољи пример мултилатералне полицијске дипломатије у пракси (видети: Calcara, 2021).

Актери полицијске дипломатије постоје како на нивоу мултилатералних форума, тако и на нивоу билатералних споразума из-

међу држава, односно држава и међународних или регионалних организација. Актере полицијске дипломатије треба разликовати од полицијских дипломата у ужем смислу те речи, а то су једино полицијски аташеи. Аташеи се одређују као „лица које су званично додељена особљу дипломатске мисије да служе у одређеном својству, лица додата дипломатској мисији као специјалисти за одређена питања” (<https://www.thefreedictionary.com/attache>, доступно 18. марта 2025), а полицијски аташеи су експерти управо за питања борбе против криминала, тероризма и других питања од интереса за полицију земаља које представљају. Они се од других актера који имају одређена репрезентативна својства разликују по томе што имају дипломатски статус и привилегије. Увек се ради о високоранжираним службеницима, официрима националних полиција који су званични представници полицијских снага своје земље у оквиру дипломатске мисије и стационирани су у амбасадама или генералним конзулатима (https://www.fedpol.admin.ch/fedpol/en/home/polizei-zusammenarbeit/international/polizeiattaches.html?utm_source=chatgpt.com, доступно 18. марта 2025). У њиховој надлежности су активности које омогућавају шири оквир полицијске сарадње. Наиме, ангажовани су у преговарачким и другим стратешким активностима на високом нивоу како би се испреговарали билатерални или мултилатерални споразуми о полицијској сарадњи у конкретним стварима (https://www.fbi.gov/about/partnerships/international-operations?utm_source=chatgpt.com, доступно 18. марта 2025). Такви преговори служе да се у потпуности утврде оквири те сарадње, у смислу обима надлежности, привилегија, норми, а касније потписани споразуми имају предност у односу на националне законе, па отуда и тежина и значај улоге ових дипломата.

У евроатлантској регији, државе које се издвајају јер имају развијену праксу упућивања полицијских аташеа јесу Француска, САД, Швајцарска, Велика Британија. Сједињене Америчке Државе у оквиру ФБИ-ја имају правне аташее (*FBI Legal Attachés [legats]*), односно представништва (канцеларије) правног аташеа којих има 62 и покривају више од 180 држава, територија и острва, са више од 250 агената и помоћног особља стационираних ши-

ром света (<https://www.fbi.gov/about/partnerships/international-operations>, доступно 24. марта 2025). Особље ових канцеларија функционише под надлежношћу америчког Министарства спољних послова (Стејт департамент) односно шефова амбасада у иностранству, и основна мисија им је успостављање и одржавање веза са главним службама за спровођење закона и безбедносним службама у иностраним земљама како би ефикасно спроводили задатке борбе против међународног тероризма, организованог криминала, сајбер криминала и осталих облика криминала општег карактера. Поред ФБИ-ја, и британска Национална агенција за криминал (*NCA*) шаље своје међународне представнике, који су, иако се формално називају међународним официрима за везу, функционално слични правним аташеима ФБИ-ја јер делују као званични представници својих власти у иностранству и стационирани су најчешће у амбасадама. Иако је званично немогуће генерализовати њихов статус као дипломатски (јер он подразумева одређени степен формалне акредитације у зависности од споразума са земљом домаћина), ипак су формално сличнији аташеима јер поред оперативне сарадње имају и надлежности у области стратешке комуникације са партнерима и обликовању политика сарадње (<https://www.nationalcrimeagency.gov.uk/what-we-do/how-we-work/providing-specialist-capabilities-for-law-enforcement/international-network>, приступљено 24. марта 2025).

Када је реч о остатку Европе, добре праксе слања полицијских аташеа има Швајцарска, која упућује полицијске аташее од 1995. године као помоћ швајцарској полицији и правосуђу у борби против озбиљног међународног криминала, а такође су стационирани у амбасадама или конзулатима. Од 1. јануара 2017. Године, они имају мандат да се баве граничним и царинским питањима у име Савезне канцеларије за царину и граничну безбедност (*FOCBS*). Аташеима Савезне канцеларије могу се доделити предмети за решавање одређених случајева криминала који захтевају прекограничну сарадњу, када сматрају да би међународне мреже могле допринети њиховом ефикаснијем решавању (<https://www.fedpol.admin.ch/fedpol/en/home/polizei-zusammenarbeit/international/polizeiattaches.html?>, приступљено 24. марта 2025).

Француска познаје институт аташеа за унутрашњу безбедност, и он представља технички контакт за локалне власти одговоран за унутрашњу безбедност, под ауторитетом амбасадора Француске у оној држави у коју је послат (<https://www.police-nationale.interieur.gouv.fr/nous-rejoindre/nos-metiers/attache-de-securite-interieure>, приступљено 24. марта 2025). Француска тренутно има око триста службеника у 160 земаља који су део мреже службеника Службе за унутрашњу безбедност, а поред полицијских аташеа у тај број улазе и њихови заменици, официри за везу, асистенти, сарадници и технички саветници (<https://rs.ambafrance.org/Sluzba-za-unutrasnju-bezbednost?.com>, приступљено 24. марта 2025). Поред Француске, и Немачка има своје полицијске представнике у иностранству, који се називају официри за везу. Они такође комбинују оперативне задатке са стратешким задацима, а статус и овлашћења одређени су им специфичним споразумима са земљом пријема. Перутују се из Савезног криминалистичког уреда (Bundeskriminalamt, ВКА) и одговорни су за унапређење међународне сарадње у спровођењу закона, размену информација и координацију истрага са партнерским агенцијама у земљи пријема (https://www.bka.de/EN/OurTasks/Remit/InternationalFunctions/LiaisonOfficers/liaisonOfficers_node.html, приступљено 25. марта 2025). Према званичним подацима Владе Републике Србије, и наша земља одашиље полицијске аташее, и то од 2009. године (називају се и официрима за везу Министарства унутрашњих послова, али имају дипломатски статус јер су упућени у дипломатско-конзуларна представништва наше земље широм света) (Влада Републике Србије, 18. фебруар 2009; Влада Републике Србије, 23. јануар 2025).

Официри за везу такође су део мреже актера полицијске дипломатије, али они, за разлику од полицијских аташеа, могу бити и без дипломатских привилегија и статуса. То су често официри средњег нивоа, специјализовани за конкретна питања, због којих су упућени у страну државу да раде заједно са страним агенцијама за спровођење закона, али углавном не кроз амбасаде, већ су стационарани у специјализованим међувладиним агенцијама на међународном или регионалном нивоу. Интерполови и Европо-

лови официри за везу, рецимо, упућени су из својих држава и као такви везани за међународну организацију, без дипломатског статуса. Они који немају дипломатски статус фокусирани су пре свега на оперативну сарадњу између агенција, на размену обавештајних и оперативних података, заједничке истраге и координацију свакодневних заједничких активности или специфичних операција. С друге стране, ДЕА, федерална америчка управа за спречавање наркотика широм света има своје официре за везу који имају полудипломатски статус – формално су везани за амбасаде и на њих се примењује Бечка конвенција, али су као и остали официри за везу усмерени на задатке оперативног карактера. Официри за везу сматрају се, дакле, посредницима за захтеве који долазе из њихових матичних земаља или иду према њима, а тичу се размене информација, доказа, испитивања, претресања, хапшења и екстрадиција (Den Boer & Block, 2013: 9). Биго (*Bigo*) је истакао да је потреба за успостављањем официра за везу у Европи седамдесетих година симптом дубоких промена у визији криминала и небезбедности, као и промена у нашој перцепцији полицијских агенција које настоје да држе под контролом друштвене изазове (Bigo, 2002). Најзад, полицијски службеници у међународним полицијским мисијама сваку активност у оквиру таквих мисија данас виде као могућност дипломатског ангажовања и „дипломатски пројекат” (Waldbauer-Hable, 2023: 506).

Прво помињање официра за везу у мултилатералном контексту везује се за форум *TREVI*, када је Радна група *III TREVI* размотрила укључивање официра за везу за питање борбе против наркотика у међународној полицијској сарадњи у септембру 1986. године (Block, 2010: 201). Данас је потпуно уобичајено да мрежу актера полицијске дипломатије чине и представници држава у мултилатералним, најчешће регионалним иницијативама као што су *SELEC* (*Southeast European Law Enforcement Center*), *PCC SEE* (*Police Cooperation Convention for Southeast Europe*) и сличне, као и званични национални представници у међународним организацијама.

Најзад, значајну улогу у мрежи актера полицијске дипломатије имају и неформални актери као што су невладине организа-

ције и истраживачке и образовне институције. Рецимо, Асоцијација европских полицијских колеџа, иако без формалних дипломатских функција, кроз стратешко умрежавање и фокус на развоју лидерских вештина и размени најбољих пракси даје корисне резултате у виду хармонизације приступа у полицијској обуци, етици и управљању (видети: The Association of European Police Colleges, 2025). Најкориснији продукт ове мреже актера са дипломатским ефектом можда је управо изградња поверења и осећај заједничке мисије, а то је од кључне важности за сарадњу земаља које деле границу, а самим тим и проблеме прекограничног криминала.

Глобална сарадња у сфери борбе против тероризма

У међународним односима готово сваки вид сарадње или заједничког деловања започиње с циљем удруженог решавања неког безбедносног проблема, а глобална контратерористичка мисија један је од таквих задатака. Сложени међудржавни односи, супротстављени национални интереси и различито дефинисане безбедносне политике држава изазов су глобалним контратерористичким активностима. Државе су често опрезне и уздржане у размени обавештајних или оперативних података и осталим заједничким операцијама услед правних ограничења или политичких тензија. Често се паралелно са мултилатералном сарадњом у оквиру глобалних или регионалних организација спроводе и унилатералне тајне операције и праве билатерални договори.

Иако тероризам није претња безбедности коју карактерише велика учесталост, што свакако јесте захваљујући добрим контратерористичким и антитерористичким мерама држава, оно што ову претњу одржава тако високо позиционираном у безбедносним агендама јесте пре свега константно осећање страха и узнемирености јавности (видети: Gallup, 2025). Поред субјективног елемента, објективне изазове за службе које се баве борбом против тероризма представљају и нови трендови када је реч о терористичкој претњи, а Хофман и Вер (Hoffman, Ware, 2020) издвојили су шест

најистакнутијих. Први је губљење границе између домаћег и интернационалног тероризма, с обзиром на то да се међународне цихадистичке групе све више ослањају на спаваче, самодоктриниране „усамљене вукове”, у спровођењу аката насиља у њиховим државама, а екстремистички покрети традиционално локалног домета убрзано се интернационализују. Други је тренд театрализације и технологизације тероризма, креирања манифеста и преношења терористичких аката уживо (видети: Lucas, Baldino, 2021: 207), што терористима омогућава да своја незадовољства саопштавају јавно и инспиришу истомишљенике и присталице да крену њиховим стопама. Трећи је константна еволуција терористичких тактика и средстава коју агенције за борбу против тероризма морају ажурно пратити, те водити рачуна о томе да терористи данас циљају меке мете, да нису више фокусирани на организовање сложених, дуготрајних операција које су подложне евентуалном откривању и да користе средства попут 3Д штампаног оружја и осталог „фантомског оружја” које нема серијски број нити је регистровано, као што је, рецимо, био случај убиства извршног директора компаније Јунајтед хелткер (*United Healthcare*) Брајана Томпсона у Њујорку (Шубаревић, 2025). Четврти забрињавајући тренд који је присутан у Канади, САД и Европи јесте и све чешћа заступљеност војних ветерана и лица са војним искуством у екстремним десничарским, али и екстремним левичарским покретима, који захваљујући својим тренинзима и вештинама завређују посебну пажњу и фокус снага безбедности. Пети тренд је конвергенција и све нејаснија линија терористичке идеологије, као и изазован пораст оних који се изјашњавају као, условно речено, „идеолошки збуњени” јер не могу јасно да издифренцирају своје идеолошке мотиве (видети: Мијалковић, Бајагић, Поповић, 2023: 320). Шести тренд уочен у мноштву напада широм света последњих неколико година, повезан са деловањем Исламске државе, јесте и „фамилијаризација” терористичког деловања, односно учешће читавих породица или више њених чланова у планирању, организовању или спровођењу терористичких активности (Hoffman, Ware, 2020).

Тероризам је данас присутан у свим националним законодавствима која инкриминишу не само чин терористичког акта већ и све активности повезане са тероризмом: организовање, финансирање, обуку, подстицање на извршење, врбовање. Овакве активности тешко се ограничавају територијално, па стога и адекватно праћење и спречавање активности повезаних са тероризмом захтевају међународну сарадњу. Та сарадња институционализована је кроз Организацију уједињених нација и бројне друге међувладине организације које се баве терористичком претњом. Резолуцијом Савета безбедности Уједињених нација 1368 међународни тероризам класификован је као претња међународном миру и безбедности (Security Council Resolution 1368, 2001). Генерална скупштина ОУН усвојила је 2006. године и Глобалну контратерористичку стратегију (*General Assembly Resolution 60/288*, 2006), која се ажурира на сваке две године (*United Nations Global Counter-Terrorism Strategy, 8th review of the Strategy*), пратећи трендове у развоју терористичке претње. Оно што изискује глобалну сарадњу у борби против тероризма јесу његова динамичност, адаптивност, транснационално деловање и честе промене у тактикама регрутовања, а напори за сузбијање радикализације и тероризма јесу „снажно повезани са тачним и благовременим прикупљањем и разменом обавештајних података између безбедносних агенција са и широм света” (Akinlabi, Alade, 2024: 31). Међународна сарадња пружа додатни подстицај владиним агенцијама да, радећи једни са другима, подигну ниво своје будности и припремљености за препознавање и елиминисање терористичких претњи.

Глобални форум за борбу против тероризма (*GCTF*) највећа је неформална иницијатива која окупља доносиоце политичких одлука и стручњаке широм света, како би разменили искуства, анализирали слабости, развијали јавно доступне алате за супротстављање тероризму и смањили рањивост људи широм света на тероризам. На регионалном нивоу, Европска унија има мноштво корисних иницијатива у области међународне сарадње против тероризма. Тако је у оквиру Европола 2016. године основан Европски центар за борбу против тероризма (*Europol European Counter*

Terrorism Centre – ECTC), као централни аналитички и оперативни центар Европола за борбу против тероризма. Усмерен је на координацију истрага и размену оперативних информација, као што су информације о претњама, плановима, терористичким групама, логистици, финансирању, аналитички извештаји. Ове информације користе националне полиције и остале партнерске организације у својим свакодневним оперативним и тактичким задацима. У оквиру Европола креиран је и канал за безбедну размену поверљивих података између агенција безбедности различитих држава, платформа СИЕНА (*Secure Information Exchange Network Application – SIENA*), која представља технолошки механизам за безбедну и заштићену међуагенцијску размену оперативних података. Поред осталих облика криминала, она је и најбржи механизам за размену оперативних података о терористичкој претњи, уз строга правила – шифрована мрежа, различити нивои приступа и обавезна верификација идентитета учесника.

Споразум из немачког града Прима (*Prüm Treaty, 2005*) дао је основ за још једну корисну иницијативу ЕУ која омогућава аутоматизовану размену података ДНК профила, отисака прстију, података о возилима држава чланица и организацији великих догађаја, како би се спречила и терористичка кривична дела. Споразум првобитно потписан само између неколико европских земаља пренесен је у оквиру ЕУ кроз одлуку Савета ЕУ из 2008. године (*Council Decision 2008/615/JHA, 2008*). У појединачним случајевима и уз одређена ограничења, државе чланице у циљу спречавања тероризма могу једна другој доставити следеће податке: презиме и име, датум и место рођења, опис услова који доводе до претпоставке да ће бити учињена кривична дела (*EUR-Lex, 2025*).

Директива Европског парламента и Савета ЕУ 2016/681 под називом Директива о евиденцији имена путника (*Passenger Name Record Directive – PNR, 2016*) акт је који омогућава државама чланицама да благовремено идентификују сумњиве путнике и потенцијалне терористичке активности тако што обавезује авиопревознике да прикупљају податке о путницима у авио-превозу и чувају их, уз обавезу дељења података надлежним органима ради

спречавања, откривања, истраге и гоњења тероризма и озбиљних криминалних дела (Directive [EU] 2016/681 of the European Parliament and of the Council).

Европол је 2005. покренуо и Информациони систем Европола (*The Europol Information System – EIS*), који представља централну базу Европола са оперативним и обавештајним подацима о свим облицима криминала, укључујући и тероризам. Систем садржи информације о тешким међународним злочинима, осумњиченим и осуђеним лицима, криминалним структурама и кривичним делима и средствима која се користе за њихово извршење. Државама ЕУ које су део Шенгенског простора на располагању је још један механизам који агенцијама омогућава брзу претрагу и размену упозорења о различитим облицима прекограничних претњи, па и о осумњиченима за тероризам и њиховим активностима у реалном времену – Шенгенски информациони систем II (*Schengen Information System II – SIS II*). Први шенгенски информациони систем (SIS) настао је у оквиру Шенгенског споразума и Шенгенске конвенције из 1990. године, а модернизовану верзију (*SIS II*) развила је и одржава Европска комисија (Директорат за миграције и унутрашње послове), уз техничко управљање Агенције Европске уније за оперативно управљање великим ИТ системима у области слободе, безбедности и правде (*eu-Lisa*). То је централизована база која садржи оперативна упозорења о траженим лицима, фалсификованим документима и украденим возилима, и не служи за даљу комуникацију и размену података, већ искључиво за примање или слање брзог упозорења које је видљиво осталим корисницима.

Директорат за миграције и унутрашње послове ЕУ основао је 2011. године још једну, за контратероризам, а пре свега антитероризам, важну иницијативу за подизање свести о радикализацији (*Radicalisation Awareness Network – RAN*), и она укључује мрежу стручњака који свакодневно раде са онима који су рањиви на радикализацију или су већ радикализовани (представници цивилног друштва, социјални радници, млади, наставници, здравствени радници, представници локалних власти, полицајци и затворски службеници). Мрежа повезује практичаре, омогућава размену добрих

пракси, публикује едукативна издања и, за разлику од претходно наведених иницијатива, представља платформу за размену знања, а не оперативних информација.

С обзиром да технолошки напредак користе и терористи, мењајући свој *modus operandi*, Европска комисија је у децембру 2015. године покренула ЕУ интернет форум (*EU Internet Forum – EUIF*) који спроводи сарадњу са технолошким компанијама ради лакшег отклањања терористичког и екстремистичког садржаја са интернета. Њихов задатак је да смање, односно онемогуће приступ онлајн терористичким садржајима и повећају обим ефикасних алтернативних наратива на интернету. Активности Форума касније су, због своје ефикасности, проширене и на борбу против сексуалног злостављања деце на мрежи (од 2019. године), трговину дрогом на мрежи и трговину људима на мрежи (од 2022. године) (https://home-affairs.ec.europa.eu/networks/european-union-internet-forum_en).

Такође, постоји и Европска база података терористичких преступника (*European Database of Terrorist Offenders*) која садржи податке о осуђеним терористима у ЕУ од 2012. године и служи као регистар за праћење лица који представљају претњу. Што се правосудне сарадње тиче, у оквиру Евроцаста је 2019. године креиран правосудни контратерористички регистар (*Eurojust Judicial Counter-Terrorism Register – JCTR*) на основу одлуке Савета ЕУ 2005/671/ЈНА. Овај регистар намењен је тужилаштвима и судовима држава чланица за размену података о активним истрагама и кривичним поступцима у области тероризма, са свим детаљима везаним за рокове, процедуре и слично. Његова предност је у томе што омогућава потпун и правовремен увид у све сегменте кривичног гоњења без пропуста у виду фрагментисане и непотпуне размене података.

Европска унија је, када је реч о међународној сарадњи у борби против тероризма, препознала значај и спољне димензије контратероризма, па је 2022. године покренула пројекат *CT JUST (Counter-Terrorism and Justice Project)* у оквиру инструмента за спољне послове и безбедносну сарадњу (*EU Foreign Policy Instrument – FPI*) и Програма за спречавање тероризма и организованог криминала у партнерским земљама. Циљ те иницијативе јесте да ојача

капацитете правосуђа партерских земаља у области борбе против тероризма, па она укључује: помоћ око унапређења нормативног оквира и усклађивање са међународним стандардима, обуку судија и тужилаца у области истрага и гоњења терористичких активности, обуку за прикупљање и чување дигиталних доказа, размену пракси и успостављање контакт тачака између држава партнера и Евроцаста. Укратко, иницијатива тежи развијању и јачању резилијентности партнерских земаља на терористичку претњу. Једна од конференција под окриљем ове иницијативе, одржана у фебруару 2025. године, показала је завидан ниво развијености техничке сарадње између институција ЕУ и земаља представника Арапске лиге (European Commission, 12 February 2025, https://fpi.ec.europa.eu/news/strengthening-international-judicial-cooperation-counterterrorism-key-takeaways-high-level-2025-02-12_en). Такође, унутар овог пројекта развијена је посебна иницијатива за унапређење поверења и сарадње између обавештајних, правосудних и истражних структура широм Африке, под називом *SPHINX* (European Commission, 28 May, 2025, https://fpi.ec.europa.eu/news/strengthening-counter-terrorism-partnerships-africa-2025-05-28_en). Ова иницијатива, коју ЕУ оцењује као пример људскоцентричног приступа контратероризму, служи не само за размену стручних знања о методологији обраде доказа и праћење финансијских токова тероризма, већ и за свеобухватно унапређење правног и институционалног оквира који је способан да решава узроке и поштује стандарде људских права у афричким земљама.

Поред Организације уједињених нација, као кровне организације која даје нормативни и етички оквир за борбу против тероризма, и ЕУ као регионалног лидера који креира инфраструктуру и културу у области антитероризма, пракса је показала да, када дође до потребе за оперативним поступањем, ЕУ често нема задовољавајуће техничке капацитете и разрађене процедуре поступања и често се за техничко спровођење операција ослања на НАТО. Стога је и НАТО, као део глобалне мреже за борбу против тероризма, усвојио Политику за борбу против тероризма (*NATO Policy Guidelines on Counter-Terrorism*, 2012, ревидирана 2021), која се за-

снива на три принципа: *свесности, њревенција и одбрана*. Оперативна сарадња обухвата размену обавештајних података, заједничке вежбе, унапређење заштите критичне инфраструктуре и подршку партнерским државама кроз програм Иницијатива за изградњу одбрамбених капацитета (*Defence Capacity Building Initiative – DCBI*).

Глобална контратерористичка сарадња је неопходна, али исто тако суочена са бројним изазовима и препрекама које је потребно постепено превазилазити, попут различитих културалних приступа тероризму, те очитом недостатку консензуса о дефиницији, идеологији, приоритетима, а самим тим и нормативним оквирима који отежавају практичну сарадњу у погледу хапшења, екстрадиције и кривичног гоњења лица повезаних са тероризмом. За разлику од терориста, који немају избора, јер уколико желе да преживе морају радити на својој динамичности и адаптивности, владине агенције су и даље „инхерентно бирократске и реактивне”, спорије се мењају, прилагођавају и често касно реагују (Hoffman, Ware, 2020). Циљ је да државе ојачају своје капацитете тако да не поступају само реактивно, реагујући на инциденте, него да буду оспособљене да предвиде претњу, координирају одговоре и континуирано предузимају превентивне мере, а одговор ускладе са елементарним стандардима поступања, поштујући људска права.

Изазови и предности полицијске дипломатије у борби против тероризма

Тероризам је адаптиван и променљив, док подаци о безбедносним структурама, пре свега о полицији, не говоре исто о њима. Наиме, полиције широм света и даље примењују своје традиционалне, застареле приступе у борби против тероризма, које се фокусирају на елиминисање лидера терористичких организација и група, организациону логистику и финансирање, што данас постаје непримењиво и бескорисно за покрете у којима нема идентификованих вођа, нема постојеће организације и нема инфраструктуре коју би требало урушити (Hoffman, Ware, 2020).

Полиција и остали субјекти који учествују у борби против тероризма морају развити капацитете за брже прилагођавање новим околностима, а полицијска дипломатија има добре предуслове да унапреди ову адаптивност. Основна претпоставка од које се полази у овом раду јесте да је полицијска дипломатија алат у сузбијању тероризма (Кекић, Никач, 2011) и да представља инструмент превазилажења бројних препрека у глобалној контратерористичкој сарадњи, и то кроз културолошко равнање и развијање поверења. Блок (*Block*) дефинише шест основних категорија разлога који руше поверење у полицијској сарадњи: корупција, супротстављени интереси полицијских агенција у датом моменту, различито дефинисане законске обавезе, ограничени ресурси, бирократске препреке и различити стандарди (Block, 2017: 21). Поверење се у полицијској сарадњи сматра социјалним механизмом за решавање проблема ризика, и то кроз механизме очекивања и посвећености (Block, 2017: 15). Наиме, размена најважнијег ресурса у раду полицијских агенција и губљење потпуне контроле над тим ресурсом кроз процес дељења чини онога ко дели информације рањивим, а једна од стратегија која се предлаже како би овај ризик био умањен јесте и постојање посредника од поверења у форми официра за везу (Block, 2017: 27).

Стога, као најважнији задаци полицијске дипломатије, поред размене најбољих полицијских пракси и омогућавања техничких, оперативних предуслова рада полицијама широм света, јесу и културолошко и цивилизацијско приближавање, те боље разумевање различитих култура, социолошких особености, идеологија и социјалних услова који утичу на перцепцију тероризма и одређују контратерористичке праксе држава.

Поред тога, савремене полицијске праксе, укључујући и контратерористичке, морају уважити потребу за адаптивним приступима борби против тероризма, који су фокусирани пре свега на добробит заједнице и који једнак приоритет дају безбедности и грађанским слободама, као и глобалној сарадњи у размени обавештајних података и изградњи капацитета (Gray, 2024: 62, 63). Истраживања доступна из демократских, западних земаља показују

да је јавност све мање толерантна на „разлоге безбедности” у ограничавању њихових грађанских и људских права и слобода (Gallup, 2025). Кофи Анан је као генерални секретар ОУН још 2005. у једном свом обраћању истакао:

„Поштовање људских права није само компатибилно са успешном стратегијом борбе против тероризма. То је суштински елемент контратероризма. Тероризам је сам по себи директан напад на људска права и владавину права. Ако их жртвујемо у нашем одговору, предаћемо победу терористима” (United Nations Secretary General, 2005).

Полицијска дипломатија, дакле, поред свих наведених изазова, има потенцијал да постигне значајне стратешке резултате који ће оперативну сарадњу полиција широм света учинити ефикаснијом и продуктивнијом. Срж полицијске дипломатије јесте рад на поверењу и већој транспарентности, разумевању и усаглашавању пракси, те „културолошком равнању” које се дешава кроз заједничко суочавање са истом претњом. Полицијска дипломатија може бити чак и „пионир за успостављање и развој добрих дипломатских односа између држава” те у томе често ићи и испред политике, односно опште дипломатске сарадње између држава (<https://www.rts.rs/lat/vesti/politika/756872/znacaj-policijske-diplomatije.html>, доступно 18. марта 2025).

Студија случаја: Полицијска дипломатија у борби против тероризма – сарадња Европола и ФБИ-ја у борби против ИСИС-а

Праксе полицијске дипломатије имају дугу историју, али пример најразвијенијих полицијско-дипломатских односа јесте сарадња ЕУ и САД, нарочито након 11. септембра (видети: Кекић, Никач, 2011: 423), док је свој зенит ова сарадња доживела након успона ИСИС-а 2014. године. Заједничка борба евроатлантске заједнице против терористичке претње која долази са периферије учврстила је идентитет ове заједнице заснован управо на тој улози. Иако се ради о цивилизацијски блиским културама, правне тра-

диције су им различите, и то је био један од важних изазова њихове сарадње. Иако су стратешки (2001) и оперативни (2002) споразум између Европола и САД веома контроверзни, посебно због разлика у стандардима заштите података, оцењује се да је однос Европола са САД добро напредовао и да обе стране имају користи од тога (Cocq, Galli, 2017: 145). Сем тога, и ови иницијални споразуми, као и други правни механизми који ће касније представљати нормативни основ продубљивању сарадње, уследили су као резултат развијања дипломатског поверења, међусобних посета и меморандума о разумевању те неформализоване размене информација и искустава без потпуног и детаљног правног оквира.

Службеници за спровођење закона који делују у дипломатском својству у иностранству, тзв. правни аташеи ФБИ-ја (*Legats*), акредитовани су још од четрдесетих година прошлог века при америчким амбасадама широм Европе, укључујући и Евроазију и Источну Европу (Берлин, Брисел, Лондон, Париз, Хаг, Берн, Копенхаген, Мадрид, Рим, Беч, Анкара, Атина, Букурешт, Кијев, Праг, Софија, Варшава, Астана, Београд, Будимпешта, Москва, Рига, Тбилиси) (FBI, 2025). И остале агенције за спровођење закона имају своје официре за везу при седишту Европола у Хагу, који, иако према америчким законима имају дипломатски статус, имају такође и оперативна овлашћења, а унутар Европола се за њих користи назив „официри за везу”, који је уобичајен за оперативне представнике. Према подацима из 2016. године, у седишту Европола, поред представника ФБИ-ја, налазили су се представници других америчких органа: Биро за алкохол, дуван, ватрено оружје и експлозиве (*US ATF*), Царина и заштита границе (*US CBP*), Управа за сузбијање дрога (*US DEA*), Служба дипломатске безбедности (*US DS*), Управа за храну и лекове (*US FDA*), Служба за имиграцију (*US ICE*), Пореска служба (*US IRS*), Управа за безбедност саобраћаја (*US TSA*), Тајна служба (*US SS*) и Департман њујоршке полиције (*US NYPD*) (Caudron, 2018).

У контексту контратерористичке сарадње између САД и ЕУ, извештаји говоре да је већ након терористичког напада 11. септембра 2001. године ЕУ појачала своје дипломатске активности са америчким колегама у домену полиције, правосуђа и гранич-

не контроле. Од тада, генерални тужилац САД, државни секретар и секретар за унутрашњу безбедност састају се на министарском нивоу са колегама из ЕУ најмање једном годишње, а на сваких шест месеци састаје се и радна група САД-ЕУ, састављена од високих званичника, како би се разговарало о полицијској и правосудној контратерористичкој сарадњи. Непосредно након напада 11. септембра и ЕУ је основала радну групу стручњака за борбу против тероризма, смештену у Европолу и састављену од представника полиције и обавештајних служби из сваке државе чланице, како би се побољшала комуникација међу овим службама и радило на вези са америчким колегама. Ова радна група поново је активирана након терористичких бомбашких напада у Мадриду 2004. ФБИ је већ тада најавио слање свог аташеа у Хаг, а Тајна служба САД именовање особе за везу са Европолем која ће радити на питањима фалсификата. Два официра за везу Европола послата су у Вашингтон 2002. године. Паралелно са полицијском сарадњом (оперативном и стратешком), развијала се и правосудна сарадња кроз Евроцаст, а представници САД су наводно позвани да присуствују састанцима шефова јединица ЕУ за борбу против тероризма (CRS Report for Congress, 2004). Све ове дипломатске активности резултирале су продубљивањем сарадње између САД и ЕУ и потписивањем споразума о размени стратешких и оперативних информација.

Наиме, 6. децембра 2001. године потписан је званични споразум између Европола и САД о стратешкој и техничкој сарадњи који је омогућио размену стратешких информација о процени претњи, трендовима, обрасцима криминала. Овај споразум није могао да укључи размену оперативних података, јер у том тренутку ЕУ закони о заштити података и приватности то нису омогућавали, али када је ЕУ створила правне и институционалне механизме, већ 2002. године потписан је допунски споразум, који је омогућио и оперативну сарадњу, односно размену личних података као што су имена и идентитет осумњичених, али и мере заштите тих података (видети: Statewatch, 2002). САД и Европол су тиме постали оперативни партнери, али се сарадња и даље одвијала контролисаним каналима и постепено. Споразум између САД и Европске

уније о коришћењу и преносу података из евиденције имена путника из ЕУ у Министарство за националну безбедност САД (*The EU-U.S. Passenger Name Record [PNR] Agreement*) ступио је на снагу 1. јула 2012. године, омогућивши праћење путника у ваздушном саобраћају осумњичених за везе са тероризмом (PNR, 2012). ФБИ сарађује са Европолом и појединачним државама чланицама и кроз постојећи шири правни оквир о узајамној правној помоћи између САД и ЕУ, а ФБИ делује под окриљем Канцеларије за међународне послове Министарства правде САД, преко које се овакви захтеви упућују. Овим споразумима се регулишу питања заједничких истражних тимова, омогућавају се прекогранично прикупљање доказа и екстрадиција између САД и земаља ЕУ, захтевају се телефонски записи, финансијске трансакције и сведочења од других јурисдикција у случајевима тероризма, као и процесуирање осумњичених за тероризам који су ухапшени у Европи, тако што се омогућава пренос доказа америчким судовима. Први у низу ових споразума ступио је на снагу 2003. године (*Agreement on mutual legal assistance between the European Union and the United States of America*, 2003).

Важан сегмент борбе против тероризма из перспективе САД било је праћење токова новца. Зато је америчко министарство финансија покренуло Програм за праћење финансирања тероризма (*TFTP*) како би пратило токове новца терориста и помогло ширим напорима владе САД да открије терористичке ћелије и мапира терористичке мреже код куће и широм света. Аналитичари ФБИ-ја рачунали су на обавештајне податке финансијске природе прибављене од стране Европола о идентификованим сумњивим банковним активностима које би указивале на трансфере новца између различитих ћелија ИСИС-а у различитим земљама, и на прослеђивање таквих података властима САД. Међутим, за овакву активност био је потребан прецизан правни оквир у виду споразума. Након неколико неуспелих покушаја у периоду од 2006. до 2010. да се постигне споразум између САД и ЕУ о приступу *SWIFT* подацима за праћење финансирања тероризма (разлози су били својствени нормативи ЕУ и укључивали су забринутост за приватност, пропорционалност и реципроцитет),

Споразум о Програму за праћење финансирања тероризма (*TFTP*) између ЕУ и САД постигнут је у јануару 2010. године, али је касније стављен ван снаге (*Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program, 2010*). Споразум је суспендован због извештаја по којима су америчке безбедносне службе кршиле мере заштите приватности и замењен је споразумом о узајамној правној помоћи (*MLA*), који олакшава размену података, али се за приступ финансијским подацима ослања на националне законе појединачних држава чланица ЕУ (*SWIFT: European Parliament votes down agreement with the US, 2010*).

За Европску унију успон ИСИС-а донео је нове изазове, нарочито узимајући у обзир серију терористичких напада у Европи 2015. године. САД су врло озбиљно схватиле ову претњу и још чвршће се повезале са Европом у контратерористичким напорима. Током јануара 2014. године у Хагу је одржан важан састанак Европола и ФБИ-ја на највишем нивоу, а тема је била анализа капацитета Европола за сузбијање тероризма и организованог криминала и могућности за интензивнију сарадњу (*EuroPol, January 31, 2014*). Први трајни официр за везу ФБИ-ја при Европолу постављен је 21. маја 2015. године (*EuroPol Annual Review, 2015*) и тако је омогућено стално и директно комуницирање у реалном времену. Његово постављање је значајно допринело убрзању и поједностављењу сарадње између Европола и ФБИ-ја, посебно у време усложњавања терористичке претње коришћењем интернет технологије за постизање терористичких циљева.

Схвативши да много страних држављана индоктринираних идеологијом радикалног ислама одлази на жаришта сукоба да ратује за Исламску државу, ФБИ и Европол потписали су у Вашингтону 2016. године међусобни споразум који ће значајно интензивирати заједничку борбу против страних бораца. Свесни опасности коју носи мрежа таквих бораца (искусних, обучених, оспособљених за ширење екстремистичких идеја и за организацију и планирање напада по повратку у САД и земље Европе), ФБИ је на осно-

ву споразума добио могућност да се прикључи Европоловој фокалној групи „Путници” (*Travellers*). Група данас функционише као један од тимова за аналитичке пројекте од интересовања за Европол (видети: *Europol Analysis Projects*, 2025), а састављена је од стручњака и аналитичара који координирају истраге држава чланица ЕУ о страним борцима. Ова група омогућила је да се заједничким обавештајним и оперативним деловањем ФБИ-ја и Европола идентификује и испрати сваки сумњив повратак потенцијалних терориста из Сирије и Ирака у земље ЕУ и партнерске земље, као и да се евидентирају и спрече активности терористичких ћелија и „ћелија спавача” (*European Union Terrorism Situation and Trend Report*, 2019: 25). Европски контратерористички центар при Европолу, чији је поменута група део, има и Јединицу ЕУ за праћење интернет пропаганде (*EU IRU*) основану такође 2015. Године, која координира напоре ЕУ у борби против приступа онлајн терористичкој пропаганди и пружа оперативну онлајн подршку за случајеве борбе против тероризма. Ова јединица прати и пријављује терористички и екстремистички интернет садржај и тесно сарађује са интернет компанијама и страним провајдерима ради његовог уклањања.

Пре него што је Европол креирао организационе и правне оквире стратешке и оперативне размене података, ФБИ је још 2013. године у Јордану започео операцију „Племенити феникс” (*Operation Gallant Phoenix*), заједничку међународну обавештајну иницијатива коју је осмислио САД, уз учешће бројних држава, укључујући НАТО земље и земље ЕУ. Њена основна замисао јесу прикупљање, анализа и размена података о страним борцима, посебно оним повезаним са ИСИС-ом и другим екстремистичким групама. Ова операција је још један од примера сарадње ФБИ-ја и Европола, с обзиром на то да је Европол према расположивим подацима послао у ту операцију свог аналитичара 16. августа 2017. године и да размену информација има искључиво са ФБИ-јем, на начин који је регулисан међусобним споразумом. Подаци се, у складу са регулативом ЕУ, користе за превентивне сврхе, како би се благовремено адресирале потенцијалне претње унутар граница ЕУ (<https://www.europarl.europa>).

eu/RegData/questions/reponses_qe/2018/000009/P8_RE(2018)000009_EN.pdf, доступно 4. октобра 2025).

ФБИ и Европол радили су у заједничкој акцији и на разбијању пропагандних мрежа и гашења кључних онлајн канала, мобилних апликација и осталих веб-садржаја које је ИСИС користио – Амак (*Amaq*), радио Ал Бајан (*Al-Bayan*), Халуму (*Halumu*), Нашир вести (*Nashir news*). У јуну 2017. године садржај медија Амак је компромитован и заплешени су им сервери, што је омогућило идентификацију радикализованих појединаца који су тај садржај делили и користили у преко сто земаља. У поновљеној акцији између 25. и 26. априла 2018. године, координираној од стране Европолове јединице за праћење интернет пропаганде (EU IRU), ови канали били су готово у потпуности онеспособљени (Europol, April 27, 2018), чиме су способност и капацитет ИСИС-а да регрутује нове чланове драматично смањени. ФБИ помаже Европолу техничким методама прикупљања обавештајних података и учествовањем у конкретним и континуираним акцијама разбијања терористичке критичне инфраструктуре онлајн, о чему сведоче и најновије акције из 2024. године (Europol, June 14, 2024). На овај начин се најефикасније и најбезбедније спречавају терористичка пропаганда и онлајн комуницирање које одржава живим терористичке мреже широм света.

Такође, према извештајима Европола, број ухапшених терориста се између 2015. и 2018. године удвостручио, а половина ухапшених повезана је са терористичким деловањем ИСИС-а (European Union Terrorism Situation and Trend Report, 2019: 15). ФБИ је дао Европолу имена преко 4500 појединаца притворених на североистоку Сирије, а листа је унета у Шенгенски информациони систем, што европским државама омогућава да идентификују те особе уколико покушају да пређу границу ЕУ (De Kerchove, Onidi, 2021). Најзад, размена обавештајних података била је и кључни помоћни механизам војних акција које су у октобру 2019. године резултирале елиминацијом Абуа Бакр ел Багдадија, вође ИСИС-а, и уништењем калифата (De Kerchove, Onidi, 2021).

Ипак, сарадња која је донела доста резултата није била без изазова. Највећи је свакако био развијање заједничких протокола за руковање оперативним и обавештајним подацима како би се помирили различити правни стандарди у области контратероризма између САД и ЕУ, односно проналажење равнотеже између прешироких овлашћења служби безбедности, које је предвидео амерички Патриотски закон из 2001. (*USA PATRIOT Act*), и регулативе ЕУ. Главни документ у ЕУ који регулише заштиту приватности података о личности и начине на који се ти подаци могу делити са трећим државама јесте ЕУ ГДПР (*General Data Protection Regulation – GDPR*), који је ступио на снагу 2018. године (*Regulation [EU] 2016/679*). Посебан документ којим се регулишу правила о заштити података о приватности само за Европол (*Regulation [EU] 2016/794*) усаглашен је са њим. Регулатива 2016/794 обавезује Европол да сме да дели податке са трећим државама само ако је ова активност претходно регулисана посебним споразумом и ако је у земљи примаоцу обезбеђен једнак ниво заштите као у ЕУ. Такође, мора бити обезбеђен принцип „минимализације података“, односно да подаци буду стриктно ограничени на конкретне податке из конкретног случаја, и најзад, европски надзорни орган за заштиту података (*European Data Protection Supervisor – EDPS*) мора контролисати те процесе (видети: *Regulation [EU] 2016/794*). *EDPS* је 2017. године преузео све надлежности надзора обраде личних података од Европоловог надзорног тела (*Europol Joint Supervisory Body – JSB*), које је до тада надзирало обраду личних података унутар Европола у складу са Конвенцијом о оснивању Европола из 1995. године ([https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:41995A1127\(01\)](https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:41995A1127(01))).

Европска комисија има овлашћење да утврди, на основу члана 45 Уредбе (ЕУ) 2016/679, да ли земља ван ЕУ са којом се лични подаци размењују нуди адекватан ниво заштите података, еквивалентан ономе који обезбеђује ЕУ (*Adequacy decisions*, 2025). Како САД немају признат адекватан ниво заштите података од стране Европске уније у области размене података у сектору спровођења закона, јер се уз општи акт (ЕУ) 2016/679 на њу примењује и посебна директива (*Law Enforcement Directive – LED [Directive (EU) 2016/680]*), ФБИ и Европол

морају стално балансирати између безбедности и приватности. То подразумева да се размена оперативних података врши на основу билатералног споразума уз прецизиране услове размене утврђене додатним актом: који органи обе стране имају приступ подацима, које су то категорије података, како се подаци достављају и чувају и под којим условима се бришу, ко одобрава приступ подацима, која комуникациона средства се користе за њихову безбедну размену и како се евиденција размене документује и контролише. Службени канал или формална контакт тачка преко које се размена између ФБИ-ја и Европола формално спроводи јесте акредитовани официр ФБИ-ја у Хагу који платформу СИЕНА може користити за контакте са јединицама широм Европе.

Остварени резултати дипломатских напора корисни су и плодносни. Ипак, кључни изазови који остају отворени односе се на усаглашавање критеријума приватности актера који деле информације, с обзиром на то да стриктна регулатива ЕУ ограничава обим личних података који се могу делити са ФБИ-јем. Уколико се ови критеријуми не приближе, то може отворити додатне спорове око тога како се лични подаци чувају, складиште и користе, а нарочито у контексту терористичке претње у успону – десничарског тероризма, јер о његовим кључним елементима постоји озбиљно неслагање између САД и ЕУ (Leidig, Van Mieghem, 2021). На поверење и одлуку да се сарадња интензивира утичу и политички разлози и забринутост многих европских земаља да САД може угрожити њихову сувереност, те да се ослањање на америчке обавештајне податке у овом моменту може сматрати рањивошћу (Washington Post, June 5, 2025). Разлике у правним системима такође стварају проблеме у процесима попут екстрадиције, јер према споразуму о екстрадицији између САД и ЕУ земље ЕУ могу одбити екстрадицију уколико осумњиченом прети смртна казна (Agreement on extradition between the European Union and the United States of America, 2003. [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22003A0719\(01\)&qid=1760397390588](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22003A0719(01)&qid=1760397390588), доступно 3. октобра 2025).

Улога полицијског аташеа ФБИ-ја у нормативном и организационо-функционалном равнању партнерских земаља јесте зна-

чајна, и сви успостављени механизми, праксе и алати развијени су на темељима изградње контаката, повезивања и поверења. Предност аташеа у области тако деликатној као што је сарадња у унутрашњим пословима и размена осетљивих података лежи у томе што је он у могућности да гради и одржава поверење кроз личне (*face-to-face*) контакте са страним званичницима и безбедносним агенцијама и повезује их са другим агенцијама. Поред координације међународних истрага у којима је партнер САД, оперативне размене информације помоћу платформе СИЕНА, повезивања са другим међународним организацијама и осталих дипломатских мера на омогућавању и олакшавању оперативне сарадње, аташеи ФБИ-ја јесу и стратеги који процењују политичку и безбедносну климу и у складу са тим дају ситуационе извештаје и препоруке. Ништа мање важна у том смислу није ни њихова улога у координацији специјализованих обука и тренинга ФБИ-ја и партнера с циљем уједначавања пракси и неговања владавине права.

Закључак

Различити национални интереси, правне традиције и друштвени ставови према питањима приватности личних података и криминалу и кажњивости генерално, уочени су као највећи изазови у сарадњи држава у решавању заједничких проблема безбедности. Дипломатија генерално, а нарочито полицијска дипломатија (врло уска и специфична форма деловања), препозната је као важан алат да се ови изазови савладају успешније и са више поверења, које је камен темељац за надоградњу и олакшавање сарадње. Како поверење није нешто што се подразумева, нарочито када је реч о размени најосетљивијих оперативних података, неопходно је радити на њему кроз развијање заједничке одговорности и моралних обавеза, односно кроз посвећеност мултилатералним нормама, конзистентност и реципроцитет (Ramel, 2025).

Поверење које директни контакти стварају довели су до унапређења оперативних резултата, па се тако према подацима из интервјуа директора ФБИ-ја из 2018. године контратероризам наводи

као једна од најуспешнијих области сарадње, на основу тога што је размена обавештајних података о осумњиченим терористима и страним борцима између САД и Европола повећана за 30% у само једној години (Caudron, 2018). Истовремено, размена обавештајних и оперативних података била је један од главних практичних изазова и стога један од кључних циљева полицијске дипломатије, како би се остварили остали циљеви контратероризма: разбијање финансијерских мрежа повезаних са ИСИС-ом, откривање, праћење и онемогућавање интернет пропаганде и врбовања и олакшавање екстрадиције и кривичног гоњења осумњичених за тероризам у различитим јурисдикцијама. Заједничке вредности чиниле су темељ овог односа, док су разлике у законима о приватности, заштити слободе говора и другим правним оквирима подстакле америчке и европске званичнике да критички и креативно размишљају о новим начинима решавања проблема (De Kerchove, Onidi, 2021).

Дипломатске праксе, поред свега наведеног, имају и шири значај јер формалне и редовне билатералне посете, мултилатерални форуми попут учешћа на Европоловој Заједничкој годишњој конференцији о тероризму и пропаганди (*ECTC Advisory Network on Terrorism and Propaganda Conference*), подстичу и неформалне облике сарадње. Тако се око најновијих дипломатских активности као врста подршке окупљају и истраживачи, научници и приватне технолошке компаније и креира се мрежа професионалаца и истраживача који деле теоријска знања, практична искуства и технолошке иновације, дугорочно унапређујући контратерористичку резилјентност држава и њених грађана.

Полицијска дипломатија има снажан потенцијал да направи мост између колективног контратерористичког деловања и унилатералног или билатералног деловања држава. Може се слободно констатовати да су се полицијско-дипломатске праксе и правни оквир сарадње међусобно конституисали и надограђивали, а да је полицијска дипломатија одиграла кључну улогу у сарадњи Европола и ФБИ-ја, од терористичких напада 11. септембра, преко заједничких операција елиминисања ИСИС-а, па до разбијања онлајн канала пропаганде данас. Полицијска дипломатија је увек

претходила споразумима о оперативној или стратешкој сарадњи, а полицијске дипломате су логистички посредник и кључна спона у размени обавештајних података, оперативној координацији и правној хармонизацији између различитих националних агенција за спровођење закона. Након постављања правних аташеа ФБИ-ја и официра за везу других америчких агенција контратерористичка сарадња је интензивирана, праћена институционалним развојем, новом правном регулативом и конкретним практичним резултатима као што је разбијање терористичке мреже ИСИС-а и његове инфраструктуре. Најзад, Европа и САД налазе се пред новим терористичким изазовима, попут успона десничарског тероризма, који ће размену података ставити пред нове изазове, а самим тим и дати неке нове задатке полицијској дипломатији на терену. Наиме, дипломате морају радити на универзализацији дефиниције десничарског тероризма и постизања консензуса око услова за уклањање говора мржње и терористичког садржаја на интернету (видети: De Kerchove, Onidi, 2021).

Полицијска дипломатија дала је кључни допринос и замајак трансформацији од *ad hoc* сарадње ка једном организованом, структурираном партнерству. Праксе полицијске дипломатије допринеле су јачању међусобног поверења, унапређењу правног оквира и пракси размене обавештајних и оперативних података, олакшале су координацију заједничких операција Европола и ФБИ-ја и као резултат донеле разбијање мреже ИСИС-а, процесуирање терориста и спречавање бројних напада који су се могли десити у Европи. Поменути изазови који се односе на приватност података и питања нормативног усаглашавања и вредносног равнања остају предмет интересовања држава које деле интерес у борби против тероризма и других облика криминала. Полицијска дипломатија ће се несумњиво развијати у правцима развоја нових технологија и наставиће да буде спона за помирење разлика и лакшу комуникацију у корист свих повезаних страна.

Литература

1. Adequacy decisions, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en, доступан 3. октобра 2025.
2. Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program (2010). [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22010A0113\(01\)](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22010A0113(01)), доступан 1. октобра 2025.
3. Agreement on extradition between the European Union and the United States of America (2003). [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22003A0719\(01\)&qid=1760397390588](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22003A0719(01)&qid=1760397390588), доступан 3. октобра 2025.
4. Agreement on mutual legal assistance between the European Union and the United States of America (2003). [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22003A0719\(02\)&qid=1759957778063](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22003A0719(02)&qid=1759957778063), доступан 1. октобра 2025.
5. Akinlabi, O.E., Alade, A. (2024). Contemporary Challenges in Counterterrorism: Identifying and Addressing Gaps at National and International Level. *Berkeley Journal of Humanities and Social Science*, 5(6): 25–38.
6. Bigo, D. (2002). Liaison officers in Europe: New officers in the European security field. In *Issues in transnational policing*, pp. 67-99. Routledge.
7. Block, L. (2010). Bilateral police liaison officers: Practices and European policy. *Journal of Contemporary European Research*, 6(2): 194–210.
8. Block, L. (2017). Establishing Trust Despite the Risks? An Analysis of the Need for Trust in Police Cooperation, in: Saskia H. and Carole M. (eds.). *Trust in International Police and Justice Cooperation*. Hart Publishing, pp. 13–29.
9. Waldbauer-Hable, P.C. (2023). Diplomats in Uniform: ‘Security Diplomacy’ Described Through a Practical Experience Report. In:

- Onditi, F., McLarren, K., Ben-Nun, G., Stivachtis, Y.A., Okoth, P. (eds) *The Palgrave Handbook of Diplomatic Thought and Practice in the Digital Age*. Palgrave Macmillan, Cham, pp. 501–519.
10. Washington Post (June 5, 2025). Europe worries about its dependence on U.S. intelligence under Trump, <https://www.washingtonpost.com/world/2025/06/05/europe-cia-intelligence-sharing/>, доступан 5. октобра 2025.
 11. Влада Републике Србије (2025). Полицијски аташеи доприносе јачању билатералне полицијске сарадње, 23. јануар 2025, <https://www.srbija.gov.rs/vest/853741/policijski-atasei-doprinosе-jacanjubilateralne-policijske-saradnje.php>, доступан 14. септембра 2025.
 12. Gallup (2025). Terrorism. <https://news.gallup.com/poll/4909/terrorism-united-states.aspx>, доступан 18. септембра 2025.
 13. General Assembly Resolution 60/288 (2006). Adopted by the General Assembly on 8 September 2006, <https://docs.un.org/en/A/RES/60/288>, доступан 24. септембра 2025.
 14. Голубовић, З. (2023). Полицијска дипломатија у дигиталном окружењу. *Безбедност*, 65(3): 148–161.
 15. Gray, C. (2024). Counterterrorism Strategies in the Age of Global Insurgency. *International Journal for Conventional and Non-Conventional Warfare*, 1(1): 56–64.
 16. Greener, B. K. (2011). The diplomacy of international policing: A case study of the New Zealand experience. *Political Science*, 63(2): 219-239.
 17. De Kerchove, G., Onidi, O. (2021). U.S.-EU Counterterrorism Cooperation Twenty Years After 9/11, <https://www.washingtoninstitute.org/policy-analysis/us-eu-counterterrorism-cooperation-twenty-years-after-911>, доступан 3. октобра 2025.
 18. Den Boer, M., Block, L. (2013). *Liaison Officers: Essential Actors in Transnational Policing*. Eleven International Publishing.
 19. Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0681>, доступан 27. септембра 2025.

20. EUR-Lex (2025). Stepping up cross-border cooperation – the Prüm decision. <https://eur-lex.europa.eu/EN/legal-content/summary/stepping-up-cross-border-cooperation-the-pr-m-decision.html>, доступан 27. септембра 2025.
21. European Commission (February 12, 2025). Strengthening International Judicial Cooperation in Counterterrorism: Key Takeaways from the High-Level Conference https://fpi.ec.europa.eu/news/strengthening-international-judicial-cooperation-counterterrorism-key-takeaways-high-level-2025-02-12_en, доступан 27. септембра 2025.
22. European Commission (May 28, 2025). Strengthening Counter-Terrorism Partnerships in Africa. https://fpi.ec.europa.eu/news/strengthening-counter-terrorism-partnerships-africa-2025-05-28_en, доступан 27. септембра 2025.
23. European Union Terrorism Situation and Trend Report (2019). https://www.europol.europa.eu/cms/sites/default/files/documents/tesat_2019_final.pdf, доступан 3. октобра 2025.
24. Europol (April 27, 2018). Islamic State Propaganda Machine hit by Law Enforcement in coordinated takedown action, <https://www.europol.europa.eu/media-press/newsroom/news/islamic-state-propaganda-machine-hit-law-enforcement-in-coordinated-takedown-action>, доступан 4. октобра 2025.
25. Europol (June 14, 2024). Major takedown of critical online infrastructure to disrupt terrorist communications and propaganda, <https://www.europol.europa.eu/media-press/newsroom/news/major-takedown-of-critical-online-infrastructure-to-disrupt-terrorist-communications-and-propaganda>, доступан 4. октобар 2025.
26. Europol (January 31, 2014). Europol and FBI discuss cooperation on countering international organised crime and terrorism, <https://www.europol.europa.eu/media-press/newsroom/news/europol-and-fbi-discuss-cooperation-countering-international-organised-crime-and-terrorism>, доступан 14. септембра 2025.
27. Europol Analysis Projects (2025). <https://www.europol.europa.eu/how-we-work/europol-analysis-projects>, доступан 2. октобра 2025.
28. Europol Annual Review (2015). https://www.europol.europa.eu/annual_review/2015/networks.html, доступан 1. октобра 2025.

29. Значај полицијске дипломатије, <https://www.rts.rs/lat/vesti/politika/756872/znacaj-policijske-diplomatije.html>, доступан 18. марта 2025.
30. Кекић, Д., Никач, Ж. (2011). Улога и делокруг рада полицијског дипломате у сузбијању тероризма. У: Зборник радова „Супротстављање тероризму - међународни стандарди и правна регулатива”, Међународна научностручна конференција, Влада Републике Српске и други у сарадњи са Ханс Зајдел фондацијом, стр. 415–428.
31. Кекић, Д., Субошић, Д. (2009). Полицијска дипломатија. *Међународни проблеми*, 61(1–2): 141–162.
32. Leidig, E., Van Mieghem, C. (2021). *The US National Strategy on Countering Domestic Terrorism as a model for the EU (Policy Brief)*. International Centre for Counter Terrorism. Hague.
33. Leira, H. (2016). A Conceptual History of Diplomacy, in: Constantinou, M. C., Kerr, P., Sharp, P. (eds). *The SAGE Handbook of Diplomacy*. SAGE.
34. Lucas, K., Baldino, D. (2021). White Knights, Black Armour, Digital Worlds: Exploring the Efficacy of Analysing Online Manifestos of Terrorist Actors in the Counter Terrorism Landscape, in: Adam H., Alastair R., Scott R., Seumas M. (eds.) *Counter-Terrorism, Ethics and Technology: Emerging Challenges at the Frontiers of Counter-Terrorism*. Sprienger, pp. 199-221.
35. Мијалковић, С, Бајагић, М., Поповић Манчевић, М. (2023). *Организовани криминал и тероризам*. Криминалистичко-полицијски универзитет, Београд.
36. Opinion – Police diplomacy’s role in fighting transnational crime <https://neweralive.na/opinion-police-diplomacys-role-in-fighting-transnational-crime>, доступан 14. 3. 2025).
37. PNR (2012). Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security, [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22012A0811\(01\)](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22012A0811(01)), доступно 28. септембра 2025.
38. Ramel, F. (2025). Beyond Diplomacy: Why Trust is the Key to Multilateral Success, *Global Governance Forum*, <https://globalgovernanceforum>.

org/beyond-diplomacy-why-trust-is-the-key-to-multilateral-success/#:~:text=To%20address%20multilateralism's%20crisis%20then%2C%20a%20relational,act%20with%20the%20support%20of%20regional%20groups, доступно 3. октобра 2025.

39. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
40. Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA.
41. Report of the Secretary-General on the Work of the Organization, (A/79/1, seventy-ninth session), United Nations, 2024.
42. Security Council Resolution 1368 (2001). Adopted by the Security Council at its 4370th meeting, on 12 September 2001. [https://docs.un.org/en/S/RES/1368\(2001\)](https://docs.un.org/en/S/RES/1368(2001)), доступан 26. августа 2025.
43. Српски официри за везу ускоро у нашим амбасадама и конзулатима широм света, 18. фебруар 2009, <https://www.srbija.gov.rs/vest/103697/srpski-oficiri-za-vezu-uskoro-u-nasim-ambasadama-i-konzulatima-sirom-sveta.php>, доступан 14. септембра 2025.
44. Statewatch (2002). Informal Ministerial Meeting. Copenhagen, September 13–14, 2002, background papers, <https://www.statewatch.org/media/documents/news/2002/sep/JHAbackground5.pdf>, доступан 27. септембра 2025.
45. SWIFT: European Parliament votes down agreement with the US, press release (2010). [https://www.europarl.europa.eu/RegData/presse/pr_info/2010/EN/03A-DV-PRESSE_IPR\(2010\)02-09\(68674\)_EN.pdf](https://www.europarl.europa.eu/RegData/presse/pr_info/2010/EN/03A-DV-PRESSE_IPR(2010)02-09(68674)_EN.pdf), доступан 1. октобра 2025.
46. The Association of European Police Colleges, <https://aepc.net/mission-statement/>, доступан 18. септембра 2025.

47. United Nations Global Counter-Terrorism Strategy, <https://www.un.org/counterterrorism/un-global-counter-terrorism-strategy>, доступан 24. септембар 2025.
48. United Nations Secretary General (2005). Kofi Annan's keynote address to the closing plenary of the International Summit on Democracy, Terrorism and Security, March 10, 2005. <https://www.un.org/sg/en/content/sg/speeches/2005-03-10/kofi-annan%E2%80%99s-keynote-address-closing-plenary-international-summit>, доступно 12. септембра 2025.
49. FBI (2025). International Offices (Legats), <https://www.fbi.gov/contact-us/international-offices>, доступан 1. октобра 2025.
50. Hart, D., Siniver, A. (2020). The Meaning of Diplomacy. *International Negotiation*, 26(2), 159-183. <https://doi.org/10.1163/15718069-BJA10003>.
51. Hoffman, B., Ware J. (2020). The Challenges of Effective Counterterrorism Intelligence in the 2020s. *Lawfare*, June 21, 2020. <https://www.lawfaremedia.org/article/challenges-effective-counterterrorism-intelligence-2020s>, доступан 20. 9. 2025.
52. https://home-affairs.ec.europa.eu/networks/european-union-internet-forum_en, доступан 27. септембра 2025.
53. <https://rs.ambafrance.org/Sluzba-za-unutrasnju-bezbednost?.com>, доступан 24. марта 2025.
54. https://www.bka.de/EN/OurTasks/Remit/InternationalFunctions/LiaisonOfficers/liaisonOfficers_node.html, доступан 25. марта 2025.
55. [https://www.europarl.europa.eu/RegData/questions/reponses_qe/2018/000009/P8_RE\(2018\)000009_EN.pdf](https://www.europarl.europa.eu/RegData/questions/reponses_qe/2018/000009/P8_RE(2018)000009_EN.pdf), доступан 4. октобра 2025.
56. <https://www.fbi.gov/about/partnerships/international-operations>, доступан 18. марта 2025.
57. <https://www.fedpol.admin.ch/fedpol/en/home/polizei-zusammenarbeit/international/polizeiattaches.html>, доступан 18. марта 2025.
58. <https://www.nationalcrimeagency.gov.uk/what-we-do/how-we-work/providing-specialist-capabilities-for-law-enforcement/international-network>, доступан 24. марта 2025.

59. <https://www.police-nationale.interieur.gouv.fr/nous-rejoindre/nos-metiers/attache-de-securite-interieure>, доступан 24. марта 2025.
60. <https://www.thefreedictionary.com/attache>, доступно 18. марта 2025.
61. Calcara, G. (2021). Balancing International Police Cooperation: INTERPOL and the Undesirable Trade-off Between Rights of Individuals and Global Security, *Liverpool Law Review*, 42: 111–142, <https://doi.org/10.1007/s10991-020-09266-9>.
62. Caudron, M. (2018). How Europol Became a Center Point for the F.B.I., *MEDIUM*, <https://medium.com/euintheus/how-europol-became-a-center-point-for-the-f-b-i-2ccc96f105bb>, доступан 3. октобра 2025.
63. Cоcq, C., Galli, F. (2017). The Evolving Role of Europol in the Fight Against Serious Crime: Current Challenges and Future Prospects, in: Saskia H. and Carole M. (eds.). *Trust in International Police and Justice Cooperation*. Hart Publishing, pp. 125–148.
64. Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008D0615>, доступан 24. септембра 2025.
65. CRS Report for Congress (2004). Europe and Counterterrorism: Strengthening Police and Judicial Cooperation (Updated October 15, 2004). https://www.everycrsreport.com/files/20041015_RL31509_3b2d4c4f9ff5c4f83b9cb675811440f020c949eb.pdf, доступан 2. октобра 2025.
66. Шубаревић, Д. (2025). Штампaj и пуцај: 3Д штампано оружје се продаје онлајн. *Политика маџазин*, 26. јун 2025. <https://magazin.politika.rs/scc/clanak/575664/Zivot/Stampaj-i-pucaj-3d-stampano-oruzje-se-prodaje-onlajn>, доступан 20. 9. 2025.

Police Diplomacy and Global Counterterrorism Efforts: Challenges and Perspectives

Abstract: *Contemporary security dynamics, particularly the phenomenon of transnational terrorism, has generated a pronounced need for innovative and institutionalised forms of cooperation among states and their respective security agencies. Within this framework, the paper examines the concept of police diplomacy as a distinctive nexus between traditional diplomacy and operational law enforcement cooperation. The principal objective of the study is to provide a comprehensive analysis of the theoretical underpinnings, principal actors, and operational manifestations of police diplomacy in counter-terrorism efforts, with specific reference to the collaborative framework established between Europol and the Federal Bureau of Investigation (FBI) in combating the Islamic State (ISIS). Police diplomacy is conceptualised herein as a specific modality of international strategic engagement that synthesises elements of security policy, foreign affairs, and the operational policing. Its principal agents—liaison officers and police attachés—function as pivotal intermediaries in the cultivation of mutual trust and the facilitation of the exchange of intelligence and personal data. Given that the fight against terrorism urges an integrated and multilateral approach, police diplomacy operates as an enabling mechanism for the timely dissemination of intelligence, the conduct of joint investigations, and the harmonisation of operational standards across jurisdictions. Mechanisms such as joint task forces, secure platforms for exchange of operational and strategic crime-related information, and operational deployments within Europol and the FBI exemplify the practical implementation of this form of cooperation. Nevertheless, the principal challenges confronting practitioners of police diplomacy pertain to reconciling divergent national interests, harmonising heterogeneous legal frameworks, addressing restrictions on the transmission of classified data, and fostering sustainable inter-institutional trust. Despite these constraints, the advantages of police diplomacy remain considerable. They are manifested in the accelerated identification of transnational criminal and terrorist networks, the enhancement of preventive capacities, and the advancement of a more nuanced understanding of terrorist dynamics at the*

global level. The cooperative relationship between Europol and the FBI in the fight against ISIS constitutes an illustrative example of institutionalised police diplomacy. The establishment of a permanent FBI liaison officer within Europol's headquarters in The Hague has substantially facilitated the rapid exchange of intelligence, the undertaking of joint investigative operations, and the analytical assessment of terrorist propaganda and network structures. This model of engagement underscores the strategic value of trust-building and sustained dialogue in addressing global security threats. Consequently, police diplomacy emerges as an indispensable instrument within the contemporary security architecture. Its function in counterterrorism reaffirms the imperative of integrating national and international capacities and of institutionalising mechanisms for enduring collaboration. The Europol–FBI partnership thus exemplifies the transformative potential of police diplomacy as a vehicle for constructing a cohesive and resilient global security community.

Keywords: *security, counterterrorism, police diplomacy*

Проф. др Дарко Т. ДИМОВСКИ¹
Правни факултет Универзитета у Нишу

ДОИ: 10.5937/bezbednost2503101D

УДК: 347.85:343.9

Прегледни научни рад

Примљен: 16. 6. 2025. године

Датум прихватања: 24. 11. 2025. године

Криминологија свемирског простора – феномен једне утопије или реалност апсурда²

Апстракт: На почетку рада аутори дају приказ најзначајнијих активности у склопу освајања свемира од стране најмоћнијих држава света. Након тога, посебна пажња је посвећена истраживању појмовног одређења криминологије свемирског простора (*space criminology*), при чему је указано на разлику између појма и појма *defensible space criminology* како не би дошло до њиховог преклапања. У наредном делу рада аутори наводе примере противправних понашања извршених у свемиру како би илустрировали потребу решавања правних проблема. Тиме читаоце уводе у следећи део рада, о могућим местима извршења кривичних дела у свемиру и истраживањима надлежности за посматрање у решавању кривичних ствари. У закључку аутори истичу да је криминологија свемирског простора иренуитно утопија, али да реалност назови апсурда њеног истраживања и посматрања недозвољених понашања ипак постоје.

Кључне речи: *space criminology*, кривична дела, надлежности, утопија, реалност.

¹ darko@prafak.ni.ac.rs, ORCID 0000-0001-5068-3338

² Рад је настао као резултат финансирања од стране Министарства науке, технолошког развоја и иновација, по Уговору евиденциони број 451-03-137/2025-03/ 200120 од 4. 2. 2025. Према Агенди за одрживи развој 2030 (А/RES/71/313), овај документ је повезан са циљем одрживог развоја број 16 – промовисати мирна и инклузивна друштва за одрживи развој, обезбедити приступ правди за све и изградити ефикасне, одговорне и инклузивне институције на свим нивоима.

Увод

Људско поимање порекла свемира има дугу историју, а посматрање неба и веровање у дејство натприродних сила на небу и ка Земљи донекле је ублажено настојањима научника да објашњавања из физике буду та која ће превладати митове. Према прихваћеном становишту, свемир је настао пре око 13,8 милијарди година. У оквиру теорије о Великом праску (*Big Bang*) настанак свемира се објашњава експлозијом веома мале и густе тачке у којој су били концентрисани простор, материја и енергија.³ Осим људске фасцинације свемиром у сазнајном смислу, временом се појавило и питање престижа најмоћнијих држава света, попут Русије, САД и Кине, у њиховом освајању свемирског простора.

Када је Совјетски Савез 1957. године лансирао сателит под називом Спутњик 1 (*Спутник-1*)⁴, сан је претворен у реалност – човек је почео да верује да је само питање времена када ће се отиснути у свемир. Пас Лајка (*Лайка*) лансиран је у свемир те исте године сателитом Спутњик 2 (*Спутњик-2*) (Bartels, Wall, 2022), а совјетски космонаут Јуриј Гагарин (*Јуриј Гагарин*) постао је први човек који је летео у свемир. Он је 12. априла 1961. године направио један круг око Земље у летелици Восток 1 (Nedeljnik, 2024). Амерички председник Џон Кенеди (*John Kennedy*) у свом говору одржаном 12. септембра 1962. године на стадиону Универзитета Рајс (*Rice University*), прокламовао је да је циљ Сједињених Америчких Држава да до 1970. године слете на Месец.⁵ Тако је НАСА (*National Aeronautics and Space Administration – NASA*) у оквиру мисије Аполо 11 (*Apollo 11*) слетела на Месец 20. јула 1969. Године. Тада су се Нил Армстронг (*Neil Armstrong*) и Баз Олдрин (*Buzz Aldrin*) искрцали из своје летелице на

³ Више о томе: Mesarec, L., *The Big Bang Theory*, Proceedings of 6th Socratic Lectures 2021.

⁴ *Sputnik 1*, NASA Space Science Data Coordinated Archive NSSDCA/COSPAR ID: 1957-001B, <https://nssdc.gsfc.nasa.gov/nmc/spacecraft/display.action?id=1957-001B>, доступан 27. 4. 2025.

⁵ *John F. Kennedy (JFK) Moon Speech Transcript: "We Choose to Go to the Moon"*, <https://www.rev.com/transcripts/john-f-kennedy-jfk-moon-speech-transcript-we-choose-to-go-to-the-moon>, доступан 28. 4. 2025.

површину Месеца, при чему је Нил Армстронг изговорио реченицу: „Ово је мали корак за човека, али велики за човечанство”.⁶

Совјетски Савез је 20. фебруара 1986. године лансирао свемирску станицу названу Мир, што је омогућило дуготрајне боравке посада у свемирском простору и спровођење научних експеримената у микрогравитационом окружењу. Иако је 2001. године расхођена због застарелости (Telegraf, 2021), присуство астронаута је настављено боравком у Међународној свемирској станици (*International Space Station – ISS*), која је направљена у међувремену.⁷ Истовремено, водеће светске свемирске агенције прокламовале су мисију слетања људске посаде на Марс након 2030. године.

Поред Сједињених Америчких Држава и Руске Федерације, у трку ка овом циљу укључила и Народна Република Кина. Истовремено Илон Маск (*Elon Musk*), један од најбогатијих људи на свету, планира да овај подухват изведе знатно раније, што у научним круговима изазива скепсу. (BBC NEWS на српском, 2025)

Боравком људи у свемиру ствара се просторни и временски оквир за појаву неких постојећих или нових облика недозвољеног понашања, што доводи до неопходности уочавања правних празнина и предлога за поновно нормирање института из области науке кривичног права, попут: надлежности за поступање, садржаја инкриминација, просторног и временског важења законодавства, примарности кривичноправне заштите и сл. Овај рад за предмет има указивање на појам криминологије свемира, односно бар на почетне, кључне тачке његовог одређења. Циљеви рада јесу да научна и стручна јавност фокус пажње преусмери на базична питања једне нове поддисциплине у криминологији, а то су: међународноправни оквир регулисања људског понашања у свемиру, противправност понашања у свемиру, спорност питања у смислу временског и просторног утврђивања узрочно-последичних веза између поступака и последица предузетих радњи. Посредни циљ рада јесте

⁶ July 20, 1969: *One Giant Leap For Mankind*, NASA, Jul 20, 2019, <https://www.nasa.gov/history/july-20-1969-one-giant-leap-for-mankind/>, доступан 28. 4. 2025.

⁷ International Space Station <https://www.nasa.gov/international-space-station/>, доступан 6. 6. 2025.

да се побуди пажња криминолога, који заступају различите теоријске концепте узрочности у криминологији, да истражују ову тему и пишу о њој, за почетак на основу постојеће литературе, како би указали на основну нит која би се могла одредити као недозвољено понашање у свемирском простору или у вези са свемиром. У раду је примењен основни криминолошки метод посматрања појаве.

Појмовно одређење свемирске криминологије

Одређивање појма криминологије свемирског простора (*space criminology*) изазива контроверзе услед тога што се мали број криминолога до сада бавио овом темом. Ипак, криминологија свемирског простора може се одредити као део криминологије посвећен проучавању криминалитета, полицијског деловања, безбедности и правде у свемиру.⁸ Другим речима, криминологија свемирског простора односи се на проучавање феноменолошких и етиолошких карактеристика криминалитета извршеног у свемиру. Како до сада није извршено успешно слетање са људском посадом на другу планету, то питање је за сада само теоријско, као феномен једне утопије или реалност апсурда. Ипак, према замислима, за десетак година се очекује слетање људске посаде на Марс, па се питање недозвољеног понашања на планети Марс поставља као дилема која спада у домен криминологије свемирског простора. Однос између кривичног права, грађанског права и међународног права, као и између научних дисциплина у оквиру ових грана права, односно нормирање односа у области ове три гране права, треба прво да понуди одговор на питање суверенитета над Месецом и другим небеским телима и из тог суверенитета проистеклих надлежности за поступање овлашћених државних/планетарних органа. Још увек постоји правна празнина у начину нормирања бројних питања о приликама вршења кривичних дела или других недозвољених понашања на неком другом небеском телу осим Земље, освојеном од стране људи. Те правне празнине до сада нису биле предмет посматрања криминологије свемирског простора.

⁸ Према: Our Story, <https://www.spacecriminology.net/about>, доступан 28. 4. 2025.

Како не би дошло до појмовног поистовећивања са једном другом криминологијом која се на енглеском језику такође означава са *space criminology*, треба истаћи да је архитекта Оскар Њуман (*Oscar Newman*) 1972. године у својој књизи *Defensible Space: Crime Prevention through Urban Design* представио идеју да је конструкцијом животне средине могуће утицати на обим криминалитета. Њуман је заступао став да ће доћи до смањења обима криминалитета, због: 1) повећања територијалног понашања одређених грађана у виду одбране одређене територије и надзора над њом, 2) коришћења простора, што резултира друштвеном кохезијом и способношћу да се интервенише и 3) одвраћања потенцијалних криминалаца од вршења кривичних дела јер знају да су одређени простори под надзором грађана. Само присуство грађана на одређеном простору који се сматра одбрањивим доводи до тога да криминалци избегавају вршење кривичних дела, јер постоји могућност да неко од грађана спречи извршење кривичног дела или постане очевидац (Димовски et al., 2015: 424). Стога се, ради разграничења ова два појма, криминологија свемирског простора означава са *space criminology*, а криминологија одбрањивог простора са *defensible space criminology*. На тај начин ће се извршити јасна диференцијација ове две криминолошке дисциплине. Случајност језичког одређења на енглеском језику уједно указује и на применљивост концепта одбрањивог простора и на простор свемира, као природног људског окружења.

Међународноправни оквир понашања у свемиру

Међународна заједница је донела низ споразума који се односе на понашање у свемиру. Након што је Совјетски Савез лансирао Спутњик 1, у оквиру Уједињених нација основана је 1958. године Канцеларија Уједињених нација за питања свемира (*United Nations Office for Outer Space Affairs – UNOOSA*). Главни циљ њеног постојања јесте промовисање међународне сарадње у мирољубивом коришћењу и истраживању свемира, као и у примени науке о свемиру и технологије за одрживи економски и друштвени развој.⁹

⁹ United Nations Office for Outer Space Affairs, <https://www.unoosa.org/oosa/en/aboutus/index.html>, доступан 29. 4. 2025.

Генерална скупштина Уједињених нација донела је Споразум о принципима који регулишу активност држава у истраживању и коришћењу свемира, укључујући Месец и друга небеска тела (*Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies*), познат под називом Споразум о свемиру (*Outer Space Treaty*). Потписивање овог документа уприличено је јануара 1967. године у Вашингтону, Москви и у Лондону. Овим споразумом је постављена основа за међународно право свемира, при чему су промовисани следећи принципи: истраживање и коришћење свемира вршиће се у корист и у интересу свих земаља и биће домен целог човечанства; свемир је слободан за истраживање и коришћење од стране свих држава; свемир није предмет националног присвајања путем захтева за суверенитет, путем коришћења или окупације, или на било који други начин; државе не смеју постављати нуклеарно оружје или друго оружје за масовно уништење у орбиту или на небеска тела, нити га смеју постављати у свемир на било који други начин; Месец и друга небеска тела користе се искључиво у мирнодопске сврхе; астронаути се сматрају изасланицима човечанства; државе су одговорне за националне свемирске активности, без обзира да ли их спроводе владине или невладине организације; државе су одговорне за штету коју проузрокују њихови објекти у свемиру и државе избегавају штетну контаминацију свемира и небеских тела.¹⁰

Већ наредне године, Скупштина УН је извршила допуну овог документа доношењем Споразума о спасавању астронаута, повратку астронаута и враћању објеката лансираних у свемир (*Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space*), који је познат и под називом Споразум о спасавању (*Rescue Agreement*). Споразумом су прописане обавезе везане за спасавање астронаута, њихов повратак и повратак објеката из свемира. Уједно је превиђено да држава која спасава астронауте не наплаћује трошкове спасавања. Њиме је извршено

¹⁰ *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies*, United Nations Office for Outer Space Affairs <https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introouterspacetreaty.html>, доступан 29. 4. 2025.

проширење хуманитарне димензије међународног права свемира, чиме се промовишу међународна солидарност и помоћ у ванредним ситуацијама у свемиру. На тај начин подржана је сарадња између држава ради реализације будућих међународних мисија у свемиру, јер у тренутку када је Споразум донет није реализована ниједна од мисија освајања Месеца, Марса или дубоког свемира. Ипак, постоје одређени недостаци, који се отелотворују у недовољно прецизним обавезама, слабој примени (јер није било случајева на које би се те одредбе примениле), као и у томе да Споразум не обухвата астронауте који у свемир путују о свом трошку (Lyall, Larsen, 2018: 113–130).

Скупштина УН је 29. новембра 1971. године донела Конвенцију о међународној одговорности за штету коју проузрокују објекти у свемиру (*Convention on International Liability for Damage Caused by Space Objects*), чиме је проширено дејство члана 7 Споразума о свемиру. У овој конвенцији детаљно су разрађена сва питања у случају штете проузроковане активностима у свемиру. Тако је, између осталог, прописана апсолутна одговорност државе која је лансирала објекат у свемир у случају да тај објекат проузрокује штету на површини Земље или у атмосфери.¹¹ Овај члан је посебно споменут јер је примењен у случају пада совјетског сателита Космос 954 на територију Канаде 1978. године. Услед овог инцидента, Совјетски Савез је исплатио Канади одштету у износу од три милиона америчких долара. (Al Jazeera, 2018)

Споразум о активностима држава на Месецу и другим небеским телима (*Agreement Governing the Activities of States on the Moon and Other Celestial Bodies*) усвојила је Скупштина УН 5. Децембра 1979. године. У јавности је познат под називом Споразум о Месецу (*Moon Agreement*). Битно је напоменути да га водеће светске силе у истраживању свемира, попут САД, Русије и Кине, никада нису потписале.¹² Разлог за то је чињеница да су у том споразуму Месец и

¹¹ Више видети: Hill Zafren, D., *Convention on International Liability for Damage Caused by Space Objects: Analysis and Background Data*, U.S. Government Printing Office, Michigan, 1972, pp. 23–47.

¹² 2. *Agreement governing the Activities of States on the Moon and Other Celestial Bodies*, New York, 5 December 1979 https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=XXIV-2&chapter=24&clang=_en, доступан 4. 5. 2025.

друга небеска тела означени као заједничко наслеђе човечанства. То значи, како је прописано чланом 11 Споразума о Месецу, да сваки бенефит који се оствари рударењем на Месецу или другим небеским телима треба да буде подједнако подељен свим нацијама, па се тиме у пракси обесхрабрује приватно улагање у рударење на Месецу и другим небеским телима. (Khatri, 2025: 35–36) Ипак, неке државе, попут Сједињених Америчких Држава, усвојиле су законе којима се грађанима омогућава да поседују било који ресурс који открију на астероидима. Иако се Закон о конкурентности комерцијалних лансирања у свемир (*Commercial Space Launch Competitiveness Act*)¹³ не односи на стицање права својине на Месецу, није немогуће да се у будућности норма промени, тако да грађани САД имају могућност да стекну својину на ресурсе на Месецу.¹⁴ Ипак, треба истаћи да Закон у члану 403 наглашава да Сједињене Америчке Државе овим актом не стичу суверенитет нити ексклузивна права над било којим небеским телом. Слично решење има и Луксембург. Наиме, у Закону од 20. јула 2017. о истраживању и коришћењу ресурса из свемира (*Loi du 20 juillet 2017 sur l'exploration et l'utilisation des ressources de l'espace*)¹⁵ прописано је право власништва над ресурсима нађеним у свемиру.

Противправна дела извршена у свемиру

Иако делује скоро незамисливо, реалност апсурда чињенично потврђује да су у свемиру већ извршена нека противправна дела. Први инцидент везује се за совјетског космонаута Германа Титова. Наиме, он је у августу 1961. године, током лета на свемирском броду Восток 2, без претходне дозволе надређених заспао и спавао дуже

¹³ H.R.2262 – U.S. Commercial Space Launch Competitiveness Act 114th, Congress (2015–2016) <https://www.congress.gov/bill/114th-congress/house-bill/2262/text>, доступан 5. 5. 2025.

¹⁴ Parkinson, Dž., BBC (Prevela i priredila N. Bogetić), *Svemir i zemaljski zakoni: Kome Mjesec zapravo pripada?*, <https://www.vijesti.me/svijet/globus/20465/svemir-i-zemaljski-zakoni-kome-mjesec-zapravo-pripada>, доступан 5. 5. 2025.

¹⁵ *Loi du 20 juillet 2017 sur l'exploration et l'utilisation des ressources de l'espace*, <https://legilux.public.lu/eli/etat/leg/loi/2017/07/20/a674/jo>, доступан 5. 5. 2025.

него што је прописано. Ипак, непланирано спавање космонаута није утицало на безбедност мисије, јер је она успешно завршена.¹⁶

Слична ситуација се догодила током мисије Меркур-Атлас 9 (*Mercury-Atlas 9*) 1963. године, када је астронаут НАСА Гордон Купер (*Gordon Cooper*), суочен са тешкоћама приликом покушаја аутоматског приземљења, без претходне дозволе контроле лета преузео ручну контролу и успешно слетео недалеко од планираног места за слетање. У конкретном случају је дошло до кршења протокола, јер је било предвиђено аутоматско приземљење, али Гордон Купер није кажњен, већ је његов дело оцењено као херојско.¹⁷

За време мисије Аполо 7 (*Apollo 7*) током 1968. године астронаути Волтер Шира (*Walter Schirra*), Дон Ајзли (*Donn Eisele*) и Волтер Канингем (*Walter Cunningham*) сукобили су се са контролом лета. До сукоба је дошло услед промрзина, напорног распореда и незадовољства одређеним инструкцијама контроле лета, што је резултирало тиме да су астронаути одбили да емитују ТВ пренос, као и да ставе кациге за време приземљења. Без обзира што овај инцидент надлежни органи нису оквалификовали као противправно понашање, сва тројица су суспендовани. Уједно, НАСА је била приморана да промени психолошку припрему и уведе побољшања у погледу комуникације са астронаутима. (Clemente, 2024)

Интересантно је споменути ситуацију током мисије ISS-42/43. Наиме, услед сукоба између Украјине и Руске Федерације 2014. године, дошло је до наглог погоршања односа руских и америчких астронаута на Међународној свемирској станици. У конкретном случају није дошло до физичког сукоба, али су контакти сведени на

¹⁶ *What Was The First Crime In Space? The Stories Of Space Criminals*, Orbital Today, <https://orbitaltoday.com/2025/01/23/what-was-the-first-crime-in-space-the-stories-of-space-criminals/>, доступан 29. 4. 2025.

¹⁷ *Cooper Maneuvers to a Bullseye Landing with Manual Control as Automatic Fails; 'I'm in Fine Shape', He Says After 22 Orbits; Dramatic Return Astronaut was Aloft over 34 Hours – Aided by Glenn by Richard Witkin Special to the New York Times Cooper Steers to Bullseye Landing by Manual Control as Automatic System Fails. Astronaut Makes dramatic return Aloft More Than 24 Hours on 22-Orbit Trip –Aided by Glenn on Re-entry*, The New York Times, <https://www.nytimes.com/1963/05/17/archives/cooper-maneuvers-to-a-bullseye-landing-with-manual-control-as.html>, доступан 30. 4. 2025.

минимум, што је био очигледан показатељ да дешавања на Земљи могу итекако утицати на одређење ситуације у свемиру, без обзира на удаљеност космонаута од дешавања на Земљи. (Orbital Today, 2025)

Ен Маклејн (*Anne McClain*) је астронауткиња коју је 2013. године НАСА изабрала за једну свемирску мисију која је трајала дуже од двеста дана.¹⁸ Ипак, она је оптужена да је током боравка на Међународној свемирској станици илегално приступила банковном рачуну своје супруге Самер Ворден (*Summer Worden*). Поступак се завршио ослобађајућом пресудом јер је утврђено да је њена супруга Самер Ворден изнела лажне оптужбе, за које је потом и одговарала пред федералним властима. У току трајања кривичног поступка против Маклејнове, она је изјавила да је приступила банковном рачуну своје супруге док је била на шестомесечној мисији на Међународној свемирској станици, при чему јој је Ворденова претходно дала податке за пријављивање на рачун. Како дозвола није била опозвана у време када је Маклејнова два пута приступала рачуну, надлежни суд је сматрао да нема елемената извршења кривичног дела. Стога је на крају поступак поведен против Ворденове. (Zdanowicz, 2020)

Ниједан од наведених примера противправног понашања током боравка у свемиру, или у вези са обављањем мисија у свемиру, није као епилог имао теже последице. Неки од примера, како је то на крају и доказано на суду, нису имали карактер противправног понашања.

Могуће локације извршења кривичних дела у свемиру и питање надлежности

Даља експанзија људи у свемиру неминовно ће допринети повећавању броја места на којима се могу извршити кривична дела. Једна од првих прилика за извршење кривичног дела у свемиру јесу свемирске станице које круже око планете Земље. Наиме, тренутно постоји неколико свемирских станица са људским посадама, што

¹⁸ McClain Anne C., *NASA Astronaut and U.S. Army Colonel*, <https://www.nasa.gov/people/anne-mcclain/>, доступан 1. 5. 2025.

знатно повећава шансе за извршење неког облика криминалитета насиља или имовинског криминалитета. Специфични услови боравка могу, без обзира на претходну обуку, довести да тога да мала размирица прерасте у физички сукоб са озбиљним последицама.

Уједно, место извршења кривичног дела у свемиру могу бити свемирске станице које круже око Месеца. (Aboawf, Suresh, 2023) Иако тренутно не постоје такве свемирске станице, НАСА у сарадњи са Европском свемирском агенцијом (*European Space Agency – ESA*), Јапанском свемирском агенцијом (*Japan Aerospace Exploration Agency – JAXA*), Канадском свемирском агенцијом (*Canadian Space Agency – CSA*) и другим партнерима планира спровођење пројекта Лунарни пролаз (*Lunar Gateway*). (Amazouz, 2025) С тим у вези, поставља се питање надлежности судова у случају да кривично дело буде извршено на свемирским станицама које круже око планете Земље. Наиме, уколико се ради о свемирској станици у власништву једне државе, одговор је једноставан. Чланом 8 Споразума о свемиру прописано је да држава регистрације има јурисдикцију и контролу над објектом у свемиру који је регистровала. У том случају су за суђење у кривичним стварима надлежни судови земље која је регистровала свемирску станицу. Ипак, у пракси је врло вероватно да је свемирска станица резултат међусобне сарадње више држава или више међународних свемирских агенција, што усложњава питање надлежности. Таква ситуација у реалности већ постоји у погледу Међународне свемирске станице, јер је она резултат заједничког рада неколико држава. Чланом 5 Споразума о Међународној свемирској станици (*International Space Station Intergovernmental Agreement – IGA*),¹⁹ потписаног 29. јануара 1998. године између петнаест држава партнера, предвиђено је да сваки партнер задржава јурисдикцију и контролу над елементима које региструје и над особљем у или на свемирској станици које чине његови држављани. Власници Међународне свемирске станице – Сједињене Америчке Државе, Руска Феде-

¹⁹ *Agreement Among the Government of Canada, Governments of Member States of the European Space Agency, the Government of Japan, the Government of the Russian Federation, and the Government of the United States of America, Concerning Cooperation on the Civil International Space Station*, https://aerospace.org/sites/default/files/policy_archives/Space%20Station%20Intergovernmental%20Agreement%20Jan98.pdf, доступан 2. 5. 2025.

рација, Јапан, Канада и европски партнери – правно су одговорни за одговарајуће елементе које обезбеђују, при чему се европске државе третирају као један хомогени ентитет. Међутим, могуће је да било која од европских држава прошири своје националне законе и прописе на европске елементе, опрему и особље. У случају сукоба надлежности, примењују се правила прописана на међународном и националном нивоу.²⁰

Такође, овим документом је разјашњен потенцијални сукоб надлежности у кривичним стварима. Тако је чланом 22 Споразума о Међународној свемирској станици прописано да се кривична надлежност одређује према држављанству починиоца. Исто тако, у случају који укључује недолично понашање у орбити које (а) утиче на живот или безбедност држављанина друге државе партнера или (б) се дешава на лету друге државе партнера, односно узрокује штету елементу лета друге државе партнера, држава партнер чији је наводни починилац држављанин ће се, на захтев било које погођене државе партнера, консултовати са том државом у вези са интересима њихових тужилаштава. У наставку поменутог члана предвиђено је да држава партнер погођена таквим поступцима може, након таквих консултација, вршити кривичну надлежност над наводним починиоцем под одређеним условом. Тако у року од деведесет дана од датума таквих консултација, или у другом року који се може обострано договорити, погођена држава партнер може имати кривичну надлежност у случају да се држава партнер чији је наводни починилац држављанин сагласи с таквим вршењем кривичне надлежности, или не пружи гаранције да ће случај покренути пред својим надлежним органима ради кривичног гоњења. Приликом доношења овог споразума водило се рачуна и о питању екстрадиције. Наиме, ако држава партнер која условљава екстрадицију постојањем уговора прими захтев за екстрадицију од друге државе партнера са којом нема уговор о екстрадицији, она може по свом избору сматрати овај споразум правним основом за

²⁰ *International Space Station legal framework*, The European Space Agency, https://www.esa.int/Science_Exploration/Human_and_Robotic_Exploration/International_Space_Station/International_Space_Station_legal_framework, доступан 2. 5. 2025.

екстрадицију у вези са наводним недоличним понашањем у орбити, при чему се екстрадиција спроводи у складу са законима замољене државе партнера. Исто тако, прописана је међусобна правна помоћ. С тим у вези, свака држава партнер ће, у складу са својим националним законима и прописима, пружити осталим партнерима правну помоћ у вези са наводним недоличним понашањем у орбити.

До извршења кривичних дела може доћи током пута у свемир. Реалност је таква да су путовања у свемир омогућена и особама које имају довољно финансијских средстава да плате путовање. Тако је, на пример, Денис Тито (*Dennis Tito*) 28. априла 2001. постао први свемирски туриста. Он је провео седам дана на Међународној свемирској станици. Лет га је коштао двадесет милиона америчких долара. (Street, 2021) Након њега је још неколико десетина богатих људи боравило у свемиру или на Међународној свемирској станици. (Li, 2025) С разлогом се поставља питање да ли би током даљег развоја свемирског туризма било могуће да појединац или организована група угрози безбедност летелице и путника зарад остваривања својих циљева. Тада би се питања надлежности, као и у претходним сличним ситуацијама, решавала тако да се могу применити норме којима се регулише надлежност у погледу расветљавања и решавања кривичних ствари.

Даље освајање космоса нужно захтева организовање дугих експедиција. Посебни услови могу узроковати бројне психичке тешкоће, што усложњава безбедност свих чланова посаде. Зато је неопходно предвидети превентивне мере, као и службу за подршку која би благовременом реакцијом спречила теже последице. Исто тако, до вршења кривичних дела или других недозвољених понашања може доћи на привременим базама на Месецу или другом небеском телу. То значи да би била могућа примена сличних метода превенције и подршке као код дуготрајних мисија.

Посебна ситуација се односи на случајеве расветљења и решења кривичних дела у трајним насеобинама на Месецу или другим небеским телима. Насеобину би највероватније чинили људи различитих националности, што усложњава питања кривичне одговорности и надлежности органа за утврђивање те одговорно-

сти. У таквим ситуацијама би било потребно да се државе претходно договоре о примени одређеног нормативног оквира, или да се за насеобину донесе засебни оквир поступања од стране надлежног органа. Хипотетичка ситуација би била да Сједињене Америчке Државе изграде објекат, а да у том објекту кинески држављанин изврши кривично дело убиства над мексичким држављанином. У том случају би се могле применити одредбе које се односе на успостављање надлежности кинеског суда сходно члану 22 Споразума о Међународној свемирској станици. Ипак, треба истаћи да се овде ради о правној празнини, јер ниједан међународни документ није предвидео овакву ситуацију. Могла би се применити само аналогија. С друге стране, могуће је да до извршења кривичног дела дође на јавном простору трајне насеобине, што би довело до тога да се питање надлежности не може решити ни применом аналогије. Стога, временом ће вероватније трајне насеобине добити сопствено кривично законодавство у којем би се решило питање надлежности.

На основу наведених места на којима је могуће извршити кривична дела јасно је да су неке потенцијалне ситуације решене, а да неке нису, јер за њима тренутно нема потребе. Ипак, убрзани развитак свемирске индустрије на Земљи, са јасно постављеним циљевима даљег освајања свемира, неминовно ће поставити питање надлежности кривичног законодавства. До разрешења свих потенцијалних ситуација мора доћи пре него што се даље освајање свемира настави.

Спорне ситуације у свемиру

Поред питања надлежности, у реалности су могуће и друге спорне ситуације. Кључни члан посаде, као што је на пример пилот, може извршити кривично дело док је на привременим или трајним базама на неком небеском телу. Одређивање притвора или поступак његовог санкционисања може животно угрозити остале чланове групе. То указује на неопходност решавања различитих питања, почев од оног чему дати предност у условима угрожености опстанка групе. На пример, да ли кључном члану групе, ако

је извршио недозвољено понашање, треба ублажити прописану кривичну санкцију тако да он својим радом надокнади штету, и то у интересу мисије? Извршење тешког кривичног дела изазива додатне дилеме, пре свега због обавезе одређивања притвора из унапред утврђених основа (Aboawf, Suresh, 2023), па се поставља питање ко би био задужен за спровођење притвора у случају новооснованих малобројних колонија. И ова околност мора бити унапред прописана, пре евентуалног оснивања колоније, у циљу доследне примене начела легалитета.

Из тога јасно произилази неколико препорука које би биле важне за опстанак и успешно функционисање привремених или трајних база на неком небеском телу. Прва препорука је да се питање важења кривичног законодавства реши пре поласка на пут и оснивање свемирске базе. Неки од међународних докумената могу се применити у одређеним ситуацијама, али животне околности могу бити знатно компликованије од потенцијалних случајева који су нормирани досадашњим решењима. Чланови базе могу бити особе различитих националности, па је потребно сагласје више држава, или да међународна организација попут Уједињених нација донесе одговарајући нормативни оквир.²¹

Ипак, у пракси је могуће и да новооснована свемирска колонија у неком тренутку прогласи аутономију у односу на матичну земљу (ако је колонију основала једна држава), слично проглашењу рата за независност британских колонија у Северној Америци. У том случају се може очекивати да будућа власт донесе сопствено законодавство.

Наредна препорука се отелотворује у томе да међу члановима базе треба да постоји лице са довољно правног знања како би могло да зна какве законске опције постоје у случају извршења неког кривичног дела. Поред тога, поставља се питање извршења кривичне санкције. За сваку од кривичних санкција може бити спо-

²¹ Размишљања могу ићи и даље – на пример, питање оснивања мировних мисија за разрешење конфликтних ситуација на свемирским станицама, или на Земљи, а у вези са догађајима на свемирским станицама које су основале различите државе. Видети: Никола Станковић, Злочини над особљем мировних мисија током њиховог развоја, *Безбедност*, 1/2024, стр. 135–158. DOI: 10.5937/bezbednost24011355

рно на који ће начин бити извршена, а то се нарочито односи на затворску казну. Извршење затворске казне подразумева неколико нужних претпоставки, јасно назначених у уџбеничкој литератури из области пенологије. Једна од њих је постојање одговарајућег особља које ће привести осуђеника на извршење уколико се то лице не одазове добровољно налогу за извршење казне. Важно је и постојање пријемног одељења у казним установама, службе за третман, службе за обезбеђење, службе за обуку и упошљавање, службе за здравствену заштиту и службе за опште послове. Одсуство пријемног одељења или једне од ових служби онемогућило би остваривање успешне реинтеграције осуђених у друштво. Тиме би се затворска казна свела на пуко затварање осуђеника, што би представљало цивилизацијски корак уназад од неколико стотина година.²² Ипак, уверења смо да би оснивање свемирске колоније представљало ванредно велики напор за људе послате у ту мисију и да би они били стављени у врло неповољну позицију јер би морали да спроводе извршење затворске казне у периоду када је ангажовање сваког члана круцијално за успостављање самоодрживе колоније. Стога за чланове посаде морају бити послати високо квалификовани људи вођени моралним начелима, али и другим психичким особинама које одговарају учешћу у тако сложеним мисијама.

Закључак

Криминологија свемирског простора, иако тек у повоју, привлачи пажњу прегалаца научне мисли. Толико тога је још увек непознато. Без обзира што су поједине државе најавиле амбициозне планове у погледу даљег освајања свемира, вероватније је да до тога неће скоро доћи, услед бројних политичких и економских изазова у свету. Исто тако, треба се осврнути и на сам наслов рада – да ли је

²² У овим околностима може се поставити као неопходно вршење процене ризика од рецидивизма, посебно у случају извршења тежих кривичних дела. Видети: Вера Петровић, Међупосматрачка поузданост инструмента за процену ризика од рецидивизма код високоризичних осуђених, *Безбедност*, 3/2023, стр. 65–81. DOI: 10.5937/bezbednost2303046P

криминологија свемирског простора утопија или стварност? У овом тренутку, она је можда пре утопијски приказ „матрикс” погледа на свет, али с обзиром на тренутни развој цивилизације, та утопија ће неприметно прерасти у стварност препуну нерешених тешкоћа међу људима. Начела легалитета и легитимитета опстаће све док постоји људски род, као неумитни стубови његовог опстанка. Будућа поколења криминолога биће у ситуацији да врше емпиријска истраживања која ће имати за циљ утврђивање специфичних феноменолошких и етиолошких карактеристика криминалитета и других облика недозвољених понашања извршених у свемиру. На тај начин је могуће дати одговор на питање да ли ће се криминалитет извршен у свемиру разликовати од кривичних дела која нас данас окружују. Вероватно не, јер ће га вршити људи, без обзира на место тренутног боравка.

Литература

1. *2. Agreement governing the Activities of States on the Moon and Other Celestial Bodies* (1979), https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=XXIV-2&chapter=24&clang=_en, доступан 4. 5. 2025.
2. *10 činjenica o čuvenoj svemirskoj stanici „Mir”: Projekat koji je prijateljio Amere i Ruse* (2021). *Telegraf*, <https://www.telegraf.rs/hi-tech/zanimljivosti-hi-tech/3319415-svemirska-stanica-mir>, доступан 28. 4. 2025.
3. Aboawf, S., Suresh S. (2023). *Crime in Space*, *Ox Jornal*, <https://www.oxjournal.org/crime-in-space/>, доступан 7. 6. 2025.
4. *Agreement Among the Government of Canada, Governments of Member States of the European Space Agency, the Government of Japan, the Government of the Russian Federation, and the Government of the United States of America, Concerning Cooperation on the Civil International Space Station*, https://aerospace.org/sites/default/files/policy_archives/Space%20Station%20Intergovernmental%20Agreement%20Jan98.pdf, доступан 2. 5. 2025.

5. Amazouz, L. (2025). *NASA's Artemis Program Takes a Big Leap With the Gateway Lunar Space Station, NASA's Artemis Gateway is one step closer to reality, marking a major milestone in humanity's return to the Moon*. Daily Galaxy, https://dailygalaxy.com/2025/02/nasas-artemis-gateway-lunar-space-station/?utm_source=chatgpt.com, доступан 1. 5. 2025.
6. Bartels, M., Wall, M. (2022). *Laika the space dog: First living creature in orbit*, <https://www.space.com/laika-space-dog>, доступан 7. 6. 2025.
7. Clemente, R. (2024). *Skylab 4: 50 years since the first 'mutiny' aboard a spacecraft*, El Pais, <https://english.elpais.com/science-tech/2024-01-15/skylab-4-50-years-since-the-first-mutiny-aboard-a-spacecraft.html>, доступан 30. 4. 2025.
8. *Cooper Maneuvers to a Bullseye Landing with Manual Control as Automatic Fails; 'I'm in Fine Shape', He Says After 22 Orbits; Dramatic Return Astronaut Was Aloft Over 34 Hours, Aided by Glenn by Richard Witkin Special to The New York Times Cooper Steers to Bullseye Landing by Manual Control as Automatic System Fails. Astronaut Makes Dramatic Return Aloft More Than 24 Hours on 22-Orbit Trip--Aided by Glenn on Re-entry*, The New York Times, <https://www.nytimes.com/1963/05/17/archives/cooper-maneuvers-to-a-bullseye-landing-with-manual-control-as.html>, доступан 30. 4. 2025.
9. *Dan kada je počela svemirska era za čovečanstvo: Let od 108 minuta Juriya Gagarina*, Nedeljnik, <https://www.nedeljnik.rs/dan-kada-je-pocela-svemirska-era-za-covecanstvo-let-od-108-minuta-juriya-gagarina/>, доступан 27. 4. 2025.
10. Dimovski, D., Popović, I., Randelović, D. (2015). Projektovana životna sredina kao način prevencije kriminaliteta, *Pravna riječ*, 12(44): 423–440.
11. Parkinson, Dž., BBC (Prevela i priredila N. Bogetić), *Svemir i zemaljski zakoni: Kome Mjesec zapravo pripada?*, Vijesti, <https://www.vijesti.me/svijet/globus/20465/svemir-i-zemaljski-zakoni-kome-mjesec-zapravo-pripada>, доступан 5. 5. 2025.
12. Hill Zafren, D. (1972). *Convention on International Liability for Damage Caused by Space Objects: Analysis and Background Data*, U.S. Government Printing Office, Michigan, стр. 23–47.

13. *H.R.2262 – U.S. Commercial Space Launch Competitiveness Act*, 114th Congress (2015–2016), <https://www.congress.gov/bill/114th-congress/house-bill/2262/text>, доступан 5. 5. 2025.
14. International Space Station, <https://www.nasa.gov/international-space-station/>, доступан 6. 6. 2025.
15. *International Space Station legal framework*, The European Space Agency, https://www.esa.int/Science_Exploration/Human_and_Robotic_Exploration/International_Space_Station/International_Space_Station_legal_framework, доступан 2. 5. 2025.
16. *Kennedy J. F. (JFK) Moon Speech Transcript: “We Choose to Go to the Moon”*, Rev, <https://www.rev.com/transcripts/john-f-kennedy-jfk-moon-speech-transcript-we-choose-to-go-to-the-moon>, доступан 28. 4. 2025.
17. NASA (2019). *July 20, 1969: One Giant Leap For Mankind*, July 20, 2019, <https://www.nasa.gov/history/july-20-1969-one-giant-leap-for-mankind/>, доступан 28. 4. 2025.
18. Khatri, A. (2025). *Moon Mysteries*, Publifye AS, стр. 35–36.
19. *Loi du 20 juillet 2017 sur l'exploration et l'utilisation des ressources de l'espace*, <https://legilux.public.lu/eli/etat/leg/loi/2017/07/20/a674/jo>, доступан 5. 5. 2025.
20. Li, A., *Jun 1 A Chronology of Space Tourists (as of June 1st, 2025)*, <https://alexli.com/thespacebar/spacetouristslist>, доступан 2. 5. 2025.
21. Lyall, F., Larsen, P. (2018). *Space Law – A Treatise*, Routledge, London, стр. 113–130.
22. *Mask ne odustaje: Prva misija na Mars sledeće godine*, BBC NEWS na srpskom, <https://www.bbc.com/serbian/articles/cedlzpq5p9jo/lat>, доступан 2.6. 2025.
23. McClain, A. C., *NASA Astronaut and U.S. Army Colonel*, <https://www.nasa.gov/people/anne-c-mcclain/>, доступан 1. 5. 2025.
24. Mesarec, L. (2021). *The Big Bang Theory*, Proceedings of 6th Socratic Lectures.
25. *Our Story*, <https://www.spacecriminology.net/about>, доступан 28. 4. 2025.

26. Petrović, V. (2023) Међупосматрачка поузданост инструмента за процену ризика од рецидивизма код високоризичних осуђених, *Безбедност* 65(3): 65–81. DOI: 10.5937/bezbednost2303046P.
27. *Sateliti 'svakodnevno' padaju oko nas*, Al Jazeera, <https://balkans.aljazeera.net teme/2018/4/7/sateliti-svakodnevno-padaju-okon-as>, доступан 4. 5. 2025.
28. *Sputnik 1*, NASA Space Science Data Coordinated Archive NSSDCA/ COSPAR ID: 1957-001B, <https://nssdc.gsfc.nasa.gov/nmc/spacecraft/display.action?id=1957-001B>, доступан 27. 4. 2025.
29. Stanković, N. (2024). Злочини над особљем мировних мисија током њиховог развоја, *Безбедност*, 66(1): 135–158. DOI: 10.5937/bezbednost2401135S
30. Street, F., *First space tourist Dennis Tito: 'It was the greatest moment of my life'*, CNN <https://edition.cnn.com/travel/article/space-tourism-20-year-anniversary-scen/index.html>, доступан 2. 5. 2025.
31. *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies*, United Nations Office for Outer Space Affairs, <https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introouterspacetreaty.html>, доступан 29. 4. 2025.
32. United Nations Office for Outer Space Affairs, <https://www.unoosa.org/oosa/en/aboutus/index.html>, доступан 29. 4. 2025.
33. Zdanowicz, C. (2020). *NASA astronaut's estranged wife charged with lying about claim that spouse improperly accessed account from space*, CNN, <https://edition.cnn.com/2020/04/08/us/nasa-astronaut-anne-mcclain-estranged-wife-charged-trnd/index.html>, доступан 1. 5. 2025.
34. *What Was The First Crime In Space? The Stories Of Space Criminals*, Orbital Today, <https://orbitaltoday.com/2025/01/23/what-was-the-first-crime-in-space-the-stories-of-space-criminals/>, доступан 29. 4. 2025.

Space Criminology – a Utopian Phenomenon or an Absurd Reality

Abstract: *At the beginning of the paper, the author gives an account of the most significant activities regarding the conquest of space by the United States of America and the former Soviet Union. After that, special attention is paid to the issue of conceptual determination of the so-called space criminology as opposed to another concept with a similar name - defensible space criminology in order to avoid confusion. In the next part of the paper, the author gives a list of illegal behaviours committed in space to illustrate the need to solve legal gaps, which is an introduction to the part of the paper focusing on possible locations of criminal acts in space and the question of jurisdiction. In this part of the paper, the author presents the potential places of execution of criminal acts in space and offers possible solutions in terms of jurisdiction. The next part of the paper refers to a number of disputed situations in space. In conclusion, the author points out that currently space criminology is a utopia, but that it can quickly become a reality.*

Keywords: *space criminology, criminal acts, issues of jurisdiction, disputed situations*

Prof. Goran MATIĆ, PhD¹

Office of the National Security Council
and Classified Information Protection

DOI: 10.5937/bezbednost2503141M

UDK: 351.746.1:347.775(497.11)“2019/2024“

Pregledni naučni rad

Primljen: 23. 6. 2025. godine

Revizija: 9. 10. 2025. godine

Datum prihvatanja: 24. 11. 2025. godine

Analysis of Trends in Security Vetting of Ministry of Internal Affairs Personnel in the Context of the Implementation of the Law on Classified Information (2019–2024)

Abstract: *This paper analyzes trends and key drivers in Serbia's security clearance process from 2019 to 2024, focusing on human resource development, data management, and legal enforcement. By examining clearance issuance data, it assesses the influence of international standards, shifting security policies, and institutional reforms. The analysis identifies persistent challenges, particularly in implementing legislation and achieving process transparency, highlighting gaps in data quality and interpretive capacity. It proposes targeted improvements, including procedural digitization, stronger interinstitutional coordination, and standardized reporting. The paper concludes by exploring the implications of pending legal reforms and recommending measures to enhance personnel capacity and specialized training for effective implementation of new standards.*

Keywords: *national security, protection of classified information, personnel security, eligibility determination process.*

¹ office@nsa.gov.rs; goran.matic@nsa.gov.rs

Introduction

Ensuring national security and safeguarding classified information are essential to Serbia's stability (The National Security Strategy, 2019). Therefore, members of the Ministry of Internal Affairs (hereinafter: MOIA) who access such data must undergo proper vetting in line with the Law on Classified Information (Law on Classified Information, 2009, Art. 48) and its by-laws².

In Serbia, information classification is regulated by the 2009 Law on Classified Information and accompanying regulations from 2011 and 2013. The system defines four levels —TOP SECRET, SECRET, CONFIDENTIAL, and RESTRICTED — designed to prevent misuse or unauthorized access to sensitive data that could threaten national interests.

Security vetting for access to TOP SECRET and SECRET information is conducted exclusively by the Security Information Agency (hereinafter: BIA). However, for SECRET-level information, both BIA and MOIA may carry out vetting, depending on the specific roles and responsibilities of MOIA personnel (Law on Classified Information, 2009, Art. 54, para 5). For CONFIDENTIAL-level information, security vetting is conducted solely by MOIA. No formal vetting is required for information classified as RESTRICTED (Mijalković, 2015: 195-208). Instead, employees sign a statement of responsibility and undergo a briefing to become familiar with their duties (Matić, Milošević; 2021: 207-213)

The MOIA is not authorized to issue security clearances. This function is exclusively performed by the Office of the National Security Council and Classified Information Protection (hereinafter: National Security Council Office), which initiates and conducts clearance procedures upon formal request from the MOIA. (Law on Classified Information, 2009, Art. 51).

² Regulation on Detailed Criteria for Determining Classification Levels TOP SECRET and SECRET, Official Gazette of the Republic of Serbia, No. 46/2013 and the Regulation on Detailed Criteria for Determining classification levels CONFIDENTIAL and RESTRICTED, Official Gazette of the Republic of Serbia, No. 105/ 2013

In addition to initiating procedures, the National Security Council Office maintains records of all security clearances issued in Serbia. For this study, data on MOIA personnel is especially relevant, forming the core of trend and practice analysis in classified information protection.

This study analyzes trends in security vetting for MOIA personnel between 2019 and 2024, with comparative insight into the Ministry of Defense (hereinafter: MOD). It focuses on implementing the Law on Classified Information and procedures for protecting data marked TOP SECRET, SECRET, and CONFIDENTIAL. In addition to tracking protection patterns, the study identifies systemic shortcomings and opportunities for improvement. Its findings aim to support more efficient clearance procedures and strengthen security awareness, especially among MOIA personnel (Dragišić et al., 2018: 172).

Methodological approach

In this research, data from the official records of issued security clearances maintained by the National Security Council Office were used for the period from 2019 to 2024. (Regulation on the content, form and method of maintaining records for access to classified information, 2010). Official records offered a reliable foundation for analyzing trends in MOIA security clearances under the Law on Classified Information. Combining quantitative (e.g., case volume and duration) and qualitative methods (e.g., identifying systemic challenges), the analysis revealed key patterns. Visualizations like histograms and pie charts supported the identification of problem areas and informed practical recommendations, such as reducing processing times and enhancing transparency.

The research encompassed all MOIA members who, in accordance with the Law on Classified Information, completed the full security clearance process (Matić, 2019: 27-116). The eligibility determination process includes several stages, starting with the completion of questionnaires (Regulation on forms of security questionnaires, 2010) and submitting requests to the National Security Council Office, conducting

security vetting, taking decisions and issuing security clearances. Data were collected for each phase of the process to identify trends, key timing factors, and procedural variations in issuing security clearances.

The methodology examines how vetting procedures vary by classification level (TOP SECRET, SECRET, and CONFIDENTIAL), alongside a review of relevant legal frameworks. It also addresses practical challenges—such as delays and procedural obstacles—that impact the efficiency and quality of clearance decisions. Visual tools, including graphs and tables, are used to highlight trends, expose system weaknesses, and identify areas for improvement within MOIA’s eligibility determination process.

The analysis drew on data managed by the National Security Council Office regarding security clearances issued to public authorities, MOIA, and MOD personnel. These records supported the study’s conclusions and recommendations for improving eligibility determinations and strengthening classified information protection. Beyond trend tracking, the data also contributes to enhancing transparency, efficiency, and strategic planning.

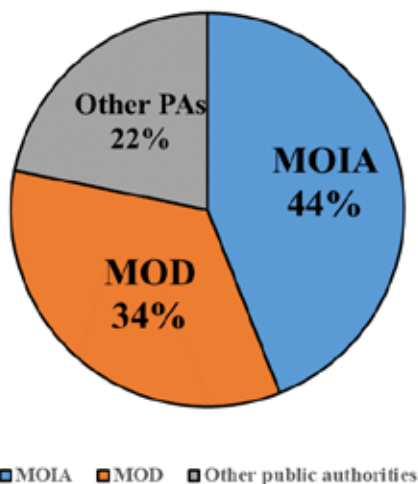
Results and discussion

This section presents findings from the analysis of security clearances issued between 2019 and 2024, based on official records from the National Security Council Office covering MOIA personnel, Ministry of Defense staff, and other public authorities. Between 2011 and 2024, the National Security Council Office conducted security vetting and issued clearances for 21,214 individuals and 485 legal entities⁵. Between 2019 and 2024 — the core period analyzed in this study — a total of 18,781 security clearances were issued, distributed as follows:

⁵ The data were taken over from the NSC Office website on 14 April 2025.

Table 1. Overview of issued security clearances by public authorities for the period 2019-2024, for all authorities, for specific categories (MOIA and MOD) and other public authorities

Year	2019	2020	2021	2022	2023	2024	Total No. by authority
TOTAL	938	697	1591	6760	4306	4489	18781
MOIA	271	120	141	5404	1229	1101	8266
MOD	221	240	303	737	2156	2763	6420
Other public authorities	446	337	1147	619	921	625	4095



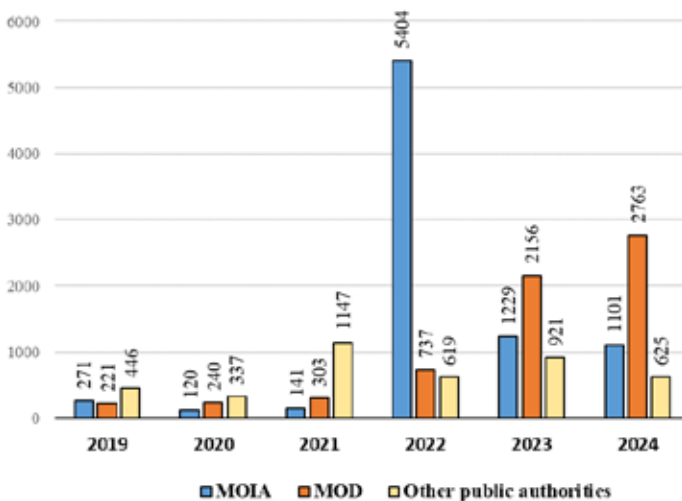
Graph 1. Ratio of issued security clearances by public authorities from 2019 to 2024 in percentages

Comparison by institutions

Including data on MOD clearances provides a valuable benchmark for comparing trends across security sectors. Given the MOD’s consistent and formalized vetting procedures, it serves as a control group for assessing the pace and patterns of clearances issued to MOIA personnel, public authorities, and legal entities. This comparative approach enables more precise evaluation of institutional differences in security vetting practices.

Table 2. Overview of issued security clearances by public authorities for the period 2019-2024

Year	2019	2020	2021	2022	2023	2024
TOTAL	938	697	1591	6760	4306	4489
MOIA	271	120	141	5404	1229	1101
MOD	221	240	303	737	2156	2763
Other public authorities	446	337	1147	619	921	625

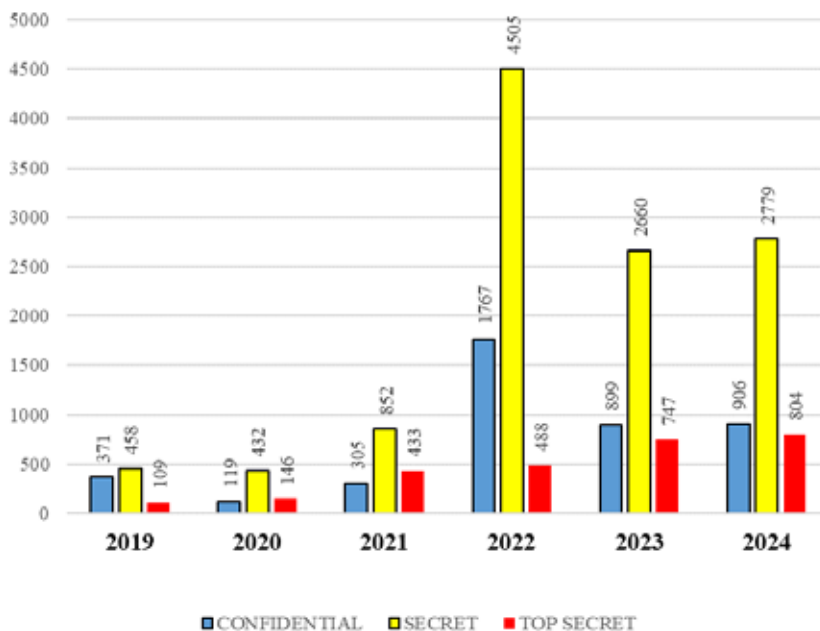


Graph 2. Ratio of issued security clearances by public authorities for the period 2019-2024, by years

Security clearances issued by years – comparative review

Table 3. Overview of number of security clearances issued to all public authorities and legal entities by years and by c. levels (2019-2024)

Year	2019	2020	2021	2022	2023	2024
CONFIDENTIAL	371	119	305	1767	899	906
SECRET	458	432	852	4505	2660	2779
TOP SECRET	109	146	433	488	747	804
TOTAL	938	697	1590	6760	4306	4489

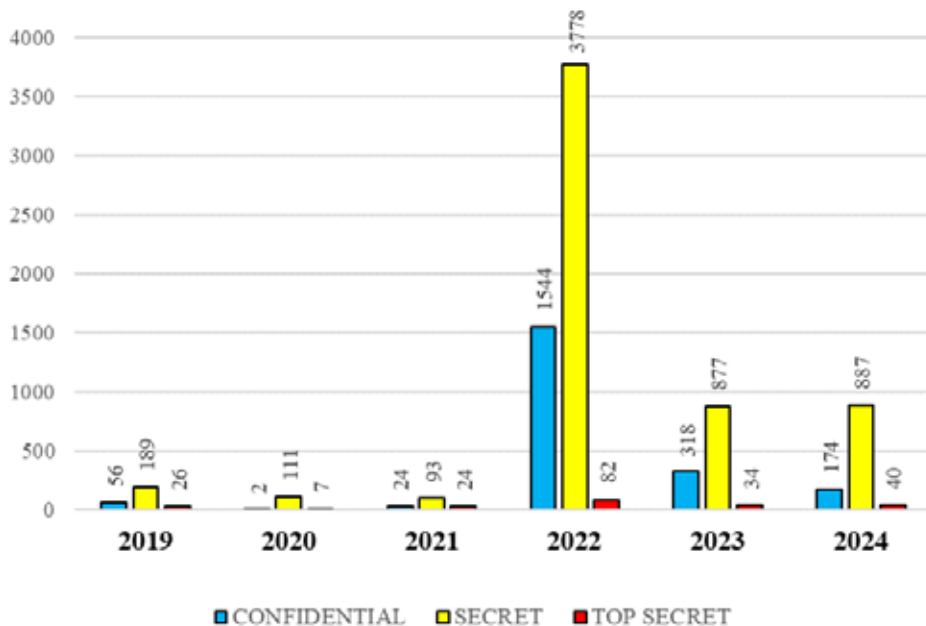


Graph 3. Ratio of issued security clearances by classification levels from 2019 to 2024

Overview of number of issued security clearances at MOIA by years and classification levels (2019–2024)

Table 4. Overview of issued security clearances at MOIA by classification levels from 2019 to 2024

Year	2019	2020	2021	2022	2023	2024
CONFIDENTIAL	56	2	24	1544	318	174
SECRET	189	111	93	3778	877	887
TOP SECRET	26	7	24	82	34	40
TOTAL	271	120	141	5404	1229	1101

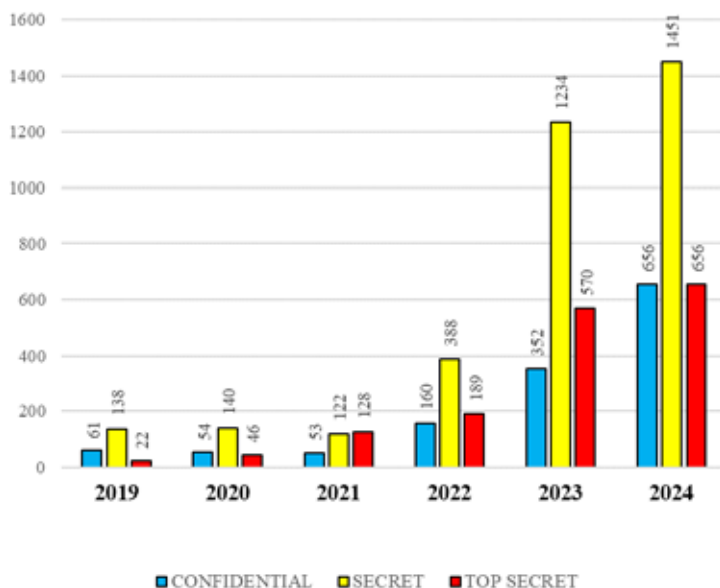


Graph 4. Ratio of issued security clearances by classification levels within MOIA for the period 2019 – 2024

Overview of issued security clearances by years and classification levels within MOD (2019–2024)

Table 5. Overview of issued security clearances by classification levels within MOD (2019-2024)

Year	2019	2020	2021	2022	2023	2024
CONFIDENTIAL	61	54	53	160	352	656
SECRET	138	140	122	388	1234	1451
TOP SECRET	22	46	128	189	570	656
TOTAL	221	240	303	737	2156	2763



Graph 5. Ratio of issued security clearances by security levels within MOD for the period 2019-2024

Methodological observations

The 2019–2024 security clearance data reveal several methodological considerations for accurate interpretation. A striking spike occurred in 2022, when MOIA issued 5,404 clearances—over 38 times the 2021 figure. The MOD saw similar growth, issuing 2,156 clearances in 2023 and 2,763 in 2024, up from just 303 in 2021. These increases likely reflect changes in security policy, institutional reforms, and efforts to align with international standards, particularly in cooperation with NATO, the EU, and other partners. They may also result from the launch of classified projects or re-vetting of personnel with prior clearances.

An additional methodological note concerns occasional discrepancies—or, in some cases, precise matches—between total clearances issued and their breakdown by classification level. For example, the MOD's 2,763 clearances in 2024 match the combined total of level-specific data (656 + 1,451 + 656), while MOIA's 5,404 clearances in 2022 align exactly with its respective category totals (1,544 + 3,778 + 82). Minor discrepancies in earlier data likely stem from administrative delays, retroactive entries, data entry errors, or timing gaps between issuance and registration in the National Security Council Office's database. Accordingly, aggregate statistics should be interpreted with caution—particularly when assessing the effectiveness and responsiveness of Serbia's classified information protection system. Complementing quantitative findings with qualitative insights into regulatory, institutional, and political developments provides a more balanced understanding of clearance trends.

Trends in the number of issued security clearances for MOIA and MOD members

Between 2019 and 2024, security clearance trends for MOIA and MOD personnel reflected institutional and regulatory shifts. The MOIA experienced a sharp rise in 2022, issuing 5,404 clearances — up from just 141 in 2021. While numbers declined in 2023 (1,229) and 2024 (1,101), they remained well above earlier years, possibly indicating the completion

of a major vetting cycle or expanded access to classified information.

The MOD followed a similar trajectory: moderate clearance numbers from 2019 to 2021 (ranging from 283 to 314) surged to 2,156 in 2023 and 2,763 in 2024. These spikes may result from new operational mandates, growing international cooperation, or efforts to align with NATO, EU, or other collective security standards.

The data reveal two key dynamics: (1) a sharp, short-term surge in clearances, likely signaling institutional changes such as new systems, revised protocols, or expanded roles; and (2) a subsequent stabilization, suggesting the end of large-scale vetting, improved efficiency, or a shift to routine renewals. These patterns should be interpreted within a broader institutional and security context—reflecting internal reforms and international obligations—rather than in isolation.

Reforms, institutional framework and trends in the process of issuing security clearances to MOIA and MOD (2019–2024)

Ministry of Internal Affairs — Between 2019 and 2024, the security clearance process for MOIA personnel evolved significantly due to legislative, institutional, and technological changes. Clearances peaked in 2022 with 6,760 issued, then declined and stabilized in 2023 (4,306) and 2024 (4,489).

Legislative reforms - During the period from 2019 to 2024, the important legislative reforms in the Republic of Serbia had an impact on the eligibility determination process of MOIA members (The Law on Police, 2018). The key legislative interventions in that period included the adoption of the Law on Information Security in 2019, amendments to the Law on Police, as well as the adoption of the Law on Records and Data Processing in the Area of Internal Affairs in 2018, which resulted in the procedural improvements in the sphere of security and classified information protection. These changes have defined the rights and obligations of police officers working with sensitive information – both personal data and classified information – and also precisely determined procedures for eligibility determination and security vetting.

Institutional and Technological Drivers — The rise in security-sensitive roles stems from expanded digital operations, advancing e-governance, and upgraded security infrastructure. New procedures and technologies have increased the number of positions requiring classified access, driving up demand for clearances.

Heightened Security Awareness — Increasing cyber threats and evolving internal and external risks have bolstered the MOIA's security culture. This has led to more rigorous vetting practices and a corresponding rise in issued clearances.

Post-2022 Stabilization — The decline in clearance numbers during 2023 and 2024 likely reflects the conclusion of a major vetting cycle and growing institutional maturity. Streamlined procedures have led to a steadier, more sustainable volume of new clearances.

Ministry of Defense – During the observed period, the number of issued security clearances within the defense system increased significantly, reflecting strategic and legislative actions, along with growing national and international security challenges.

Legislative and institutional reforms – Amendments to the Law on Defense and the Law on the Serbian Armed Forces in 2018, as well as by-laws, regulating the area of security vetting (The Rulebook on Personnel Security Vetting conducted by the Military Security Agency, 2015), classified information protection (Regulation on Detailed Criteria for Determining Classification Levels CONFIDENTIAL and RESTRICTED within the Ministry of Defense, 2014) and the organization of the defense system laid the foundation for strengthening mechanisms for controlling access to classified information. The introduction of new information protection measures within the defense sector required broader implementation of eligibility determination procedures for individuals and legal entities accessing classified information.

Security and Defense Infrastructure — The adoption of advanced technologies, upgraded command systems, and domestic and international security initiatives has expanded roles involving classified data, significantly increasing demand for cleared personnel.

Geopolitical and Security Challenges — Rising cyber and hybrid threats have driven efforts to reinforce Serbia’s defense system through a stable, standardized vetting framework. The surge in clearances, followed by declines in 2023 and 2024, likely marks the completion of the initial phase of implementing these enhanced procedures.

Analysis of Security Vetting by Data Type — From 2020 to 2024, MOIA and MOD personnel experienced a surge in security clearance activity, peaking in 2022 before stabilizing. Within the MOIA, the issuance of 6,760 clearances in 2022 was driven by legislative reforms and internal digitalization. Subsequent declines in 2023 (4,306) and 2024 (4,489) suggest the conclusion of mass vetting and improved procedural efficiency. The MOD followed a similar path. Amendments to the Defense Law in 2018 expanded classified positions, prompting steady clearance growth through 2022, followed by stabilization in 2023 and 2024—indicating institutional consolidation in the eligibility process. These trends highlight a deepening institutional commitment to safeguarding classified data. What began as a period of high-volume clearance issuance has matured into a phase of sustainable development. This shift reflects increased awareness of emerging security threats—cyberattacks, hybrid warfare, and digital vulnerabilities—and the adoption of a more integrated approach to data protection. Looking forward, advances in information technology, the integration of artificial intelligence, and continued alignment with international standards are expected to strengthen Serbia’s national security through more robust vetting frameworks.

Duration of eligibility determination process

Duration and Procedural Dynamics of Security Vetting — The time required for vetting procedures varies by classification level. Higher-level clearances, especially for TOP SECRET information, involve more extensive assessments—covering personal, professional, and familial backgrounds—resulting in longer processing times than those for CONFIDENTIAL access. The application of the Law on General Administrative Procedure further extends the process, as a separate

decision confirming the fulfillment of conditions must be issued and become legally effective before a clearance is granted. While legally necessary, this step can lengthen timelines, particularly during peak demand periods.

The 2022 surge in clearances placed temporary pressure on institutional capacity, leading to delays in some cases. Still, it also signaled stronger coordination and greater urgency around national information protection. In response, authorities introduced reforms—recruiting additional personnel, enhancing interinstitutional coordination, and upgrading technology through digitalization and integrated databases. These changes contributed to a more stable and efficient system in 2023 and 2024.

The trends highlight the need for ongoing refinement of vetting procedures and a strategic, resource-driven approach to ensure timely processing, legal compliance, and consistency with both national standards and Serbia's international security obligations.

Challenges and obstacles in eligibility determination process

Despite previous increases in MOIA security clearances, the eligibility determination process still faces major efficiency challenges. Contributing factors include limited staffing, weak coordination—particularly between MOIA and the National Security Council Office—and underuse of modern digital tools. Processing delays, communication gaps, and resource constraints likely contributed to the decline in clearances issued in 2023 and 2024, despite rising demand amid growing institutional and security complexity. Security vetting remains a cornerstone of national security. Addressing systemic barriers requires targeted action across three key areas:

1. Human Resource Strengthening — Investing in recruitment, training, and retention — supported by favorable work conditions — can expand operational capacity and reduce bottlenecks in the clearance process.

2. Adoption of Digital Tools — Implementing centralized electronic platforms, automating workflows, and integrating databases would improve transparency, accuracy, and institutional efficiency.
3. International and Regional Cooperation — Aligning with modernized international vetting frameworks through training exchanges and policy benchmarking would further refine Serbia's classified information protection system.

The success of these reforms hinges on coordinated institutional action, defined responsibilities, and ongoing evaluation. Only through a strategic, resource-driven approach can Serbia build a resilient, legally sound, and future-ready security clearance system.

Research problems and limitations

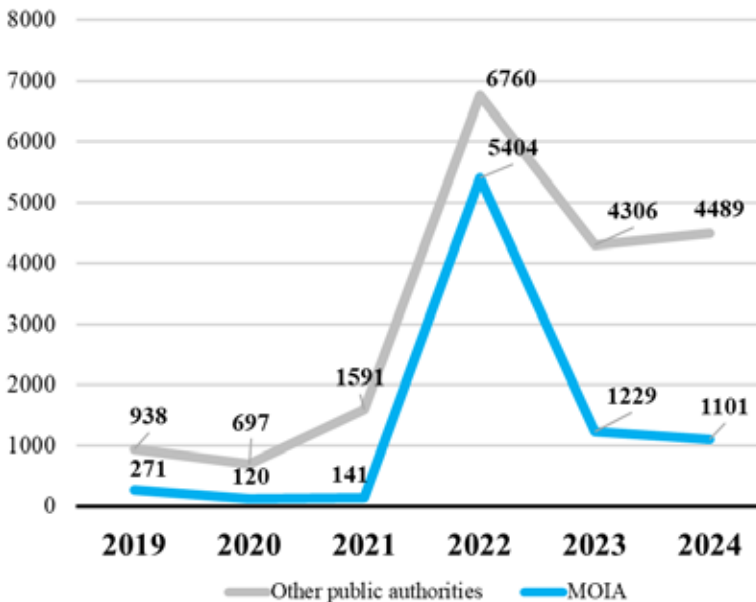
While official statistics support baseline trend analysis, they are predominantly quantitative and lack contextual depth. Missing elements—such as employee profiles, job roles, educational backgrounds, and classified-related responsibilities—limit the scope for more nuanced interpretations. Additionally, the absence of data on negative vetting outcomes and their causes restricts risk assessment and the development of targeted preventive measures. These gaps emphasize the need to strengthen data collection, especially in qualitative dimensions, to improve understanding of the security clearance landscape.

Despite these limitations, available data offers a valuable foundation for tracking long-term trends, establishing benchmarks, and institutional comparisons—particularly between MOIA and MOD. Such analysis not only supports strategic planning and procedural refinement but also enables targeted resource allocation to areas of heightened vulnerability, like MOIA's clearance framework.

Conclusion

The 2019–2024 analysis of eligibility determinations reveals a pivotal shift, with a 2022 peak in clearances driven by legislative reforms, expanded

sensitive roles, and heightened security demands. The stabilization seen in 2023 and 2024 reflects the end of an intensive vetting cycle and the rise of a more efficient, optimized system. Looking ahead, sustained investment in digital modernization, institutional coordination, and human and technical capacity is vital to ensure long-term effectiveness. Strengthening personnel vetting—both for individuals and entities—is key to safeguarding sensitive data. With these measures, Serbia can build a resilient, adaptive, and accountable clearance system that meets national security needs while aligning with international standards.



Graph 6. Growth rate of the number of issued security clearances from 2019 to 2024, correlation between MOIA and other public authorities

Sustained implementation of these efforts—alongside the proposed strategies—will be pivotal in enhancing the efficiency of vetting and clearance procedures while reinforcing Serbia’s overall framework for classified information protection and national security.

References

1. Dragišić, Z., Manojlović, D., Jović, V. (2018). Bezbednosna provera – kontraverze u radu organa bezbednosti (komparativni pravni i bezbednosni pristup). *Vojno delo*, 69(7): 156-175.
2. *Law on Classified Information*, Official Gazette of the Republic of Serbia, No. 104 of 16 December 2009.
3. *Law on Defense*, Official Gazette of the Republic of Serbia, No. 116 of 11 December, 2007; No. 88 of 28 October 2009; No. 10 of 29 January 2015; and No. 36 of 10 May 2018.
4. *Law on Information Security*, Official Gazette of the Republic of Serbia, No. 6 of 28 January 2016; No 94 of 19 October 2017, and No. 77 of 31 October 2019.
5. *Law on Police*, Official Gazette of the Republic of Serbia, No. 6 of 28 January 2016; No. 24 of 26 March 2018, and No. 87 of 13 November 2018.
6. *Law on Records and Data Processing in the Area of Internal Affairs*, Official Gazette of the Republic of Serbia, No. 24 of 26 March 2018.
7. *Law on the Serbian Armed Forces*, Official Gazette of the Republic of Serbia, No. 116 of 11 December 2007; No. 88 of 28 October 2009; No. 10 of 29 January 2015; No. 88 of 23 October 2015 (CC Decision); No. 36 of 10 May 2018; No. 94 of 27 December 2019; No. 74 of 23 July 2021.
8. Matić, G. (2019). *Sektor bezbednosti i odbrane i obrada podataka o ličnosti u Republici Srbiji*, Zaštita podataka o ličnosti u sektoru bezbednosti i odbrane – Vodič kroz zakonsku regulativu, CUPS i Misija OEBS u Beogradu, str. 27-116.
9. Matić, G., Milošević, M. (2021). *Основи безбедности*. Факултет за пословне студије и право Београд.
10. Mijalković, S. (2015). *Bezbednosno proveravanje lica – tradicionalni modeli i primeri dobre prakse*; Nauka, bezbednost, policija, 20(2): 195-208.

11. *National Security Strategy of the Republic of Serbia*, Official Gazette of the Republic of Serbia, No. 94 of 27 December 2019.
12. Office of the National Security Council and Classified Information Protection (2025), Sertifikati. , accessed on 14 April 2025.
13. *Regulation on Detailed Criteria for Determining Classification Levels “TOP SECRET” and “SECRET”*, Official Gazette of the Republic of Serbia, No.46 of 24 May 2013.
14. *Regulation on Detailed Criteria for Determining Classification Levels “CONFIDENTIAL” and “RESTRICTED”*, Official Gazette of the Republic of Serbia, No. 105 of 29 November 2013.
15. *Regulation on Detailed Criteria for Determining Classification Levels “CONFIDENTIAL” and “RESTRICTED” within the Ministry of Defense*, Official Gazette of the Republic of Serbia, No. 66 of 29 June 2014.
16. *Regulation on the Content, Form and Method of Maintaining Records for Access to Classified Information*, Official Gazette of the Republic of Serbia No. 89 of 29 November, 2010.
17. *Regulations on Forms of Security Questionnaires*, Official Gazette of the Republic of Serbia, No. 30 of 7 May 2010.
18. *Rulebook on Personnel Security Vetting Conducted by the Military Security Agency*, Official Military Gazette, No. 25 of 21 September 2015.

Анализа трендова у безбедносним проверама припадника Министарства унутрашњих послова у контексту спровођења Закона о тајним подацима (2019–2024)

Апстракт: Овај рад анализира трендове и кључне чиниоце у процесу издавања безбедносних сертификата у Републици Србији у периоду од 2019. до 2024. године, са посебним освртом на развој људских ресурса, управљање подацима и примену правног оквира. Кроз анализу података о издатим безбедносним сертификатима, процењује се утицај међународних стандарда, измена безбедносне политике и институционалних реформи на осигурање безбедносних провера. Истраживање указује на постојеће изазове, нарочито у примени законодавства и осигурању транспарентности процеса и открива недостатке у квалитету и интеракцији података. Рад предлаже циљана побољшања, укључујући дигитализацију процедура, јачање међуинституционалне сарадње и стандардизовано извештавање. Закључно, размајрају се ефекти предстојећих правних реформи и дају препоруке за јачање кадровских капацитета и увођење специјализованих обука ради ефикасније примене нових стандарда.

Кључне речи: национална безбедност, заштитна тајних података, персонална безбедност, процес издавања безбедносних сертификата.

Санела Д. АНДРИЋ¹

Криминалистичко-полицијски универзитет у Београду

Ана С. МУТАВЏИЋ²

Криминалистичко-полицијски универзитет у Београду

Весела М. МИЛОВАНОВИЋ³

Министарство унутрашњих послова Републике Србије

ДОИ: 10.5937/bezbednost2503143A

УДК: 004.056.5:572.087

174:351.755.62

Прегледни научни рад

Примљен: 7. 8. 2025. године

Ревизија: 9. 10. 2025. године

Датум прихватања: 24. 11. 2025. године

Етички и безбедносни аспекти употребе отисака папиларних линија као биометријске идентификације

Апстракт: Поред свег развоја технике и технологије, истраживања папиларних линија и даље представља најраспрострањенији метод реистрације и идентификације особа. Јединствености, универзалности, непроменљивости и преносивости чине отиске папиларних линија поузданом научно верификованом биометријском карактеристиком. У криминалистичкој техници (форензици) метод дигитализације користи се за реистрацију и идентификацију особа у циљу истраживања учиниоца кривичних дела. Међутим, у савременом друштву, под утицајем развоја информационо-комуникационих технологија, идентификација помоћу отисака папиларних линија користи се у „цивилном сектору“ за откривавање сигурносних бртва, сефова, мобилних телефона, рачунара и слично. У раду је даје преглед основних карактеристика отисака папиларних линија, са освртом на монода-

¹ sanela.andric@kpu.edu.rs

² ana.mutavdzic@kpu.edu.rs

³ vesela.milovanovic@mup.gov.rs

књигописирање и акценцијом на етичким и безбедносним аспектима њихове (зло)употребе као биометријске карактеристике.

Кључне речи: етика, безбедност, полицajsка етика, отисци папиларних линија.

Увод

Савремена криминалистичка техника (форензика) за идентификацију особа користи биометријске карактеристике попут отисака папиларних линија прстију, дланова и табана, очне ретине/ириса, ДНК профила и записа гласа. Раније су се за регистрацију и идентификацију учинилаца кривичних дела користиле различите рудиментарне (застареле) и неетичке методе, попут сакаћења, жигосања, осмуђивања (код мушкараца), али и антропометрија, која представља први покушај научне регистрације и идентификације особа. С развојем наука, нарочито криминалистичке технике (форензике) и информатике (информационо-комуникационих технологија) долази до установљавања и развоја савремених метода за регистрацију и идентификацију особа које се заснивају на научним и етичким принципима и које су олакшале процес проналажења учинилаца кривичних дела. У савременом друштву биометрија је добила ширу употребу у цивилном сектору и користи се свакодневно за идентификацију и верификацију особа. Биометријски системи који се користе за регистрацију и идентификацију особа јесу: АФИС (AFIS – *Automated Fingerprint Identification System*), ДНК, 3Д фотометрија, антропологија и фацијална реконструкција, геометрија лица, геометрија длана, распоред вена, изглед очне ретине и ириса, анализа телесних мириса, одонтолошка идентификација, фоноскопија, анализа рукописа и потписа (Бјеловук, 2022: 27).

Правни основ за форензичку регистрацију⁴ у Републици Србији дају следећа правна акта: *Закон о полицији*, који дефинише полицијске послове и послове криминалистичко-форензичке идентификације, *Законик о кривичном процесу*, који уређује процедуру узимања биометријских узорака, односно узорака биолошког порекла, затим *Закон о евиденцијама и обради података у области унутрашњих послова*, који регулише утврђивање идентитета, *Закон о заштити података о личности*, који спречава злоупотребу прикупљених података, док *Закон о националном ДНК регистру* уређује област вођења Националног ДНК регистра. Правилник о криминалистичко-форензичкој регистрацији, узимању других узорака и криминалистичко-форензичким вештачењима и анализама регулише поступање полицијских службеника током форензичке регистрације (Бјеловук, 2022: 29–31). У члану 62 Закона о полицији истакнуто је да су полицијски службеници овлашћени да врше криминалистичко-форензичку регистрацију, док се у члану 64 као врсте полицијских овлашћења наводе провера и утврђивање идентитета лица (Закон о полицији).

Папиласкопија, која је првобитно настала као метод регистрације и верификације особа у циљу проналаска учиниоца кривичних дела, у савременом друштву има ширу употребу. Данас отисци папиларних линија за верификацију особа имају распрострањену (цивилну) употребу и користе се за осигуравање/откључавање сигурносних брава, сефова, мобилних телефона, рачунара и слично. Отисци папиларних линија су јединствени за сваку особу и не мењају се током живота. У поређењу са лозинкама и картицама теже их је копирати и украсти, омогућавају брзу аутентификацију, нарочито на мобилним уређајима, у банкарству и контроли приступа. Међутим, њихова употреба носи и одређене ризике. Биометријске базе могу бити мета хакера и „цурење” ових података је трајни безбедносни ризик, те се могу користити без информисаног пристанка у системима за праћење и масовни надзор.

⁴ Регистрационе збирке су базе података о личности које садрже биометријске податке и евиденције. Погледати опширније у: Бјеловук, И. (2022). *Криминалистичка техника*. Криминалистичко-полицијски универзитет, Београд.

Трагови папиларних линија као биометријска идентификација

Папиларне линије су рељефне линије на кожи прстију, дланова и табана које формирају цртеже. Представљају идентификационе карактеристике које имају велики значај за криминалистичку технику, односно форензику. С обзиром на то да папиларне линије формирају графички цртеж и садрже отворе/завршетке знојних и лојних жлезда, оне уједно представљају и морфолошку и биолошку идентификациону карактеристику сваке особе. Морфолошки, оне остављају цртеж, односно траг који је јединствен за сваку особу, док биолошки представљају извор ДНК материјала јер су папиларне линије прстију, дланова и табана прекривене знојем и епителним ћелијама које се перманентно љуште са коже (Бјеловук, 2022: 41–42; Бјеловук, Ламовец & Васовић, 2023: 29). Научно верификоване идентификационе карактеристике папиларних линија јесу универзалност, непроменљивост, индивидуалност, могућност груписања и преносивост. То значи следеће: да папиларне линије на прстима, длановима и табанима поседују сви људи на свету; да се оне формирају још у трећем гестацијском месецу и образују цртеж који се не мења током живота већ се сразмерно увећава; да су јединствене код сваког човека, нису исте на прстима једне шаке, не понављају се ни код једнојајчаних близанаца јер постоји разлика у врсти и положају минуција; може се извршити типизација цртежа папиларних линија; остављају латентне површинске трагове јер су константно прекривене знојем (Бјеловук, 2022: 42–43).

За визуелизацију латентних трагова папиларних линија користе се физичке и хемијске методе. Као физичке методе користе се разне врсте дактилоскопских прахова и суспензија које се заснивају на адхезивној сили и које не доводе до физичке реакције између зноја и супстанце која се користи за визуелизацију. Дактилоскопски прахови који се најдуже користе јесу: златни прах, графитни или угљени прах, магнетни прах, прашкови у боји и флуоресцентни прашкови/УВ прашкови (Бјеловук, 2022: 176). Нове мање штетне методе заснивају се на (био)полимерним материјалима, попут декстрана као компоненте праха за визуелизацију латентних трагова. Декстран је биоразградив

и биокомпатибилан, нетоксичан је и спречава штетне ефекте по особе које га користе (Vučković, et al., 2021a: 149–160; Vučković, et al., 2020b: 83–86). Хемијске методе за изазивање латентних трагова папиларних линија подразумевају употребу реагенса који изазивају хемијску реакцију са неком супстанцом из зноја, а примењују се код трагова на порозним подлогама попут хартија и платна. Реагенси који се најчешће користе у хемијским методама јесу сребро-нитрат (AgNO_3), нинхидрин, ДФО (ДФО), ИНД (ИНД) и ПД (ПД) раствори (Бјеловук, 2022: 180–184). Након изазивања/визуелизације, трагови папиларних линија се фиксирају, фотографишу размерном камером, описују у увиђајном записнику и изузимају са места догађаја дактилоскопским фолијама. Дактилоскопска фолија може бити црна, бела и желатинаста (Бјеловук, 2022: 179).

Дактилоскопија је метод за регистрацију и идентификацију на основу папиларних линија на кожи прстију. Декадактилоскопија је метод за регистрацију и идентификацију особа на основу проучавања папиларних линија на свих десет прстију (*deka* – десет, *dactilo* – прст, *skopein* – гледати, посматрати), док је монодактилоскопија метод за регистрацију и идентификацију особа на основу проучавања папиларних линија на једном прсту (*monos* – један, *dactilo* – прст, *skopein* – гледати, посматрати). У савременој криминалистичкој техници/форензици картотека дактилоскопске збирке дигитализована је и преведена у АФИС систем (Бјеловук, 2022: 46).

Безбедносни аспект биометријских система

Отисци папиларних линија представљају најраспрострањенији метод биометријске идентификације особа и пружају високу прецизност и ефикасност. Регистрација и идентификација на основу отисака папиларних линија комфорна је и неинвазивна, а с развојем технике и технологије, нарочито информационо-комуникационих технологија, њена употреба је знатно олакшана. Међутим, њихова употреба отвара низ етичких питања и могућност злоупотребе, попут нарушавања приватности, крађе идентитета,

неовлашћеног прикупљања, злоупотребе од стране државних органа, „подметања” отисака и слично, иако се сугерише се да су биометријски идентификациони документи имуни на ове злоупотребе или изузетно отпорни на њих, те да су заправо облик заштите од њих (Alterman, 2003: 139). Технологија отисака прстију је тренутно најпоузданија, уз тврдњу да је стопа лажног прихватања (FAR) и стопа лажног одбијања (FRR) 0,01% или мања. То значи да се мање од једне особе од 10.000 људи упари са туђим отисцима прстију (FAR) или се не упари са сопственим отисцима прстију (FRR). Односно, ако неко жели да нас верификује/идентификује, наши отисци прстију ће нас идентификовати у 99,99 случајева од 100. Међутим, да ли је заиста тако?

Недавно је Међународна организација цивилног ваздухопловства (ICAO) усвојила глобални хармонизовани план за интеграцију биометријских идентификационих информација у пасоше и друге машински читљиве путне исправе. Међутим, повезивање биометријских база података може представљати опасност по заштиту података о личности, а масовна употреба биометријских система може довести до социјалне контроле и дискриминације, нарочито у ауторитарним режимима, где се такви системи могу (зло)употребити за праћење и контролу грађана. Биометријске идентификације потенцијално могу нанети штету појединцима, кроз кршење грађанских слобода и права. Чак ни људи са кривичним досијеом тренутно нису нужно криминалци, те органи за спровођење закона немају право да спроводе надзор над општом популацијом без икаквих доказа и основане сумње. (Alterman, 2003; Sutrop & Laas-Mikko, 2012). „Етика биометријске идентификације не може да почива на претпоставци да су подаци апсолутно безбедни” (Alterman, 2003: 142).

Биометријски систем је аутоматски систем за идентификацију и аутентификацију особа који користи јединствене биолошке карактеристике појединца, попут отиска прста, лица, дужице ока, гласа, мрежњаче и слично. Због високе ефикасности биометријског система отисака прстију у верификацији и идентификацији особа, бројне владине и приватне организације користе овај сис-

тем у безбедносне сврхе (Joshi et al., 2018). Биометријски системи данас имају широк опсег примене – од система за евиденцију радног времена малих компанија до система контроле приступа за нуклеарне уређаје; од контроле приступа, контроле граница, војних база, заштите осетљивих података, преко банкомата, кредитних картица, онлајн трансакција до заштите приватних рачунара и мобилних телефона. Међутим, иако употреба биометрије побољшава безбедност, сами биометријски системи су рањиви и подложни спољашњим претњама (хаковање и претња малициозним програмима), тако да је све већа употреба биометрије у безбедносне сврхе наметнула потребу за истраживањем метода напада на биометријске системе (Alaswad et al., 2014).

Напади на биометријске уређаје и системе деле се у четири групе: 1) напади на нивоу обраде и преноса, 2) напади на нивоу улаза (*input*), 3) напади на позадину (*back-end*), 3) напади на (биометријски) упис и 4) напади током процеса пријављивања (Alaswad et al., 2014).

Напади на улазном нивоу (*input*) дешавају се у тренутку прикупљања података, те системи морају имати резервне процесе у случају квара. Најчешћи улазни напади су спуфинг (*spoofing* – имитација отиска прста), пропуштање или саботажа уређаја (*buffer overflow*, прекомерно светло које омета сензор, кратак спој или прекидање улазних података). Напади на позадински систем (*background*) јесу напади на системе за упоређивање узорака или одлучивање. Најчешћи су напади на базу, збирку отисака, при чему може доћи до крађе идентитета. На крају, напади током процеса пријављивања обухватају коришћење лажних докумената за идентификацију, сарадњу са корумпираним службеницима и хаковање електронског система за пријаву. Заштита од свих наведених напада подразумева енкрипцију, заштићену комуникацију и систем за откривање неовлашћених измена података (Alaswad et al., 2014).

Када је реч о биометријском систему отисака прстију, идентификовано је шеснаест тачака напада. Тај систем може бити мета напада администратора система, овлашћеног корисника, лаика који покреће *DoS* напад коришћењем биометријске апликације

је попут банкомата или противника (хакера) који поседује знање о биометријском систему. Напади који долазе од администратора система називају се инсајдерским нападима или административним преварама. Тачке напада на биометријски систем су следеће: 1) директни и индиректни напад – директни напад се врши приказивањем биометријских карактеристика регистроване особе циљањем улазног уређаја или апликације како би се приступило систему, док се код индиректног напада подразумевају стручност и познавање биометријских система како би се пресреле информације. Овде ћемо нагласити да су поједини аутори извршили процену рањивости система за верификацију отисака прстију која је показала да је преко 75% покушаја директног напада било успешно, док су други аутори доказали да 11 различитих система за препознавање отисака прстију прихвата вештачки створене лепљиве (желатинске) прсте; 2) одбацивање – искоришћавање ограничења биометријског система феноменом лажног прихватања; 3) контаминација или прикривена аквизација (преузимање) – несвесно остављање отисака папиларних линија у свакодневној рутини које нападач користи за генерисање лажних отисака тако што врши визуелизацију и подизање латентних трагова и прављење калупа (мулажирање); 4) присила – нападач може употребом силе натерати особу да унесе своје биометријске податке, а могућност ових инцидената постоји на недовољно обезбеђеним банкоматима; 5) немар – овакви напади се дешавају уколико особа заборави да се одјави са биометријске апликације; 6) администратор система или овлашћено лице могу покренути напад; 7) напади на сензоре манипулисањем биометријским подацима – напад лажним отиском, креирањем лажног прста или мењањем отиска регистроване особе и слично; 8) напади помоћу екстракције карактеристика – циљање модула за екстракцију карактеристика тако да он постане неспособан да генерише стварну карактеристику која одговара достављеном отиску прста; 9) напад на модул техничке заштите шаблона – нападач циља информације у вези са кључем у алгоритму који се користи за шифровање (енкрипцију); 10) напади на модул за подударање, хардверску или софтверску компоненту која је одговорна за извршавање подударања током фазе аутентификације; 11) напад на базу података шаблона/збирке отисака – циљање на

базу података директно или индиректно путем споља компроми-тованог система како би се поново употребили или изменили шаблони/збирке отисака; 12) напад типа „човек у средини” – нападач пресеће комуникациони канал како би прикупио биометријске податке легитимне особе; 13) измена права приступа – уписивање корисника са различитим привилегијама или правима приступа у биометријски контролисану апликацију; 14) поништавање одлуке – нападач користи тзв. тројанског коња (компјутерски вирус) да поништи модул за одлучивање и окрене резултат верификације у своју корист; 15) напад ускраћивања услуге (DoS) – убацивање мноштва лажних захтева за приступ („бомбардовање система”) до тачке у којој рачунарски сервер није више у могућности да обради валидне захтеве; 16) упад – нападач проваљује у складиште шаблона преко екстерног система. На крају, постоје и напади без напора услед системских ограничења. Овде се мисли на нетачну аутентификацију и одбијање услед лажног неподударања (Joshi et al., 2018: 4–10).

Поред наведених тачака напада на биометријске системе постоје четири модела претњи које представљају начин да се идентификују различите могућности напада или потенцијалне претње и рањивости у биометријском систему (Joshi, 2018). Први модел дали су Рата и сарадници (*Ratha et al. model*). Овај модел на основу приступне тачке информација у биометријском систему идентификује осам слабости (рањивости) које доводе до специфичног типа напада – напад на сензоре, односно, лажна биометријска презентација на сензору; напад пресретањем комуникационог канала између сензора и екстрактора карактеристика; напад заобилажењем модула за екстракцију карактеристика помоћу тројанског коња; напад на комуникациони канал између екстрактора карактеристика и упаривача; напад на модул за подударање и поништавање резултата помоћу тројанског коња, како би генерисао висок резултат подударања и послао позитиван одговор биометријски контролисаној апликацији и потпуно заобишао процес аутентификације; напад који помаже уљезу да истражи начине за цурење података, што омогућава прикупљање шаблона и њихову модификацију; напад на комуникациони канал између базе пода-

така шаблона и модула за подударане како би нападач прикупио шаблоне и директно их репродуковао или изменио да би приступио систему са идентитетом различитих корисника; напад који омогућава заобилажење свих компоненти система и директно манипулисање одлуком система у своју корист како би се поништиле карактеристике перформанси биометријске апликације. Други модел претњи је модел „рибље кости” (*The fishbone model*) који приказује пет узрока рањивости биометријских система: унутрашњи квар, администрација, инфраструктура, небезбедна обрада и патент или биометријска отворености. Овај модел наглашава опште грешке које треба избегавати и безбедносне технике које треба имплементирати у биометријске системе. Најједноставнији начин за обезбеђивање биометријског система јесте чување шаблона и системских модула (компоненти) на паметним картицама. Трећи модел дали су Нагар и сарадници (*The Nagar et al. model*). Овај модел се наслања на модел „рибље кости” при одређивању узрока рањивости биометријских система – небезбедна инфраструктура, очигледност биометрије и унутрашњи квар. Четврти модел су направили Бартлоу и Цукић (*Bartlow and Cukic framework*) и разложен је на неколико модула и подсистема – модул административног посматрања односно управљања системом, подсистем ИТ окружења и биометријски подсистем. Овај модел се може користити само као референтна вредност за тестирање и валидацију постојећих и предложених безбедносних техника (Joshi et al., 2018: 10–14). Међутим, биометријска аутентификација је последњих година заменила лозинке и постала најпопуларнији модел аутентификације па заштита биометријских података постаје приоритет. (Lovisotto, et al., 2020)

Када је у питању Република Србија, биометријски подаци (фотографија, отисци прстију и потпис) који се прикупљају приликом издавања путних и личних исправа користе се искључиво за ту сврху, односно само за изразу и проверу идентитета у вези са личним и путним исправама. Обрада биометријских података строго је ограничена *Законом о заштити података о личности* и *Законом о њеним исправама*, податке обрађује искључиво Минис-

тарство унутрашњих послова (МУП) ради издавања докумената и вођења евиденција, те се узети подаци не смеју користити у друге сврхе без изричите законске основе. Међутим, у оквиру кривичног поступка или међународне сарадње, уз судски налог или на основу међународног уговора, могућа је употреба биометрије за идентификацију лица. Министарство унутрашњих послова, као надлежни орган који прикупља биометријске податке приликом издавања личних и путних исправа, има право приступа тим подацима за издавање докумената, искључиво за проверу идентитета, у оквиру истрага (ако се трага за особом), у сарадњи са другим државним органима у складу са законом (тужилаштво, суд). МУП не може давати те податке трећим лицима без јасног законског основа. Тако, на пример, здравствене установе немају приступ биометријским подацима из система за путне исправе. Те податке могу користити искључиво у специфичним случајевима, као што су вештачења у судским поступцима, одлуке суда (у кривичном поступку) и хитне мере по одобрењу надлежног органа. У редовним здравственим поступцима (пријем, лечење, дијагноза) нема основа за коришћење података као што су отисци прстију или дигитални потпис из пасоша. Такође, установе образовног система (школе, факултети) немају никакво законско овлашћење да приступају или користе биометријске податке из система МУПРС. Чак и ако се ради о идентификацији ученика (нпр. за испите или евиденцију присуства), она се може спроводити само на основу података које ове установе прикупљају саме, уз сагласност ученика или њихових родитеља.⁵

На крају је неопходно да се осврнемо на могућности смањења безбедносних ризика употребе отисака папиларних линија као биометријске идентификације, односно, биометријских подата-

⁵ Информисати се опширније у: *Закон о йолицји*, Службени гласник Републике Србије, бр. 6/2016, 24/2018 и 87/2018, *Закон о йуйним исыравама*, Службени гласник Републике Србије, бр. 90/2007, 116/2008, 104/2009, 76/2010, 62/2014 и 81/2019, и *Закон о зашйиийи йодайшака о личностйи*, Службени гласник Републике Србије, бр. 87/2018.

ка уопштено. Непроменљивост отисака прстију уједно представља и предност и ману. Предност је брза и једноставна идентификација, а мана је то што биометријски подаци не могу бити замењени уколико су угрожени. На пример, уколико су лозинка или број кредитне картице на мети хакера, они се могу заменити, док код отисака прстију та опција не постоји. Да би се безбедносни ризик умањио, уводи се концепт поништиве биометрије (*cancelable biometrics*), који су предложили Рата и сарадници (Ratha, et al., 2001). Поништива биометрија представља концепт у којем се оригинални биометријски податак (нпр. отисак прста) намерно трансформише (деформише) математичком функцијом у нови, изведени шаблон, који се користи за идентификацију и аутентификацију, док се оригинал никада не чува. Ако тај шаблон буде компромитован, може се једноставно „поништити” и заменити новим, применом другачије трансформације над истим биометријским узорком – слично као промена лозинке. На тај начин, поништива биометрија омогућава ревокацију и поновно издавање биометријских података, чиме се смањује ризик неповратног губитка приватности који постоји код традиционалних биометријских система, где се једном откривени отисак не може променити (Ratha, et al., 2001, 628–633).

Етички аспект и могућност злоупотребе биометријских података

Претпоставке о неовлашћеном приступу и коришћењу биометријских података могуће су као и са свим другим подацима о личности. С развојем информационо-комуникационих технологија и вештачке интелигенције (AI) наши подаци се налазе свуда и потенцијално су свима доступни. Свакодневно остављамо шифре на разним серверима, користимо отисак прста за приступ паметним телефонима и рачунарима, а сви ти подаци остају похрањени у „неком делу интернета”. Стога је легитимно поставити питање о безбедности личних подата. Међутим, прецизних истраживања и података о злоупотреби биометријских података у нашој држави још увек нема.

Такође, када је реч о етичком аспекту (зло)употребе отисака прста као биометријске идентификације, домаћих истраживања нема. С развојем информационо-комуникационих технологија појавила се и нова врста криминала – високотехнолошки криминал – и требало би истраживања окренути у том смеру. Засад нам примери злоупотребе биометријских података долазе из Индије, Кине и Сједињених Америчких Држава (САД). Индијски национални биометријски систем складишти отиске прстију од више милијарди грађана. У октобру 2023. године дошло је до „цурења” података када се десио безбедносни пропуст на систему за документа Вест Бенгал (*West Bengal*). Фотографије и отисци прстију корисника били доступни јавности пре него што је грешка уочена и отклоњена. Полицији су стизале пријаве да су криминалне групе клонирале отиске прстију из регистара, правиле силиконске отиске и вршиле аутентификације, чинећи кривично дело неовлашћене банковне трансакције. Наводи се да је 500 GB података „процурело” са сервера фирме Зелена мисао (*ThoughtGreen*), а грешка је омогућила нападачу на систем (хакеру) да погоди шеснаестоцифрене шифре за издавање власничких права (*Biometric update.com*, 2023).⁶ Затим је у Кини забележен случај масовног кршења људских слобода и права неетичним и присилним узимањем биометријских података. Хјуман рајтс воч (*Human Rights Watch*) утврдио је да су кинеске власти систематски прикупљале биометријске податке становника Ујгурског региона – отисак прста, глас, ДНК, ирис – формирајући централизован надзор и профилисање локалног становништва. Биометријски подаци коришћени су за надзор кретања, детекцију „неповерења” и друге облике контроле мањинске заједнице. Становници су без пристанка подвргнути биометријској идентификацији и присилној интервенцији кампова за преваспитавање (*re-education*). Од краја 2016. године, кинеска влада је подвргла 13 милиона етничких Ујгура и других муслимана у Син-

⁶ Цео текст погледати на: *State government fixes bug exposing Aadhaar biometric records*, *Biometric.com*, Oct 13, 2023, 1:09 pm EDT | Chris Burt, https://www.biometricupdate.com/202310/state-government-fixes-bug-exposing-aadhaar-biometric-records?utm_source=chatgpt.com, доступан 29. 7. 2025.

Ћангу масовном произвољном притварању, присилној политичкој индоктринацији, ограничењу кретања и верском угњетавању. Процене указују да се под овом појачаном репресијом скоро милион људи држи у камповима за „политичко образовање”. Владина „Кампања снажног удара против насилног тероризма” претворила је Синђанг у један од главних кинеских центара за коришћење иновативних технологија у сврху друштвене контроле. Извештај који је поднео Хјуман рајтс воч пружа детаљан опис и анализу мобилне апликације коју полиција и други званичници користе за комуникацију са Интегрисаном платформом за заједничке операције (IJOP, 一体化联合作战平台), једним од главних система које кинеске власти користе за масовни надзор у Синђангу. Хјуман рајтс воч је први пут известио о тој платформи у фебруару 2018. године, напомињући да полицијски програм прикупља податке о људима и пријављује званичницима оне које сматра „потенцијалном претњом”. Поједине особе су притворене и послате у кампове за политичко образовање и друге установе. „Обрнутим инжењерингом” ове мобилне апликације тачно је утврђено које врсте понашања и људи циља овај систем масовног надзора (*Human Rights Watch*, 2019).⁷ Трећи случај долази из САД, где је тексашки тужилац 2022. године поднео пријаву против компаније Мета (Фејсбук – *Facebook*) због наводног складиштења отисака прстију и гласовних записа без информисаног пристанка корисника како захтева државни закон. Компанија Мета је претходно платила 650 милиона америчких долара (USD) за тужбу због незаконите употребе биометријских података у држави Илиноис. Речима државног тужиоца Тексаса Кена Пакстона, Мета је 2022. године пристала да плати 1,4 милијарде долара тужбу државе Тексас због неовлашћеног прикупљања биометријских података корисника. То је други највећи споразум компаније Мета са савезним или државним законодавцима, након споразума од пет милијарди долара са Феде-

⁷ Цео извештај погледати на: *Human Rights Watch*, China's Algorithms of Repression, Reverse Engineering a Xinjiang Police Mass Surveillance App, https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass?utm_source=chatgpt.com, доступан 29. 7. 2025.

ралном трговинском комисијом из 2019. године због кршења приватности потрошача (*Axios*, 2022).⁸ На основу наведених примера индикативне су могућности етичке злоупотребе биометријских података, било да су у питању државне службе или приватне компаније. „Цурење” и злоупотреба података могуће су услед грешке на серверима и злоупотребе службеног положаја, а последице се крећу од кривичних дела која врше криминалне групе до државне контроле коју спроводе владине институције.

Етички аспект (зло)употребе отисака папиларних линија као биометријске идентификације односи се пре свега на заштиту приватности и аутономије појединца, као и на одговорност институција које те податке прикупљају и користе. Да би се спречиле злоупотребе, неопходно је увести низ техничких, правних и организационих мера које ће осигурати да се биометријски подаци користе искључиво у сврху за коју су прикупљени и омогућити да корисник има контролу над својим подацима. Пре свега, прикупљање биометријских података мора бити засновано на информисаном и добровољном пристанку, уз јасно објашњење где, на који начин и колико дуго ће се прикупљени подаци чувати. Институције треба да се придржавају начела минимизације података (прикупљање само онога што је неопходно) и да обезбеде строгу контролу приступа и шифровање шаблона. Неопходна је и законска регулатива, односно, прописивање санкција за неовлашћено прикупљање (без информисаног пристанка), обраду и/или дистрибуцију биометријских података, као и надзор независних тела. Поред тога, треба промовисати етичку одговорност и транспарентност. Тачније, корисници морају знати како се њихови подаци користе и имати право на приступ, кориговање или брисање својих биометријских података. Комбинација технолошке заштите, правне контроле и (про)етичке свести представља најделотворнији начин за спречавање злоупотреба.

⁸ Цео текст погледати на: *Texas AG sues Meta for allegedly exploiting users' biometric data*, *Axios.com*, https://www.axios.com/2022/02/15/texas-facebook-meta-biometric-data?utm_source=chatgpt.com, доступан 29. 7. 2025.

На крају можемо поставити филозофско-етичко питање: ако се узимање биометријских података заснива на добровољности и неприсилности, а њихово похрањивање у базе података је обавезно ради утврђивања идентитета и уређено законом, да ли се онда заиста заснива на добровољности? И да ли се заиста безбедност особа и података о личности може гарантовати вулнерабилним биометријским системима? Бројна етичка и безбедносна питања се отварају, те је неопходно да се спроведу домаћа истраживања и да се покуша дати одговор на егзистенцијалистичко питање – колико смо заиста безбедни?

Закључак

Трагови папиларних линија, као јединствено и непроменљиво морфолошко обележје сваког појединца, представљају један од кључних елемената у области криминалистичке технике и форензичке идентификације. Њихова универзалност, индивидуалност и могућност типизације омогућавају ефикасно повезивање физичких трагова са конкретним лицима, што значајно доприноси откривању и расветљавању кривичних дела и идентификацији учиниоца. Посебан значај у криминалистичкој пракси има монодактилоскопија, која омогућава идентификацију на основу отисака само једног прста, што је од пресудне важности у случајевима када се на месту кривичног догађаја налазе само делимични трагови. Међутим, у савременом друштву је дошло до ширења употребе метода биометријске идентификације помоћу отисака папиларних линија и на цивилни сектор, те се он свакодневно користи за откључавање личних рачунара и мобилних телефона, сигурносних брава и сефова, за верификацију и одобрење приступа објектима и слично.

Развој савремених технологија, посебно информационо-комуникационих технологија и биометријских система као што је АФИС, значајно је унапредио брзину и ефикасност идентификације, али истовремено отворио и бројна етичка и правна питања. Биометријски подаци, укључујући трагове папиларних линија,

представљају осетљиву категорију личних података чија заштита захтева изузетну пажњу. Могућности њихове злоупотребе, посебно у контексту неовлашћеног надзора, профилисања и нарушавања приватности, намећу потребу за јасним и прецизним нормативним оквирима који ће регулисати прикупљање, обраду и чување ових података. Рањивост биометријских података, нарочито биометрије отисака папиларних линија, произилази из њихове широке употребе у верификацији и идентификацији особа, од система за евиденцију радног времена, система контроле приступа, контроле граница, војних база, заштите осетљивих података, преко банкомата, кредитних картица, онлајн трансакција до заштите приватних рачунара и мобилних телефона. У Републици Србији, правни основ за формирање и коришћење регистрационих збирки представљају *Закон о полицији*, *Законик о кривичном поступку*, *Закон о евиденцијама и обради података у области унутрашњих послова*, *Закон о заштити података о личности* и *Закон о националном ДНК регистру* који уређује област вођења Националног ДНК регистра, док *Правилник о криминалистичко-форензичкој идентификацији* регулише поступање полицијских службеника током форензичке регистрације.

Упркос очигледним предностима, верификација и идентификација особа на основу отисака папиларних линија као биометријска метода није лишена недостатака, а услед тога ни бројних изазова. Биометријски системи су подложни бројним врстама напада, попут хаковања, крађе идентитета и манипулације подацима, али и злоупотреби од овлашћених лица и државних органа. Поред тога, етичке дилеме у вези са приватношћу, добровољношћу и транспарентношћу обраде, складиштења и чувања података остају нерешене. Иако национални закони, попут *Закона о заштити података о личности*, штите грађане од злоупотребе, технолошки развој и недовољна информисаност јавности остављају простор за потенцијалне злоупотребе. Чињеница да су биометријски подаци све заступљенији у свакодневnoj употреби, а да притом нема довољно домаћих истраживања о њиховој безбедности, указује на потребу за критичким преиспитивањем, едукацијом јавности и сталним

унапређењем правне регулативе и технолошке заштите. У светлу тога, поставља се суштинско питање – да ли смо заиста безбедни у друштву које све више зависи од система који, иако ефикасни, нису непогрешиви.

Закључно, трагови папиларних линија задржавају свој статус једног од најпоузданијих извора идентификације у криминалистичкој пракси. Међутим, њихова примена мора бити заснована на начелима законитости, пропорционалности и поштовања основних људских права, како би се обезбедила равнотежа између безбедносних потреба друштва и заштите индивидуалне слободе.

Литература

1. Alaswad, A. O., Montaser, A. H., Mohamad, F. E. (2014). Vulnerabilities of biometric authentication threats and countermeasures. *International Journal of Information & Computation Technology*, 4(10): 947–58.
2. Alterman, A. (2003). “A piece of yourself”: Ethical issues in biometric identification. *Ethics and information technology*, 5(3): 139–150.
3. Бјеловук, И. (2022). *Криминалистичка техника*. Криминалистичко-полицијски универзитет, Београд.
4. Бјеловук, И., Ламовец, Ј., Васовић, Р. (2023). Визуелизација латентних трагова папиларних линија на бакарним површинама таложеном метала. *Безбедност*, 65(3): 29–45.
5. Vučković, N., Glođović, N., Radovanović, Ž., Janačković, Đ., Milašinović, N. (2020a). A novel chitosan/tripolyphosphate/L-lysine conjugates for latent fingerprints detection and enhancement. *Journal of Forensic Sciences*, 66(1): 149–160.
6. Vučković, N., Dimitrijević, S. D., Milašinović, N. (2020b). Visualization of Latent Fingerprints Using Dextran-based Micropowders Obtained From Anthocyanin Solution. *Adli Bilimler ve Suç Araştırmaları*, 2(2): 83–133.
7. Joshi, M., Mazumdar, B., Dey, S. (2018). Security vulnerabilities against fingerprint biometric system. *arXiv preprint arXiv:1805.07116*.

8. Lovisotto, G., Eberz, S., Martinovic, I. (2020, September). Biometric backdoors: A poisoning attack against unsupervised template updating. In *2020 IEEE European Symposium on Security and Privacy (EuroSecP)*, pp. 184–197.
9. Ratha, N. K., Connell, J. H., Bolle, R. M. (2001). Enhancing security and privacy in biometrics-based authentication systems. *IBM systems Journal*, 40(3): 614–634.
10. Закон о полиции, Службени гласник Републике Србије, бр. 6/2016, 24/2018 и 87/2018.
11. Закон о поиним исправама, Службени гласник Републике Србије, бр. 90/2007, 116/2008, 104/2009, 76/2010, 62/2014 и 81/2019.
12. Закон о заштити података о личности, Службени гласник Републике Србије, бр. 87/2018.
13. Sutrop, M., Laas-Mikko, K. (2012). From identity verification to behavior prediction: Ethical implications of second generation biometrics. *Review of policy research*, 29(1): 21–36.

Електронски извори

1. *Human Rights Watch*, China's Algorithms of Repression, Reverse Engineering a Xinjiang Police Mass Surveillance App, https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass?utm_source=chatgpt.com, доступан 29. 7. 2025.
2. *State government fixes bug exposing Aadhaar biometric records*, Biometric.com, Oct 13, 2023, 1:09 pm EDT | Chris Burt, https://www.biometricupdate.com/202310/state-government-fixes-bug-exposing-aadhaar-biometric-records?utm_source=chatgpt.com, доступан 29. 7. 2025.
3. *Texas AG sues Meta for allegedly exploiting users' biometric data*, Axios.com, https://www.axios.com/2022/02/15/texas-facebook-meta-biometric-data?utm_source=chatgpt.com, доступан 29. 7. 2025.

Ethical and Security Aspects of the Use of Papillary Line Imprints as Biometric Identification

Abstract: *Despite the development of technics and technology, the drawing of papillary lines still represents the most widespread method of registration and identification of persons. The uniqueness, universality, immutability and transferability of papillary line prints make them a reliable, scientifically verified biometric characteristic. However, due to the widespread use of fingerprints for verification the question of the security of the use of this biometric feature arises. There are assumptions about possible unauthorized access and use of biometric data, along with all other personal data. With the advancement of technology, especially information and communication technologies and artificial intelligence (AI), our data is everywhere and is potentially accessible to everyone. Every day we leave passwords on various servers, we use our fingerprints to access smartphones and computers, and all this data remains stored in “some part of the Internet”. Therefore, it is legitimate to ask about the security of personal data, yet there is still no precise research on the misuse of biometric data in our country. Biometric systems are susceptible to numerous types of attacks, such as hacking, identity theft, data manipulation, and misuse by authorized persons and government agencies. In addition, ethical dilemmas regarding privacy, voluntariness, and transparency of data processing, storage, and retention remain unresolved.*

Keywords: *ethics, security, police ethics, fingerprints.*

Ненад Н. КОВАЧЕВИЋ¹

Министарство одбране, Секретаријат, Београд, Република Србија

Немања Р. СТЕВАНОВИЋ²

Универзитет „Унион-Никола Тесла”,

Факултет за дипломатију и безбедност, Београд

ДОИ: 10.5937/bezbednost2503163K

УДК: 351.751:347.775(497.11)

004.056.5(497.11)

Прегледни научни рад

Примљен: 23. 9. 2025. године

Датум прихватања: 24. 11. 2025. године

Друштвено-правна ограничења у примени Закона о слободном приступу информацијама од јавног значаја

Апстракт: У савременом свету, где је потреба за транспарентношћу и отвореношћу важна карактеристика функционисања демократских друштва, проблеми одмеравања релеванних интереса давања информација од јавног значаја у односу на заштитну властоделачку информацију представљају изазове који могу да наруше равнотежу између транспарентности и безбедности. Један од главних проблема који се јавља у овом контексту јесте конфликт између потребе за транспарентношћу и грађанским учешћем у безбедности. Грађани имају право да буду информисани о активностима државе, али истовремено постоји неопходност заштите националних интереса. Иако је ова материја у српском законодавству уређена у складу са стандардима најразвијенијих демократија, ипак је показала да се у њиховој примени јављају проблеми. У овом истраживању разматра се решење у складу са којим је уређен слободан приступ информацијама од јавног значаја у контексту заштите властоделачке информације, са фокусом на идентификовање проблема са којима се Министарство

¹ nenad.kovacevic7@yahoo.com, <https://orcid.org/0009-0002-1003-2498>.

² nemanjastevanovic04@gmail.com, <https://orcid.org/0009-0001-1893-603X>.

одбране суочава у пракси. Аутори закључују да професионална и у оквирима дозвољене транспарентности неопходна комуникација са јавношћу, уз паралелно јачање безбедносне културе друштвене заједнице кроз указивање на значај националне безбедности и заштитне вишњих вредности државе, као и новелирање процеса из ове области, представљају основу процеса који за циљ има остваривање ове врсте равнотеже. Јасно остварени модалитети сарадње између војних структура, владе и цивилног друштва омогућавају усклађивање интереса и остварују процес за рационални дијалог свих актера овог процеса, што поред смањења рањивости овог врло важног сектора безбедности, јесте и основа изградње функционалне и јаке демократске система.

Кључне речи: *претежнији интерес, национална безбедност, информације од јавног значаја, заштитна тајности података, људска права и слободе, слободан процес.*

Увод

Иако су стандарди транспарентности по питањима функционисања државе имплементирани у националном законодавству, јавност је заинтересована, али и забринута за оправданост тајности података и њихове потенцијалне злоупотребе. Та заинтересованост се односи, поред оправданости заштите државне тајне (видети: Ковачевић, 2024: 20–21), и на потенцијалну злоупотребу од стране државе, имајући у виду да постоји евидентан број случајева код којих се примењују одредбе Закона о тајности података (Службени гласник Републике Србије, бр. 104/2009), а да се притом не могу довести у везу са националном безбедношћу, већ се везују за комерцијалне активности државе. Транспарентност је, сматра Галнур (Galnoor), један од стандарда савремене демократске државе, али чињеница је да држава и даље „прикрива” најосетљивије податке у великој количини других различитих података (Galnoor, 1977: 66). Из тог разлога Галнур наводи да „остваривање права за учешће у процесу одлучивања о релевантности података представља моћан вид контроле и огледа се у чињеници да је интересовање јавности

за остварење контроле приликом одлучивања о релевантности података претежније у односу на интересовање о начину на који се спроводи тајност података” (Galnoor, 1977: 66–67).

Право на слободан приступ информацијама настало је као резултат развоја савремене правне државе и партиципативне демократије, у којој грађанин постаје „четврта власт” и активни учесник у друштвеним процесима (Миленковић, 2015: 129–130). Како наводе поједини аутори, с аспекта грађанских права и слобода постоји неизоставна потреба да се приликом разматрања тајности врши анализа тајности и у контексту демократских права и слобода грађана (Costas, Grey, 2014: 1423–1447). Сходно томе, имајући у виду значај и комплексност предметне материје, уочава се да прописи који регулишу слободан приступ информацијама морају бити јасни и предвиђати изузетке за информације које би могле угрозити националну безбедност, а који у том делу могу одступити од прокламованих права и слобода. Стога су одговорност и прецизност у доношењу таквих закона кључни за одржавање равнотеже (Безбрадица, Марковић, 2022: 175). С друге стране, у покушају проналаска равнотеже између неопходности одржавања одређених података тајним и интереса јавности, појављују се и легитимни разлози који оправдавају примену тајности података. Најбројнији међу тим разлозима јесу они који се односе на заштиту националне безбедности, што је истовремено у супротности са интересима грађана по питању достигнутих права и слобода у савременој демократској држави, на основу којих јавност има право да зна како држава руководи, превасходно, одбраном и спољним пословима (Carter, Franklin, 1991: 319).

Предметна област у националном законодавству регулисана је сходно међународним стандардима који се односе на владавину права и поштовање људских права, по узору на најразвијеније западне демократије. Прописи, најзначајнији за ово истраживање, којима је уређена област слободног приступа информацијама од јавног значаја јесу: Закон о слободном приступу информацијама од јавног значаја (Службени гласник Републике Србије, бр. 120/2004, 54/2007, 104/2009, 36/2010 и 105/2021) (ЗОСПИОЈЗ) и За-

кон о тајности података. Такође, важно је напоменути да је у складу са Уставом Републике Србије из 2006. године, право на приступ информацијама постало и уставом гарантовано право грађана. На основу ЗОСПИОЈЗ, претпоставља се да је интерес јавности да буде у току са информацијама ове врсте оправдан, односно да претеже у односу на супротстављене интересе. Притом, овим законом су регулисана и одређена ограничења. Једно од тих ограничења односи се на заштиту националне безбедности и, без обзира на степен демократске развијености неког друштва, није могуће градити другачији приступ од онога који је у домаћем законодавству присутан у погледу транспарентности и одређивања категорија оних који могу остварити увид у документа у поседу органа јавне власти. Врло је тешко и замислити могућност успостављања другачијег нормативног оквира, јер овако како је постављен, национални законски оквир има за циљ да обезбеди легитиман интерес целокупног друштва. Иако су појмови јавног интереса и тајности врло често у супротности, код заштите тајних података постоји евидентан јавни интерес да они задрже одређени степен тајности. Јер, као што је до сада већ наведено, заштита националних интереса подразумева заштиту виталних вредности и државе и друштва. Отуда, стављањем ознаке одређеног степена тајности на поједине податке држава не штити само своје интересе и своје вредности, већ и интересе и виталне вредности друштва, што је у складу са схватањем концепта националне безбедности у ширем смислу (Мијалковић, 2009: 55). Да је задатак одговорног руководства да формира јавно мњење и да не попусти пред његовим притисцима, потврђује и став који доминира класичним реалистичким теоријама, а који заступа његов главни представник – Ханс Моргентхау (*Hans Morgenthau*). Према његовом мишљењу, државно руководство се приликом доношења одлука у вези са вођењем ефикасне спољне и безбедносне политике мора руководити искључиво заштитом националних интереса (Morgenthau, 1967: 142). Како је национални интерес неодвојиво језгро националне безбедности, посматрајући ограничење приступа подацима са тог аспекта, постоје мишљења у стручној литератури по којима се тајне доводе у директну везу са корупцијом, лошим управљањем и неефикасношћу (Meijer, Hart, Worthy, 2018), што је још један од дод-

атних мотива да се ова област адекватно уреди и да се успоставе функционални механизми за праксу.

Имајући у виду да је национално законодавство у делу који се односи на предметну област усаглашено са законодавствима других савремених држава, долази се до основног питања које ће бити предмет истраживања у овом раду: да ли је постигнута равнотежа између слободног приступа информацијама од јавног значаја и заштите националних интереса, с аспекта заштите државне тајне? Циљ рада је да се идентификују проблеми уочени у досадашњој пракси у примени прописа којима је уређен слободан приступ информацијама од јавног значаја, са посебним освртом на начин на који је ова област регулисана у систему одбране Републике Србије. Сходно истраживањима, у овом раду разматрају се и могућа решења која би олакшала рад органа јавне власти, не угрожавајући притом право на слободан приступ информацијама од јавног значаја. У складу са очекиваним исходима у погледу анализе, издваја се као констатација и потреба за изменом постојећих законских одредби у циљу превазилажења уочених недостатака. Имајући у виду да се ток имплементације може оцењивати искључиво квалитативним методама, реализован је интервју са експертима, који су учествовали у изради правних прописа из области заштите тајних података и њиховог усклађивања са људским правима и слободама, а који су истовремено и ангажовани на пословима у вези са слободним приступом информацијама од јавног значаја (овлашћено лице). Обављена су три експертска интервјуа: два интервјуа са особама које су активно укључене у процес развоја области слободног приступа информацијама од јавног значаја – академским професором³ и овлашћеним лицем Министарства одбране за слободан приступ информацијама од јавног значаја⁴ – и један експертски интервју са представником радне групе која је учествовала у изради Нацрта закона о изменама и допунама За-

³ Унутар транскрипта интервјуа означен као ЕИ1 (експертни интервју 1).

⁴ Унутар транскрипта интервјуа означен као ЕИ2 (експертни интервју 2).

кона о слободном приступу информацијама од јавног значаја⁵. Експертски интервју као метод прикупљања вербалних података употребљен је са намером добијања на други начин недоступних података, при чему истраживачима експерти не представљају „објекат” истраживања, већ сведоке релевантних процеса које настоје да прикажу. Истраживање је реализовано применом полустандардизованог интервјуа, који представља тип научног разговора којим се, на најефикаснији начин, могу остварити отвореност и флексибилност као кључне карактеристике квалитативног истраживачког приступа. Интервју је формално и садржајно разрађен, тако да је говор испитаника вођен унапред припремљеним питањима (Ђурић, 2016). Примарни истраживачки циљ интервјуа било је прикупљање података који нису у довољној мери доступни широј јавности, а значајно доприносе разумевању предмета истраживања. Приликом израде рада коришћене су и друге методе попут анализе садржаја, дескрипције и синтезе. Основни проблем представљао је сужен избор одговарајуће литературе. Значај и допринос рада огледа се у обједињавању и систематизацији теоријских и искуствених сазнања из ове области, могућности лакшег и потпунијег разумевања значаја функције овлашћеног лица, њиховог места и улоге у систему одбране, као и проблема са којима се сусрећу у поступању у различитим ситуацијама.

Национални правни оквир и пракса ЕУ у примени прописа за слободан приступ информацијама од јавног значаја

У периоду од 2004. до 2010. године правни оквир којим је уређивана тајност података у Републици Србији претрпео је одређене реформе, сходно актуелним стандардима међународног права који се превасходно односе на основне принципе савременог демократског друштва (Ковачевић, 2024: 27). Народна скупштина Републике Србије донела је крајем новембра 2004. године Закон о слободном приступу информацијама од јавног значаја, који је до

⁵ Унутар транскрипта интервјуа означен као ЕИЗ (експертни интервју 3).

данас четири пута мењан, изменама и допунама које су уследиле 2007, 2009, 2010. и 2021. године (Миленковић, 2010: 14). На тај начин Република Србија је добила закон који је у значајној мери био усклађен са међународним стандардима у овој области, што потврђује и Глобални рејтинг права на информације (енг. *Global Right to Information Rating Map*) према којем је Република Србија тренутно позиционирана на трећем месту од укупно 140 земаља (*Global Right to Information Rating*, 2025).⁶ Усвајање датог Закона, поред детаљног регулисања ове области, допринело је и трансформацији до тада свеprisутног наратива да је тајност неизбежно начело рада органа јавне власти, што је уједно била и главна карактеристика ове области до почетка XXI века. Примена овог закона трансформисала је такав наратив у оно што данас познајемо као начело транспарентности рада, које је у великој мери присутно чак и у систему какав је онај војног карактера. С друге стране, разматрањем праксе уочавају се одређени проблеми у примени тог закона – и од стране његових адресата (органи јавне власти) и од стране бенефицијара који би требало да дођу до информација. Законом је, ради остваривања овог права, основан и Повереник за информације од јавног значаја и заштиту података о личности, као самостални државни орган који је независан у вршењу своје надлежности. Уставом Републике Србије из 2006. године, право на приступ информацијама постало је и уставом гарантовано право грађана.

У одређеним органима јавне власти руководиоци су искористили могућност одређивања овлашћених лица за поступање по захтевима за слободан приступ информацијама од јавног значаја. Примера ради, у министарству надлежном за послове одбране министар је донео Одлуку о одређивању овлашћених лица за поступање по захтевима за слободан приступ информацијама од јавног значаја у Министарству одбране и Војсци Србије (акт Правне управе Секретаријата министарства број 272-3/24 од 12. јуна 2024. и број 272-23/24 од дана 15. октобра 2024).

⁶ У вези са наведеним, од 2011. године Глобални рејтинг права на информације рангира квалитет законских одредаби у овој области на основу њиховог мерења према 61. критеријуму.

Закон о тајности података на снази је од 2010. године и њиме је уређена јединствена заштита тајности података у органима јавне власти. Према једном од саговорника у оквиру спроведеног експертског интервјуа, предност српског Закона о тајности података у односу на слична решења у другим земљама јесте то што представља део нормативног троугла. Наиме, овај закон се врло експлицитно везује и за Закон о слободном приступу информацијама од јавног значаја и за Закон о заштити података о личности, јер он по свом садржају мора имати везе са та два закона и та веза је у њему експлицирана. Да је правни оквир који уређује заштиту тајности података усаглашен са прописима других међународних субјеката потврђује и више склопљених споразума из области размене и заштите тајности података – два мултилатерална и 14 билатералних споразума (подаци које је за потребе овог истраживања доставила Канцеларија Савета за националну безбедност и заштиту тајних података).

Усклађивање Републике Србије са Европском унијом (ЕУ) дуготрајан је и свеобухватан процес који обухвата политичке, правне, економске и институционалне реформе ради прилагођавања стандардима и правним тековинама ове организације. Додатно, унапређење националне безбедности и одбране кроз процес европских интеграција, уз поштовање специфичности Републике Србије, јесте њен примарни одбрамбени интерес (Стратегија одбране РС, 2019). Пратећи дефинисани национални интерес Републике Србије у погледу стратешког опредељења за пуноправно чланство у ЕУ и њену обавезу да на путу европских интеграција свој национални правни оквир усклади са правним стандардима ове организације, ЕУ издвајамо као референтан пример праксе у примени прописа за слободан приступ информацијама од јавног значаја. У примени и тумачењу ових прописа, ЕУ се такође суочава са одређеним изазовима који се, према истраживању Центра за медијски плурализам и медијску слободу⁷ (енг. *The Centre for Media*

⁷ Спроводи напредна истраживања и праћење медијског плурализма широм Европе са циљем пружања подршке у домену демократије, одговорности и основних права.

Pluralism and Media Freedom – CMPF), спроведеном 2022. године, своде на неколико кључних проблема (CMPF, 2023). Прво, одређе-ни прописи који уређују приступ информацијама често имају ог-раничену примену, јер су усмерени искључиво на поједине гране власти. Уз то, процедуре за захтевање и добијање информација не-ретко су нејасне и лоше дефинисане, што ствара правну несигур-ност и отежава грађанима и новинарима остваривање овог права. Последица тога је неједнака примена закона и постојање админис-тративних баријера у пракси. Затим, многобројна јавна тела не ус-певају да успоставе и одржавају уредне и систематизоване евиден-ције, што отежава приступ релевантним документима. Лоше вође-ње докумената не само да нарушава ефикасност институција већ и подрива поверење јавности у институционалну транспарентност и доступност података. Даље, органи јавне власти често се ослањају на изузетке од обавезе објављивања информација, нарочито оних који се односе на заштиту приватности. Иако је заштита личних података важна, у пракси се ови изузеци неретко злоупотребљавају како би се прикриле информације о деловању јавних службеника, чак и у случајевима када су ти службеници ангажовани у вршењу јавних функција. Оваква пракса значајно умањује јавну контролу над институцијама. Главни проблем јесте у томе што, и на националном нивоу и унутар институција ЕУ, процеси доношења одлука често нису довољно транспарентни. То ствара утисак затворености власти и умањује могућност јавности да правовремено утиче на креирање политика, што је супротно принципима демократског управљања. Иако закони о приступу информацијама имају за циљ да омогуће надзор и повећају одговорност институција, неки појединци и организације их понекад користе у сврху финансијске добити или намерне опструкције рада јавних органа. Такве злоупотребе могу довести до преоптерећења система, што онемогућава благовремено поступање по захтевима легитимних тражилаца информација и нарушава интегритет система транспарентности. Поред наведеног, законодавства држава чланица ЕУ нису усклађена са законодавством ЕУ у делу који се односи на предметну област, што отвара могућност за настанак недоследности и потешкоћа у обезбеђивању једнаког приступа за све грађане (Marti, Kraetzig, 2024). Наведени изазови са

којима се суочавају и државе чланице ЕУ указују да су за унапређење права на приступ информацијама, осим усавршавања законодавног оквира, неопходни и његова доследна примена, ефикасна евиденција, спречавање злоупотреба и подизање свести о важности транспарентности као темеља демократског друштва.

На основу података из поменутог извештаја Центра за медијски плурализам и медијску слободу закључује се да многе европске владе, упркос користима које добра имплементација и примена закона о приступу информацијама могу донети, доживљавају сопствене политике приступа информацијама као претњу и проналазе изговоре да ограниче права подносилаца захтева (Bleyer-Simon et al., 2023: 32). У том контексту, као карактеристични проблеми у примени овог прописа наведени су „ћутање администрације” (Билић, Валечић, 2023), одбијање захтева за слободан приступ информацијама од јавног значаја и злоупотреба примене изузетака регулисаних у другим законима (Milosavljevic, Biljak-Geijević, 2023), прекорачење рокова за одговор на захтеве за информације, као и дуготрајни и неефикасни механизми у поступцима жалби (Spasov et al., 2023).

Да разлике у погледу робусности правне заштите права на приступ информацијама постоје, потврђује и „Аксес инфо Европа” (*Access Info Europe*⁸). У вези са наведеним, Центар за медијски плурализам објашњава да добра оцена закона није гарант да ће он бити адекватно имплементиран и примењиван, што се може видети из примера појединих држава попут Албаније, Хрватске, Србије и Словеније. У том контексту могу се навести примери држава којима право на слободан приступ није уставом дефинисано право, и држава које имају слабије оцењене законе, попут Француске, Данске и Луксембурга, а обезбедиле су ефикасан приступ информацијама (CMPF, 2023).

Изузеци од закона су карактеристика свих законодавстава, која обично захтевају посебне разлоге за неоткривање (Hilebrandt,

⁸ Невладина организација за људска права посвећена промоцији и заштити права на приступ информацијама у ЕУ.

2017). Често постоје велика изузећа за сва обавештајна и безбедносна питања, приватност, делове процеса креирања политика и комерцијално осетљиве области. У даљем тексту анализираће се недостаци који се односе на примену законских одредби о слободном приступу информацијама од јавног значаја са посебним освртом на податке који су означени одређеним степеном тајности у систему одбране Републике Србије.

Проблеми у примени ЗОСПИОЈЗ

Постављање одређених ограничења у погледу приступа подацима различитог карактера углавном је довољно да изазове пажњу јавности и створи негативан наратив и према субјектима који такве информације поседују и према самим подацима који се на овај начин штите. Међу теоретичарима ове области постоји сагласност о томе да свака активност у погледу ограничавања приступа подацима резултира и различитим негативним последицама. О томе говори и Доналд Роват (*Donald Rowat*), који заузима став да сваки вид ограничавања приступа подацима има потенцијал да проузрокује нежељене појаве попут збуњености и несигурности саме државне управе, отежавања рада одређених професија и слично (Rowat, 1979: 23). Слободан приступ информацијама од јавног значаја, као што смо већ објаснили, представља једно од кључних права у демократском друштву, које грађанима и организацијама цивилног сектора омогућава да увидом у рад јавних институција контролишу трошење јавних средстава и врше притисак за одговорно и транспарентно управљање. Ипак, у пракси, остваривање овог права наилази на бројне изазове и препреке. Поједине институције злоупотребљавају одредбе о заштити података, проглашавајући информације „службеном тајном”, „пословном тајном” или „податком о личности” – чак и када то објективно није случај. Службеници који обрађују захтеве често нису адекватно обучени, па или не знају како да поступе, или се руководе политичким притисцима и интересима надређених. Иако Повереник за информације од јавног значаја и заштиту података о личности има овлаш-

ћења да доноси обавезујуће одлуке, многа тела их не извршавају, а санкције су ретке и благе. У складу са статистичким подацима наведеним у Извештају о раду Повереника, у 2024. години је изјављено 20.012 жалби Поверенику због повреде права на приступ информацијама од јавног значаја (Извештај, 2025: 83). У истом Извештају се констатује и да је проценат позивања на тајност података у значајном расту, као и да се веома често дешава да изостане адекватно образложење органа јавне власти о разлозима због којих сматра да је у неком конкретном случају заштита тајног података претежнији интерес у односу на интерес права јавности да зна (Извештај, 2025: 23). Према поменутом извештају, у 2024. години од укупно 1.072 предмета у којима су решењем одбијали захтеве тражилаца информација као неосноване, органи јавне власти су се у 206 предмета (19,2%, што је дупло више у односу на 2023. годину) позвали на тајност информација или докумената. У 146 предмета или у 13,6% органи јавне власти су се позвали на члан 2 ЗОСПИОЈЗ – „да ли је информација од јавног значаја?”; у шест предмета или у 0,6% позвали су се на члан 10 ЗОСПИОЈЗ – да је информација већ доступна јавности (Извештај, 2025: 90). „Одредбама актуелних националних прописа којима је уређена заштита тајности података делимично је омогућено остваривање контроле јавности над евентуалном злоупотребом тајности података, у смислу указивања и предузимања неких мера којима би се то спречило. У складу са Законом о тајности података, када се ради о онима који нису кључни адресати закона – органи јавне власти изван система националне безбедности, постоји механизам контроле који би могао да оправда очекивања. С друге стране, унутрашња контрола или контрола унутар система националне безбедности, посебно у делу који се односи на приступ тајним подацима, остварује се делимично од стране посланика Народне скупштине.” (ЕИЗ)

„Примена одредби ЗОСПИОЈЗ у вези је и са политичким ривалитетом и односом неповерења између Повереника и органа јавне власти, што је неоправдано. Такав приступ врло често има за последицу отежавање рада органа власти јер толико тога је било на терету ових органа да су многи органи јавне власти практично

били блокирани у свом раду. У прилог наведеном подсећам на злоупотребе од стране адвоката који су у једном тренутку схватили да могу да зараде новац на основу ЗОСПИОЈЗ.” (ЕИ1) „Наиме, изменама ЗОСПИОЈЗ из 2021. године и пресудом Управног суда 2022. године омогућено је да тражилац информације ангажује адвоката који покреће жалбени поступак пред Повереником. Адвокатска такса за ову услугу износи 49.500 динара.” (ЕИ2)

Наведени пример злоупотребе ЗОСПИОЈЗ од стране тражиоца карактеристичан је због тога што се у периоду од 2022. до 2024. године у органима јавне власти број захтева увећао за око 100%. У прилог наведеном иду и статистички подаци садржани у Годишњем извештају Повереника за 2024. годину, као и подаци других органа јавне власти. „Примера ради у систему одбране током 2021. године било је око 150 предмета, док је у периоду од 2022. до 2024. године, било преко 300 предмета.” (ЕИ2)

Носиоци извршне власти често не обезбеђују институционалну подршку за спровођење ЗОСПИОЈЗ. Политичка воља за транспарентност је селективна и често симболична. Нека министарства, јавна предузећа и локалне власти систематски одбијају да поступају по решењима. Повереник нема извршна овлашћења и не може принудно спровести своје одлуке. „Повереник никада није поступао у складу са Законом када се ради о одлучивању о жалби органа јавне власти и никада није одмеравао супротстављене интересе онако како му Закон налаже. Овај независни орган, између осталог, направио је и водич у коме се дефинише како би Повереник требало да одмерава сукобљене интересе, што је за предметно истраживање интерес тајности рада. С једне стране је интерес јавности да зна, а с друге је оправдани интерес органа јавне власти да не дозволе увид јавности у одређени документ. Када дође до жалбе, односно када дође до тога да је орган јавне власти ускратио тражиоцу информацију, тражилац се жали поверенику који у свом раду никада није одмеравао интересе већ је произвољно, арбитрарно одлучивао.” (ЕИ1)

Када је у питању систем одбране, одређени број захтева за приступ информацијама од јавног значаја односи се на податке који су означени одређеним степеном тајности. „У поступању Пове-

реника по жалбама на основу самог ЗОСПИОЈЗ и на основу Закона о општем управном поступку (Службени гласник Републике Србије, бр. 18/2016, 95/2018 – аутентично тумачење и 2/2023 – одлука УС) било је ситуација да се од стране Повереника добије конкретан налог, односно решење којим се жалба тражиоцу уважава и налаже Министарству одбране да се доставе подаци који су у највећем броју случаја означени степеном тајности ‘ПОВЕРЉИВО’, а у појединим случајевима чак и ‘СТРОГО ПОВЕРЉИВО.’” (ЕИ2)

„Органи власти у највећем броју случајева бирају пре да плате прекршајну казну због тога што нису обезбедили приступ информацијама од јавног значаја него што ће компромитовати истрагу или одати неку тајну за коју знају да ће направити велику штету.” (ЕИ1)

У министарству надлежном за послове одбране, руководилац органа је одредио овлашћена лица за поступање по захтевима за слободан приступ информацијама од јавног значаја у Министарству одбране и Војсци Србије. Наведена лица, поред послова из прописаног делокруга, поступају и по захтевима за слободан приступ информацијама од јавног значаја, а да за те послове не примењу посебну надокнаду. Значај и одговорност овлашћених лица произлази из чињенице да она поступају по значајном броју захтева за приступ информацијама од јавног значаја у релативно кратким роковима. На питање у вези са применљивошћу дефинисаног начина одмеравања претежних интереса („троделни тест”) један од експерата сматра да је тест примењив, али не у потпуности. „Делови троделног теста су: препознавање интереса који се сукобљавају – примера ради интерес који се везује за тајност података и с друге стране интерес јавности да дође до тог податка; утврђивање потенцијалне штете уколико би дошло до повреде једног од тих интереса; неопходност приступа информацијама, односно ограничење. У том смислу треба размишљати не само у правцу да ли су ти интереси супротни један другом или да ли постоји опасност од настанка штете него да ли је и неопходно ићи у ограничење или по Закону о тајности података или по ЗОСПИОЈЗ. Потом, ако се, рецимо, ради о томе да је потребно једну информацију

заштити као тајну или је потребно да дође до предаје те информације јавности, односно омогућавање јавности да се упозна са документом, онда се оправдано размишља да ли је то средство које се жели користити подобно средство да заштити одређени интерес. Примера ради, ако је тај документ већ отишао у јавност онда нема никаквог смисла штитити га као тајни податак зато што је доступан свима. Затим, да ли је механизам који се користи, било да се везује за Закон о тајности података или за ЗОСПИОЈЗ, подобан („тест подобности“) да оствари циљ који се жели остварити, а увек се обрадом података остварује неки циљ. Сходно наведеном може се поставити питање да ли се исти циљ може остварити означавањем податка нижим степеном тајности. Додатно, тест који се састоји из теста потребности, подобности и неопходности у ужем смислу, потребно је унети у ЗОСПИОЈЗ, да би органи имали упутство како ефикасније приступати ограничењу слободног приступа.” (ЕИ1)

Приступ информацијама од јавног значаја у систему одбране, с друге стране, представља посебно осетљиво и комплексно питање јер постоји неопходност да се успостави равнотежа између два темељна интереса: транспарентности и права јавности да зна, као основа демократије и владавине права и заштите националне безбедности, и заштите података који би могли угрозити безбедност државе и њених грађана ако се открију. „Један од најзаступљенијих проблема када је у питању систем одбране јесте учестала појава да се кроз захтев за слободан приступ траже неки лични подаци (нпр. решења о превозу, решења о плати, о неким накнадама) што не представља информације од јавног значаја, из разлога што уколико се такво решење једном учини доступним јавности то решење онда исто мора касније да буде учињено доступним сваком другом тражиоцу. Даље, прописане рокове видим као још један од проблема са којима се пракса рада Министарства одбране суочава. Ови рокови су релативно кратки, посебно у већим органима јавне власти као што је Министарство одбране, где овлашћено лице мора да се обрати одређеној јединици, команди или установи Војске Србије или организационој целини Министарства одбране и да затражи

податке, што углавном изискује више времена од прописаног рока од 15 дана.” (ЕИ2)

И одговорност овлашћеног лица Министарства одбране за приступ информацијама од јавног значаја у Србији, као и у другим државним органима, дефинисана је у ЗОСПИОЈЗ. Иако је законски оквир јасан, у пракси постоје бројни проблеми и изазови у раду овлашћених лица, нарочито у осетљивим секторима као што је одбрана. Овлашћена лица у Министарству одбране и Војсци Србије јесу војна лица, цивилна лица, и државни службеници (Жнидаршич, Милисављевић, 2024: 120), и у свом раду се суочавају са: сложеном интерном процедуром, потребом за вишеструким одобрењима од надређених структура, недостатком дигитализације и евиденције о траженим информацијама. У складу са датим проблемима, значајно се успорава процес одговора на захтеве и губи се поверење јавности у институције. „Изменама Закона из 2021. године проширена је одговорност, у смислу да није одговорно само овлашћено лице за непоступање по тим захтевима него и сваки други запослени у том органу јавне власти. Када је у питању систем одбране, то би конкретно било и неко друго лице које је запослено у некој другој целини или евентуално руководилац који не дозвољава да се одређени подаци доставе овлашћеном лицу. Али ни са овом изменом одредби закона није у потпуности регулисала одговорност искључиво лица одговорних за не поступање по захтеву.” (ЕИ2)

Критеријуми за одређивање тајности података кључни су за заштиту информација које могу утицати на националну безбедност, економију, приватност грађана или пословне интересе. Ипак, у пракси се јављају бројни проблеми у вези с дефинисањем, применом и поштовањем тих критеријума. Критеријуми су често формулисани на апстрактан начин („угрожавање националне безбедности”, „економски интереси државе”), што омогућава субјективно тумачење. То може довести до прекомерне класификације података или злоупотребе тајности ради скривања информација од јавности. „Критеријуми за ближе одређивање тајних података релативно су уопштени, што омогућује флексибилност запослених у раду са великим бројем тајних података у оружаним снага-

ма, али истовремено отвара могућност за већу злоупотребу. С аспекта ЗОСПИОЈЗ, непостојање прецизнијих критеријума отежава рад и поступање овлашћеног лица по захтеву, нарочито у поступку који следи по жалби на решење. Такође, ни сам култура схватања важности ЗОСПИОЈЗ и Закона и тајности података није развијена на високом нивоу, посебно у делу који се односи на заштиту тајности података, односно националних интереса, са тежиштем на примени одредби прописа приликом одређивања тајних података.” (ЕИЗ)

Принцип правне сигурности један је од темељних принципа правне државе и још један од недостатака у примени ЗОСПИОЈЗ. Он значи да су правни прописи јасни, предвидиви и да се не мењају често или ретроактивно на начин који би угрозио права грађана. „Устаљена пракса поступања, пре свега судова, могла би да се посматра као део корпуса људских права. Човек има оправдано очекивање да зна да може да предвиди какав ће исход поступка бити. У развијеним демократијама, и то је оно што врло често истичем, та предвидљивост исхода поступка иде до нивоа од 95%. Уколико поставимо питање било ком адвокату у Републици Србији, он ће нам рећи да не може да предвиди исход ниједног поступка и то је оно што забрињава због тога што урушава принцип правне сигурности.” (ЕИЗ)

Универзални проблем односи се и на технолошки развој и могућности јавности да лако приступи информацијама. Савремено друштво генерално зависи од друштвених мрежа и савремених информационих технологија које омогућавају брзо дељење информација. Такве околности захтевају да систем одбране једне државе брзо и адекватно реагује, постављајући изазов контроле информација.

Предлози

У складу са резултатима истраживања закључује се да је пракса указала на одређене недостатке законодавства којим је регулисан слободан приступ информацијама од јавног значаја. С тим у вези, било би целисходно новелирати одређене прописе, попут

ЗОСПИОЈЗ и Закона о тајности података. Имајући у виду осетљивост области за коју јавност исказује све веће интересовање и проблеме приступа информацијама од јавног значаја у односу на националну безбедност, као адекватно решење намеће се то да оружане снаге и други органи сектора безбедности буду изузети од примене Закона, по узору на неке друге државе у региону. Будући да то на нивоу националног законодавства није могуће, јер је Уставом Републике Србије прописано да се „достигнути ниво људских и мањинских права не може (се) смањивати” (члан 20), изменом појединих одредби олакшао би се посао, пре свега овлашћеним лицима. Један од предлога на основу ког би се олакшао рад овлашћених лица односи се на продужетак рокова по узору на Закон о општем управном поступку, где је рок за поступање у првом степену тридесет дана. Наравно, овај предлог се не би односио на изузетке у случајевима кад су угрожени живот, заштита животне средине и др., где су рокови краћи од петнаест дана.

Додатно, неки од предлога за измене Закона односио би се на одвајање захтева за слободан приступ информацијама од захтева за добијање неких података или уверења и обавештења о управном поступку, што и јесте суштина, по узору на црногорско и хрватско решење.

Следећи предлог за измене ЗОСПИОЈЗ био би да се у тај закон инкорпорира тест који се односи на одмеравање интереса, као и да се у складу са новим одредбама предузму активности ради ефикаснијег рада запослених и дизања свести о значају слободног приступа информацијама од јавног значаја. Приликом измена наведеног Закона било би значајно редефинисати и прекршајне одредбе, односно механизме заштите, јер су они сада уређени на неприципијелан начин и омогућавају органима власти да изаберу плаћање казне уместо омогућавања јавности да приступи информацијама, чак и у оним случајевима када то није оправдано.

Поред измена ЗОСПИОЈЗ, било би целисходно изменити и Закон о тајности података, имајући у виду да је пракса указала на потребу да се тај закон осавремени, да се употпуни, као и да се обезбеде нека прецизнија или делотворнија решења. Нека од поме-

нутих решења односила би се на надзор над поступањем над Законом о тајности података. Наиме, актуелно решење надзора не даје очекиване резултате и самим тим би можда требало размишљати о децентрализованом систему надзора, у смислу да се надлежност за надзор пренесе на органе јавне власти који имају капацитет за спровођење инспекцијског надзора, попут оних у систему одбране.

Такође, имајући у виду да су посебни критеријуми за ближе одређивање тајних података прилично уопштени, што олакшава корисницима рад у поступцима одређивања тајних података, требало би размислити о прецизирању критеријума, пре свега ради смањивања могућности злоупотребе овог закона, као и олакшавања рада овлашћених лица у поступању по жалбама.

Имајући у виду да је чланом 39 ЗОСПИОЈЗ регулисана обавеза објављивања информатора, очекивано је да би израда што потпунијег информатора, у смислу да се у њему што детаљније одговори на питања и да се он редовно ажурира, утицала на смањење броја захтева за слободан приступ, а самим тим и на растерећење овлашћених лица.

Поред наведеног, као мера за превазилажење уочених проблема неизоставно је предузимати активности на ефикаснијој интеракцији са јавношћу и подизању свести о значају заштите националних интереса.

Закључак

На основу спроведеног истраживања може се закључити да је актуелним законодавством успостављена равнотежа између основних људских права и слобода и националне безбедности у Републици Србији, због тога што је и у члану 1 Устава РС регулисано да је Република Србија заснована на идеји људских права. Према идеалистичком схватању, национална безбедност и људска права не би требало да буду у сукобу, иако је у пракси то много другачије. Ради постизања адекватне равнотеже између заштите националне безбедности, људских права и слобода и интереса јавно-

сти, у демократским друштвима се тежи: балансу између заштите грађана и очувања слобода, транспарентности у раду институција сектора безбедности, демократској контроли и правним средствима заштите права.

Иако је националним законодавством предметна материја уређена у складу са стандардима које делимо са најразвијенијим демократијама, уочени су одређени проблеми који настају у имплементацији тих закона. Овлашћено лице за поступање по захтеву за слободан приступ информацијама од јавног значаја у органима власти има изузетно важну функцију за систем, нарочито у систему одбране. С обзиром да је у овом систему већина података насталих у раду или у вези са радом означена одређеним степеном тајности, то у поступку по захтеву за овлашћено лице представља смерницу за могућа ограничења у погледу давања приступа. Међутим, законска регулатива указује да то није довољно да би се ограничио приступ информацијама. Овлашћено лице је у обавези да цени претежнији интерес, односно да врши процену да ли би омогућавањем приступа информацијама од јавног значаја настала „озбиљна штета”. При том, приликом одмеравања претежнијег интереса, има обавезу да води рачуна о уставом загарантованом праву јавности да зна, односно да буде обавештена. Управо због тога је функција овлашћеног лица у систему одбране колико важна, толико и неопходна. Приликом поступања по захтеву за слободан приступ информацијама од јавног значаја, овлашћено лице је у обавези да сачува сваки податак чијим би омогућавањем приступа могао да угрози живот, здравље, сигурност или које друго важно добро неког лица, као и податак који би могао да угрози одбрану земље, националну или јавну безбедност и међународне односе. Ради заштите оваквих вредности, а узимајући у обзир да се, с разлогом, већина података у систему одбране означава одређеним степеном тајности, овлашћено лице се налази у позицији континуираног одмеравања претежнијег интереса, као и спречавања настајања сваког вида „озбиљне штете”, водећи се пре свега циљем заштите националне безбедности кроз очување оперативне способности одбрамбеног система.

У складу са резултатима спроведеног истраживања може се закључити да је национални правни систем на прагу савремених решења и усклађивања са међународним стандардима које прописује међународно право, а који су у примерима добре праксе показали могућност да се на тој основи изграде ефикасни механизми деловања. Низ институционалних, законодавних, техничких и друштвених мера које је даље неопходно предузети, на за сада добро постављеној основи за даљи развој модела решавања изазова слободном приступу информацијама од јавног значаја, посебно у односу на националну безбедност, може резултирати изградњом система у којем би информације ове врсте заиста и представљале јавно добро, које је адекватно успостављеним системом заштите виталних вредности државе и друштва ослобођено могућности угрожавања услед спровођења интереса јавности.

Литература

1. Безбрадица, А., Марковић, В. (2022). Тест(ови) балансирања и ограничење права на приступ информацијама од јавног значаја у српском праву. У: *Заштити људских права и слобода у светлу међународних и националних стандарда*. Правни факултет Универзитета у Приштини са привременим седиштем у Косовској Митровици, Косовска Митровица, стр. 173–200.
2. Bilic, P., Valecic, M. (2023). *Monitoring media pluralism in the digital era: application of the Media Pluralism Monitor in the European Union, Albania, Montenegro, the Republic of North Macedonia, Serbia and Turkey in the year 2022. Country report: Croatia*. Florence, Italy.
3. Bleyer-Simon, K., Brogi, E., Carlini, R., Da Costa Leite Borges, D., Nenadic, I., Palmer, M., ... Žuffova, M. (2023). *Monitoring media pluralism in the digital era: Application of the media pluralism monitor in the European Union, Albania, Montenegro, the Republic of North Macedonia, Serbia and Turkey in the year 2022*. European University Institute.
4. Carter, T., Franklin, M. (1991). *The First Amendment and the Fourth Estate*. New York: The Foundation Press.

5. Centre for Media Pluralism and Media Freedom (2023). *Decision-Making Transparency in Europe identified as top priority on International Right to Know Day*. <https://www.access-info.org/2017-09-29/decision-making-transparency-in-europe-identified-as-top-priority-on-international-right-to-know-day/>, доступан 20. 5. 2025.
6. Costas, J., Grey, C. (2014). Bringing secrecy into the open: Towards a theorization of the social processes of organizational secrecy. *Organization Studies*, 35(10): 1423–1447.
7. Galnoor, I. (1977). *The Information Marketplace. Government Secrecy in Democracies*. New York: Harper & Row.
8. Ђурић С. (2016). Интервјуисање експерата: специфичности и принципи примене. *Годишњак Факултета безбедности*, 2016(1): 11–28.
9. Hillebrandt, M. Z. (2017). *Living transparency: The development of access to documents in the Council of the EU and its democratic implications*. Amsterdam Center for European Law and Governance.
10. Ковачевић, Н. (2024). Државна тајна – еволуција правног уређења заштите тајности по-датака. *Војно дело*, 76(4): 19–34.
11. Marti, N. V., Kraetzig, V. (2024). Why Europe Needs a Harmonised Access to Information Act. *Verfassungsblog: On Matters Constitutional*.
12. Meijer, A., 't Hart, P., Worthy, B. (2018). Assessing government transparency: An interpretive framework. *Administration & Society*, 50(4): 501–526.
13. Мијалковић, С. (2009). Национална безбедност – од вестфалског концепта до постхладноратовског. *Војно дело*, 61(2): 55–73.
14. Миленковић, Д. (2010). Приручник за примену Закона о слободном приступу информацијама од јавног значаја, <https://www.poverenik.rs/images/stories/dokumentacija-nova/vodic/prirucnikzaprimenuzakonacir.pdf>, доступан 4. 4. 2025.
15. Миленковић, Д. (2015). Управно процесна и други слични облици заштите права на приступ информацијама у компаративном праву. *Страни правни живот*, 59(3): 116–129.
16. Milosavljevic, M., Biljak-Gerjevic, R. (2023). *Monitoring media pluralism in the digital era: application of the Media Pluralism Monitor*

- in the European Union, Albania, Montenegro, the Republic of North Macedonia, Serbia and Turkey in the year 2022. Country report: Slovenia.* Florence, Italy.
17. Morgenthau, H. J. (1967). *Politics among Nations: The Struggle for Power and Peace* (4th ed.). New York: Knopf.
 18. Rowat, D. (1979). *Administrative Secrecy in Developed Countries.* New York: Columbia University Press.
 19. Spassov, O., Ognyanova, N., Daskalova, N. (2023). *Monitoring media pluralism in the digital era: application of the Media Pluralism Monitor in the European Union, Albania, Montenegro, the Republic of North Macedonia, Serbia and Turkey in the year 2022. Country report: Bulgaria.* Florence, Italy.
 20. Жнидаршич, В. Милисављевић, С. (2024) Анализа особина субјектата кривичних дела против Војске Србије одређених кривичним закоником. *Crimen*, 15(1): 106-121
doi: 10.5937/цримен24011023.

Правни прописи

1. Global Right to Information Rating. (2025). Law on Free Access to Information of Public Importance – Serbia, <https://www.rti-rating.org/country-data/Serbia/>, доступан 28. 4. 2025.
2. Повереник за информације од јавног значаја и заштиту података о личности. (2025). Извештај Повереника за информације од јавног значаја и заштиту података о личности за 2024. годину, https://www.poverenik.rs/images/stories/dokumentacija-nova/izvestajiPoverenika/2024/Godi%C5%A1nji_izve%C5%A1taj_2024.pdf, доступан 3. 5. 2025.
3. *Стирашеија одбране Републике Србије*, Службени гласник Републике Србије, бр. 94/2019.
4. *Устав Републике Србије*, Службени гласник Републике Србије, бр. 98/2006 и 115/2021.

Друштвено-правна ограничења у примени Закона о слободном
приступу информацијама од јавног значаја

5. *Закон о слободном њрисџују информацијама од јавної значаја*, Службени гласник Републике Србије, бр. 120 /2004, 54/2007, 104/2009, 36/2010 и 105/2021.
6. *Закон о џајносџи џодаџака*, Службени гласник Републике Србије, бр. 104/09.
7. *Закон о опитем управном поступку*, Службени гласник Републике Србије, бр. 18/2016, 95/2018 – аутентично тумачење и 2/2023 – одлука УС.

Socio-Legal Constraints in the Implementation of the Law on Free Access to Information of Public Importance

Abstract: *In the era of global social changes and rapid technological development, free access to information of public importance has emerged as a key indicator of the level of democratic development of a society. From the perspective of social significance, free access to such information represents a decisive factor in establishing effective state and social mechanisms to combat various forms of threats, such as corruption. At the same time, free access to this type of information is defined as a fundamental human right in modern democratic societies, grounded in the principles of transparency, government accountability, and citizen participation in public affairs. However, despite its recognized social value and foundation in human rights and freedoms, certain restrictions are justifiably imposed in practice, primarily concerning the protection of national security. Even in such cases, limitations must be clearly defined by legislation. Nonetheless, the misuse of the concept of national security—often invoked as an unfounded justification for denying access to public information—may lead to mistrust in institutions. Therefore, transparency in institutional work, while respecting the need to protect sensitive data, constitutes the cornerstone of an adequate system.*

In the Republic of Serbia, the right to free access to information of public importance is guaranteed by the Constitution, the Law on Free Access to Information of Public Importance, and international conventions such as the European Convention on Human Rights and the International Covenant on Civil and Political Rights. Particular challenges in the realization of this right, especially in balancing national security interests with the public's right to know, arise in the defense sector. Although the defense system inherently involves specific security sensitivities, it is not exempt from the obligation of transparency. The principle of accountability in democratic societies requires that defense institutions remain accessible to the public, except in cases where disclosure would seriously jeopardize national security. Problems occur when public authorities broadly interpret and misuse the notion of national security to conceal information of public interest.

The Commissioner for Information of Public Importance and Personal Data Protection plays a crucial role in overseeing the implementation of the

law. However, in recent years, the capacities of this institution have been limited, while the enforcement of its decisions often depends on political will and institutional readiness to act in accordance with the law. Of particular concern is the systematic ignoring or rejection of some of the most significant requests, such as those related to the spending of public funds or contracts with private companies. One of the key challenges in the upcoming period will be strengthening the independence and institutional capacity of the Commissioner, as well as raising citizens' awareness of their right to request information. Additionally, ensuring real accountability of institutions that violate the law remains of utmost importance, as this is still insufficiently enforced in practice.

Keywords: *prevailing interest, national security, information of public importance, protection of classified information, human rights and freedoms, free access.*

Упутство ауторима

Часопис Министарства унутрашњих послова Републике Србије „Безбедност“ објављује научне радове из подручја права, наука о безбедности, полицијских наука и криминалистике на српском и енглеском језику, који претходно нису објављивани.

Часопис излази три пута годишње. PDF верзија часописа доступна је на адреси: <http://www.mup.gov.rs> у поднаслову **Публикације**.

Рукописи се достављају преко система за online уређивање часописа, посредством платформе Assistant - Српски цитатни индекс (SCIndex), путем опције „Пријави рукопис“, за који је потребно регистровати налог, уколико сте нови корисник, путем линка: <https://aseestant.ceon.rs/index.php/bezbednost/login>

Текст рукописа треба да буде урађен на рачунару (фонт Times New Roman, ћирилично писмо, величина слова 14 pt за наслов – bold, 12 pt за основни текст, 65 словних знакова у једном реду, од 26 до 30 редова на једној страници, стандардне маргине). Научни и стручни радови могу да буду обима до 16 страна (30.000 знакова укључујући размаке).

На самом почетку писања текста обавезно укључити аутоматску хифенацију текста (Page Layout, Hyphenation, Automatic), а како не би долазило до непотребног размака између речи у реченици.

Рад треба да садржи: апстракт, кључне речи, текст чланка, закључак, литературу и резиме на енглеском језику. Код оригиналних научних радова апстракт садржи циљ истраживања, методе, кључни резултат и закључак (од 100 до 250 речи које читаоцу омогућавају да брзо и тачно оцени релевантност чланка кроз кратак информативни приказ). Апстракт на српском језику треба да стоји између заглавља

(име аутора и наслов рада) и кључних речи. После апстракта налазе се кључне речи (до пет).

Након апстракта следи текст чланка чију структуру за оригиналне научне радове чини: увод, материјал и методи, резултати, дискусија и закључак.

Код прегледних радова структуру текста чини увод, поднаслови, закључак и литература. Називи подналова у раду пишу се фонтом величине 12 pt, bold, центрирано на средини и без коришћења редних бројева.

Резиме на енглеском језику поставља се на крају текста, после одељка Литература, са називом рада (величина фонта текст 12 pt – italic). Резиме на енглеском језику даје се у проширеном облику (300-400 речи) са детаљнијим презентовањем резултата истраживања.

Назив и број пројекта, односно назив програма у оквиру којег је чланак настао, као и назив институције која је финансирала пројекат или програм наводи се у посебној назнаци при дну прве стране чланка.

Табеларни и графички прикази треба да буду дати на једнообразан начин, с тим што се називи табела пишу изнад, а називи графичких приказа испод. Прикази се могу дати и у виду посебног прилога на крају чланка, с тим што је потребно у тексту нагласити позивање на њихов садржај (Прилог 1, Прилог 2, ...). Пожељно је да наслови свих приказа буду дати двојезично, на српском и на енглеском језику (величина фонта 11 pt, italic), у формату JPEG или EPS, и да њихова резолуција износи минимум 300 dpi. За графичке прилоге урађене у Excel-у и другим апликативним софтверима треба користити различите растерске тонове црне боје.

Фусноте (напомене) користити само за суштинска запажања, нужне пропратне коментаре, упућивање на корисну литературу (Више о томе ...) и назнаке о коришћеним помоћним изворима (на пример, о научној грађи, законској регулативи, приручницима, документима, извештајима итд.), али не могу бити замена за цитирану литературу.

Цитате (навођење) у тексту не обележавати фуснотама, већ на крају цитата или при позивању на нечије дело (Мијалковић, 2006). Обавеза је аутора да се приликом позивања на изворе у оквиру чланка, тј. цитирања других аутора, њихова имена пишу у оригиналу, са годином објављеног рада и бројем странице у загради, која је одвојена једним табулатором након знака интерпункције – две тачке (Мијалковић, 2009: 147), а уколико се цитира више од два аутора, тада се у тексту помиње само први уз скраћеницу: *et all.* (Урошевић *et all.*, 2009: 92). Зарезом се одваја аутор од године издања, а тачка-зарезом (;) различити аутори различитих дела (Симоновић, 2012; Ђорђевић, 2013), при чему се низ референци даје абecedним редом у оквиру једног пара заграда. Број стране се од године издања одваја двотачком (:). Ако се наводи исти аутор са више радова у једној години, тада се уз наредне радове додају абecedна слова поред године, као на пример: (Милојковић, 2013а), (Милојковић, 2013б) итд. Страна имена у тексту би требало транскрибовати на српски језик, с тим што се у загради наведе име у оригиналу. Референце у заградама би требало писати у оригиналу.

Ако је аутор институција или се ради о колективном носиоцу ауторских права, наводи се минимум података неопходан за идентификацију (Републички завод за статистику, 2009).

Приликом цитирања извора са Интернета наводи се Интернет адреса, на пример: (<http://www...> , доступан 10. 1. 2010. године). Због сталне измене *www* окружења, наводи се датум када је текст скинут са мреже. За референце у електронском облику потребно је нагласити да се ради о електронском извору – Електронска верзија и/или Интернет адреса.

Од суштинске је важности да се цитати у тексту и листа библиографских јединица на крају текста у потпуности слажу. Сваки цитат из текста мора да се нађе на листи библиографских јединица и обрнуто. Такође, само цитати из текста је потребно да буду на листи библиографских јединица.

У списку литературе радови се наводе у оригиналу (референце се не преводе на језик рада), са нумерацијом, абecedним редом по презименима аутора и то на следећи начин:

Врста рада	Референце
Часопис	Симоновић, Б. (2009). Стандардизација и акредитација као један од начина професионализације полиције и криминалистичке службе. <i>Безбедност</i> , 51(1-2): 236-253.
Монографија	Мијалковић, С. (2009). <i>Национална безбедност</i> . Криминалистичко-полицијска академија, Београд.
Зборник радова	Бановић, Б., Маринковић, Д., (2005). <i>Специјалне истражне радње и нове тенденције у савременој науци кривичног права</i> , У Зборник радова „Нове тенденције у савременој науци кривичног права и наше кривично законодавство“, XLII Саветовање Удружења за кривично право и криминологију СЦГ, Златибор-Београд, стр. 509-543.
Законски прописи	<i>Закон о полицији</i> , Службени гласник Републике Србије, бр. 101/2005, 63/2009 - Одлука УС 92/2011 и 64/2015.
Е-извор	Witkowski, J., (2002). <i>Can Juries Really Believe What They See? New Foundational Requirements for the Authentication of Digital Images</i> , Journal of Law & Policy, 10: 267, http://law.wustl.edu/Journal/10/p267_Witkowski_book_pages.pdf . доступан 10. 1. 2010.

Наслови цитираних домаћих часописа, монографија, уџбеника и зборника радова дају се у оригиналном, пуном облику, али никако у преведеном облику.

Рукописи подлежу анонимној рецензији два рецензента из земље или иностранства. Рецензенти не могу бити из исте институције у

којој су запослени аутори чланака.

Уредништво задржава уређивачко право да на основу рецензије, актуелности рада, увида у рад и вођене евиденције одлучи да ли ће, када и у ком обиму рад бити објављен. Могуће примедбе и сугестије рецензента и/или уредника достављају се ауторима ради исправке.

Објављени радови се хонораришу, а необјављени се не враћају ауторима. Аутори би требало Уредништву да доставе: пуно име и презиме, адресу, е-mail, број телефона, фотокопију личне карте и банковне картице, на адресу: Уредништво часописа „Безбедност“, Булевар Зорана Ђинђића 104, 11070 Нови Београд, телефон: 011/3148-734, телефакс: 011/3148-749, е-mail: upobr@mup.gov.rs.

Позивамо све досадашње и нове ауторе да својим стручним, научним прилозима обогате садржај нашег, у научној и стручној јавности већ афирмисаног часописа са дугогодишњом традицијом, а у заједничком циљу да се унапреди полицијска пракса, подигне ниво безбедносне културе, и обезбеди праћење савремених научних и стручних достигнућа у безбедносној проблематици. Такође, напомињемо да је могућ заједнички – коауторски наступ страних и домаћих аутора.

**ГЛАВНИ И ОДГОВОРНИ
УРЕДНИК ЧАСОПИСА
„БЕЗБЕДНОСТ“**

Проф. др Божидар Ошашевић



PDF верзија часописа доступна је на адреси: <http://www.mup.gov.rs> у поднаслову Публикације

БЕЛЕШКЕ:

БЕЛЕШКЕ:

БЕЛЕШКЕ:

www.mup.gov.rs

Упутство ауторима