УДК: 342.738:061.1EU
Biblid 1451-3188, 25 (2026)
Год XXV, бр. 94-95, стр. 94–119
Изворни научни рад
Рад примљен 13. 05. 2026. године
Рад одобрен 02. 06. 2026. године
DOI: https://doi.org/10.18485/iipe_ez.2026.25.94_95.5

НОРМАТИВНЕ ПАРАЛЕЛЕ ЗАШТИТЕ ЛИЧНИХ ПОДАТАКА У ЕВРОПСКОЈ УНИЈИ И У РЕПУБЛИЦИ СРБИЈИ

*Сергеј УЉАНОВ**

***Апстракт**:* У ери четврте индустријске револуције, подаци о личности постали су један од највреднијих ресурса дигиталне економије, али истовремено и једна од најрањивијих тачака приватности појединца. Њихово масовно прикупљање, алгоритамска обрада и глобални проток информација наметнули су потребу за чврстим и униформним правним оквиром, који може да одговори на изазове које традиционално право није предвидело. Овај рад анализира степен усклађености и кључне нормативне паралеле између правног оквира заштите података о личности у Европској унији (ЕУ) и Републици Србији. Централни предмет истраживања је однос између Опште уредбе о заштити података (*General Data Protection Regulation* – GDPR) и домаћег Закона о заштити података о личности (ЗЗПЛ) из 2018. године. Аутор полази од тезе да је Република Србија, у оквиру процеса европских интеграција, извршила екстензивну хармонизацију прописа, преузимајући основне концепте, начела обраде и права лица на која се подаци односе из европског модела. У првом делу рада разматрају се еволутивни процеси који су довели до усвајања актуелних прописа, док се централни део бави компаративном анализом института као што су начела обраде, правни основи и улога надзорних тела. Посебан акценат стављен је на институционални оквир,

* Факултет за пословне студије и право, Универзитет „Унион – Никола Тесла“, Београд. E-mail: sergej.uljanov@fpsp.edu.rs. ORCID iD: https://orcid.org/0000-0003-1739-0335

упоређивањем овлашћења Повереника за информације од јавног значаја и заштиту података о личности у Републици Србији са надзорним телима у државама чланицама ЕУ, уз осврт на значајне разлике у казненој политици и механизмима принуде. Завршни сегмент рада посвећен је изазовима прекограничног преноса података и перспективама Републике Србије у погледу добијања Одлуке о адекватности од стране Европске комисије. Закључна разматрања указују на то да, упркос високом степену нормативне усклађености, практична примена и обезбеђивање пуне ефективности права у Републици Србији и даље наилазе на изазове услед специфичних друштвено-правних околности и административних капацитета.

Кључне речи: Заштита података о личности, *General Data Protection Regulation* (GDPR), Закон о заштити података о личности (ЗЗПЛ), Повереник за информације од јавног значаја и заштиту података о личности, хармонизација права

1) УВОД

Живимо у добу у којем су подаци о личности престали да буду тек пука техничка карактеристика појединца и постали једна од најснажнија валута глобалне економије. Револуционарни напредак у областима вештачке интелигенције, обраде великих количина података (*big data*), и свеприсутне дигитализације довео је до ситуације у којој традиционални концепти приватности постају недовољни. Као део наше реалности „интернет и друштвене мреже су, без претеривања, постале део нашег свакодневног живота, 'ушавши' у сваки део људског бића, у сваки његов ген".[1] У таквим околностима, право више не може бити само пасивни посматрач друштвених промена, већ мора постати активан механизам заштите дигиталног интегритета сваког човека. Развој права заштите података о личности на глобалном нивоу карактерише тежња за успостављањем универзалних стандарда који превазилазе националне границе, чиме се приватност штити у контексту све интензивније дигиталне размене података.[2] ЕУ је, препознајући ове изазове, донела Општу уредбу о заштити података (GDPR) не само као регулаторни акт већ и као цивилизацијски стандард који настоји

[1] Драгана Петровић, „Сајбер безбедност vs. приватност – општа разматрања и основи заштите", *Европско законодавство*, Година XXII, бр. 84, октобар–децембар 2023, стр. 191.

[2] Lee A. Bygrave, *Data Privacy Law: An International Perspective*, Oxford University Press, Oxford, 2014, p. 112.

да појединцу врати контролу над његовим дигиталним трагом.[3] За Републику Србију овај европски пут није представљао само спољнополитички циљ већ и неопходност унутрашње правне трансформације. Доношење новог Закона о заштити података о личности (ЗЗПЛ), био је одговор на насушну потребу за правном сигурношћу у земљи која се убрзано креће ка потпуној дигитализацији јавних услуга и привредних токова.[4] У жељи да избегнемо пуку компаративну анализу законских одредби потрудићемо се да осветлимо дубљу динамику односа између права ЕУ и домаћег права. Кроз четири специфичне целине, истраживање нас води од историјских корена заштите података, преко суштинских начела обраде која су заједничка за обе јурисдикције, па све до институционалне борбе за ефикасну примену тих права у пракси. Посебна пажња биће посвећена прекограничним токовима података, који данас представљају крвоток међународне трговине, а чији су нормативи постали мерило демократичности и правне уређености једне државе. Иако на први поглед текст домаћег закона делује као веран одраз европског модела, стварна слика се појављује тек када анализирамо како се та правила суочавају са специфичностима нашег административног апарата и казненог система. У наредним редовима покушаћемо да пронађемо одговор на питање: да ли је Република Србија усвајањем европских норми заиста постала део заједничког безбедног дигиталног простора, или је пред нама још увек дуг пут до претварања правне теорије у стварну заштиту сваког појединца?

2) ЕВОЛУЦИЈА И ИЗВОРИ ПРАВА ЗАШТИТЕ ПОДАТАКА О ЛИЧНОСТИ У ЕУ И У РЕПУБЛИЦИ СРБИЈИ

Заштита података о личности у савременом правном поретку више се не посматра само као изведени сегмент права на приватност, већ и као аутономно основно право које појединцу омогућава стварну контролу над сопственим дигиталним идентитетом. Као један од најдинамичнијих сегмената модерних правних система, ова област је прешла дуг пут

[3] "Regulation (EU) 2016/679", *Official Journal of the European Union*, L 119, Luxembourg, 2016, односно General Data Protection Regulation (GDPR) или Општа уредба о заштити података ЕУ, донета је 14. априла 2016, а ступила на снагу 24. маја 2016. Њена обавезна примена почела је 25. маја 2018.

[4] „Закон о заштити података о личности", *Службени гласник Републике Србије*, бр. 87/2018, Београд, 2018, донет је 9. новембра 2018, ступио на снагу 21. новембра 2018, а у примени је од 21. августа 2019.

еволуције – од примарно техничког питања безбедности информација до нивоа фундаменталног људског права које је дубоко укорењено у уставним оквирима развијених демократија. Нормативна паралела између ЕУ и Републике Србије која је данас евидентна, није само резултат географске близине или пуке правне технике. Она је директна последица сложеног и деценијама дугог процеса европских интеграција и тежње ка стварању јединственог и безбедног дигиталног тржишта. Овај процес је кулминирао усвајањем капиталних правних аката који су суштински променили начин на који субјекти јавног и приватног сектора прикупљају, чувају и обрађују информације. Разумевање тренутног правног оквира у Републици Србији стога је немогуће без детаљне анализе његових европских корена и међународних стандарда који служе као заједнички именитељ оба система.

Развојни пут правне регулације – од Директиве 95/46/ЕС до Опште уредбе о заштити података (GDPR)

Развојни пут заштите података о личности унутар ЕУ представља еволуцију од инструмента за олакшавање слободног протока информација на унутрашњем тржишту до успостављања једног од најстрожих режима заштите основних људских права у дигиталном добу. Овај процес није био линеаран, већ је представљао директан одговор на убрзани технолошки развој и све већи значај података као „погонског горива 21. века". Концепт дигиталне приватности је у овом периоду еволуирао од базичне техничке заштите до комплексног система људских права.[5] Камен темељац модерне заштите података у ЕУ била је Директива Европске заједнице 95/46/ЕС.[6] Донета у време када је интернет био у повоју, она је поставила основне принципе који су и данас релевантни: начело законитости, ограничење сврхе и сразмерност. Међутим, као правни инструмент, Директива је по својој природи захтевала имплементацију кроз национална законодавства држава чланица. Ово је довело до озбиљне фрагментације правног оквира.[7] Државе су користиле широко поље дискреције које им је директива остављала,

[5] Orla Lynskey, *The Foundations of EU Data Protection Law*, Oxford University Press, Oxford, 2015, p. 44.

[6] "Directive 95/46/EC", *Official Journal of the European Communities*, L 281, Luxembourg, 1995, донета је 24. октобра 1995, ступила на снагу 13. децембра 1995 и престала да важи 25. маја 2018.

[7] Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide*, Springer, Berlin, 2017, p. 12.

стварајући различите нивое заштите и административне баријере које су отежавале пословање компанијама које су хтеле да делују на нивоу целе Уније. Правни пејзаж се суштински мења 2009. године ступањем на снагу Лисабонског уговора.[8] Овим уговором, Повеља о основним правима ЕУ добија карактер примарног права у овом међународноправном субјекту, а њен чл. 8. прокламује заштиту података о личности као аутономно основно право, одвојено од општег права на приватност.[9] Ово је био кључни тренутак који је приморао европске институције да осмисле нови, снажнији и јединственији регулаторни оквир. Као одговор на ове изазове, након вишегодишњих преговора, 2016. године усвојена је GDPR. За разлику од претходне директиве, GDPR је Уредба, што значи да је директно применљива у свим државама чланицама без потребе за посредовањем националних парламената. Циљ је био јасан: унификација права (*harmonisation by regulation*) која је нужна због технолошке револуције.[10] GDPR је увела радикалне промене у парадигму заштите, које можемо означити као:

- *Екстериторијалну примену*: Правила се примењују на све субјекте који нуде робу или услуге грађанима ЕУ, без обзира на то где се седиште компаније налази (нпр. Силицијумска долина у Сједињеним Америчким Државама).
- *Концепт одговорности* – "accountability": Више није довољно само поштовати закон, већ руковалац мора бити у стању да у сваком тренутку документовано докаже да поступа у складу са прописима.
- *Нова права грађана:* Уведени су институти попут права на заборав (брисање) и права на преносивост података, који оснажују правни положај појединца у односу на позицију технолошких гиганата.
- *Строге казне:* Увођење казни до 20 милиона евра или 4% укупног годишњег промета на светском нивоу дало је „оштрицу" овом пропису, претварајући заштиту података из административног оптерећења у приоритетно питање корпоративног управљања.

---

[8] "Treaty of Lisbon", *Official Journal of the European Union*, C 306, Lisbon, 2007, потписан је 13. децембра 2007, а ступио на снагу 1. децембра 2009.

[9] "Charter of Fundamental Rights of the European Union", *Official Journal of the European Union*, C 303, Luxembourg, 2007, проглашена је свечано у Ници 7. децембра 2000, а њена прилагођена верзија проглашена је у Стразбуру 12. децембра 2007. и ступила на снагу 1. децембра 2009.

[10] Christopher Kuner *et al.*, Christopher Kuner *et al.* (eds.), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, Oxford, 2020, p. 24.

Наведена транзиција из Директиве 95/46/ЕС за GDPR означила је крај ере у којој је заштита података била опциона или секундарна, постављајући стандард који ће убрзо постати глобални „репер“ *(benchmark)* или референтна вредност за законодавне реформе у Републици Србији.

Хармонизација домаћег законодавства и доношење Закона о заштити података о личности (ЗЗПЛ)

Процес хармонизације права заштите података о личности у Републици Србији нераскидиво је везан за амбиције наше земље ка чланству у ЕУ. Овај пут карактерише транзиција од базичног нормативног оквира ка комплексном систему који настоји да у потпуности реплицира високе европске стандарде, при чему је процес европеизације домаћег законодавства постао кључни покретач реформи у области основних права. Постојећа уставноправна гаранција тајности података недвосмислено представља *conditio sine qua non* овог нормативног прилагођавања[11] Први значајнији корак учињен је доношењем Закона о заштити података о личности из 2008. године.[12] Овај акт био је моделован према тада важећој Директиви 95/46/ЕС и представљао је пионирски подухват у домаћем правном систему. Њиме је први пут системски уређена ова област и успостављена је независна институција Повереника за информације од јавног значај и заштиту података о личности (Повереник).[13] Међутим, Закон је веома брзо почео да показује озбиљне недостатке. Његове одредбе биле су превише опште, казнена политика неефикасна, а процедурална решења нису могла да испрате дигиталну трансформацију друштва. Додатни проблем представљала је чињеница да је Република Србија 2008. године била на почетку дигитализације, док је деценију касније обрада података постала основна делатност не само технолошких компанија већ и државне управе. Кључни правни и политички импулс за суштинску реформу произашао је из Споразума о стабилизацији и придруживању, према чијим је чланом 81. Република

[11] „Устав Републике Србије“, чл. 42, *Службени гласник Републике Србије*, бр. 98/2006 и 115/2021, Београд, 2006.

[12] „Закон о заштити података о личности“, *Службени гласник Републике Србије*, бр. 97 од 27. октобра 2008, 104 од 16. децембра 2009 – др. закон, 68 од 18. јула 2012 – УС, 107 од 9. новембра 2012, 87 од 13. новембра 2018 – др. закон, Београд, 2008, престао да важи 21. августа 2019.

[13] „Закон о заштити података о личности“ (2008), чл. 2, т. 11.

Србија преузела обавезу да своје законодавство усклади са правним тековинама ЕУ, уз обезбеђивање независног надзорног тела са довољним ресурсима.[14] Како је ЕУ у међувремену усвојила GDPR, Србија се нашла пред императивом не само да „поправи" стари закон већ и да изгради потпуно нови систем који ће бити компатибилан са новим европским поретком.[15] Резултат тог процеса је актуелни домаћи ЗЗПЛ, усвојен у новембру 2018. године, са одложеном применом до августа 2019. Овај Закон није само усклађен са GDPR-ом, већ представља његову дословну рецепцију у домаћи правни поредак.[16] Доношење ЗЗПЛ-а било је праћено бројним стручним полемикама. Критичари су истицали да је „механичко превођење" сложене европске уредбе на српски правни језик довело до одређених номотехничких нејасноћа и тешко преводивих термина. Ипак, законодавац се одлучио за овај приступ како би осигурао да српске компаније и институције говоре „истим језиком" као и њихови партнери у ЕУ. Специфичност српског Закона, која га разликује од самог текста GDPR-а, јесте то што је у свој текст Закона инкорпорисао и решења из тзв. „Полицијске директиве" (*Law Enforcement Directive* – LED), односно Директиве (EU) 2016/680.[17] То значи да ЗЗПЛ у Србији јединствено регулише и општу обраду (коју врше фирме, банке, болнице) и обраду коју врше надлежни органи у сврхе спречавања, истраге и откривања кривичних дела. Овакав „свеобухватни" приступ учинио је Закон изузетно обимним и комплексним, али је формалноправно затворио круг хармонизације, испуњавајући захтеве из Поглавља 23 у преговорима са Европском унијом.

---

[14] "Stabilisation and Association Agreement between the European Communities and their Member States, of the one part, and the Republic of Serbia, of the other part", *Official Journal of the European Union*, L 278, Luxembourg, 2008, потписан је у Луксембургу 29. 4. 2008, у Републици Србији ратификован 9. септембра 2008, а ступио на снагу 1. септембра 2013.

[15] Андреј Дилигенски *et al.*, *Право заштите података – GDPR*, Институт за упоредно право, Београд, 2019, стр. 148.

[16] Стефан Андоновић, Драган Прља, *Основи права заштите података о личности*, Институт за упоредно право, Београд, 2020, стр. 37–40.

[17] "Directive (EU) 2016/680", *Official Journal of the European Union*, L 119, Luxembourg, 2016, донета је 27. априла 2016, ступила на снагу 5. маја 2016, а у обавезној примени од 6. маја 2018.

Међународни уговори као заједнички именитељ

Поред примарних законских аката, нормативна паралела између ЕУ и Републике Србије темељи се на чврстом ослонцу међународног права, где кључну улогу играју документи Савета Европе. Док GDPR представља врхунац регионалне унификације унутар ЕУ, међународни уговори служе као шири оквир који омогућава да се заштита података третира као универзална вредност, а не само као тржишно правило. Централно место у овом контексту заузима Конвенција о заштити лица у односу на аутоматску обраду личних података, позната као Конвенција 108, усвојена 1981. године.[18] Ова конвенција је једини правно обавезујући међународни инструмент глобалног карактера који државе обавезује да у своје унутрашње право угради базичне принципе заштите података.[19] За Републику Србију, ратификација ове Конвенције и њеног Додатног протокола била је од кључног значаја, јер је тиме започет процес усклађивања домаћег правног система са европским стандардима.[20] Према Уставу Републике Србије потврђени међународни уговори саставни су део правног поретка и примењују се непосредно, што значи да принципи Конвенције 108 имају снагу која је изнад обичних законских одредби. Еволуција овог међународног оквира настављена је усвајањем тзв. Конвенције 108+, која је модернизована верзија Конвеције 108 из 2018. године. Овај документ директно је усклађен са стандардима GDPR-а и донет је с циљем да се принципи приватности заштите у ери вештачке интелигенције и масовног профилисања.[21] За Републику Србију, као

[18] "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data", *European Treaty Series*, No. 108, Strasbourg, 1981, донета је 28. јануара 1981, ступила на снагу 1. октобра 1985, ратификована у Савезној Републици Југославији 22. маја 1992, а у Републици Србији ступила на снагу 1. јануара 2006. године.

[19] Graham Greenleaf, "'Modernising' data protection Convention 108: A safe basis for a global privacy treaty?", *Computer Law & Security Review*, 29, 4, p. 431.

[20] „Закон о потврђивању Протокола о измени Конвенције о заштити лица у односу на аутоматску обраду личних података", *Службени гласник Републике Србије – Међународни уговори*, бр. 4/2020, Београд, 2020, донет је 24. фебруара 2020, а ступио на снагу 11. марта 2020.

[21] "Convention for the Protection of Individuals with regard to the Processing of Personal Data: modernised Convention 108, Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data", *Council of Europe Treaty Series*, No. 223, Stasbourg, 2018, усвојена у Елсинору, ступиће на снагу када је 38 од 55 држава потписница Конвенције 108 буде ратификовало, у Републици

потписницу, ово је од огромног значаја јер јој омогућава да задржи статус земље која дели „европске вредности“ у погледу дигиталних права, чак и пре званичног чланства у ЕУ. Такође, неизоставан извор права је и Европска конвенција о људским правима, која гарантује право на поштовање приватног и породичног живота. Кроз богату праксу Европског суда за људска права, овај правни акт је интерпретиран тако да укључује и заштиту података о личности.[22] Будући да су и Република Србија и све државе чланице ЕУ потписнице ове Конвенције, одлуке суда у Стразбуру служе као заједнички путоказ за тумачење стандарда заштите. Наведени спектар правне регулативе делује као „везивно ткиво“ између права ЕУ и права Републике Србије. Он осигурава да, без обзира на мање номотехничке разлике у текстовима GDPR-а и домаћег ЗЗПЛ-а, суштина заштите остане идентична. Управо ови међународни стандарди представљају основу на којој Република Србија гради свој захтев за добијање Одлуке о адекватности (*adequacy decision*) од стране Европске комисије, што би коначно био и доказ да су наше „нормативне паралеле“ са Европском унијом постале потпуне.

3) УПОРЕДНА АНАЛИЗА ОСНОВНИХ НАЧЕЛА И ПРАВНИХ ОСНОВА ОБРАДЕ

Док прво поглавље нуди историјски и формални контекст, друго поглавље се бави супстанцијалним вредностима на којима почива заштита података. Нормативна паралела овде престаје да буде теоријска и постаје практична: Одредбе чл. 5 и чл. 6 GDPR-а односно чл. 5 и чл. 12 ЗЗПЛ-а, представљају „устав“ за сваког руковаоца подацима. У овом делу рада анализираћемо како су ови стубови заштите имплементирани у оба система и да ли идентичан текст закона увек подразумева и идентичну примену у пракси.

Анализа основних начела обраде – од законитости до одговорности

Начела обраде представљају фундаменталне аксиоме којих се сваки руковалац мора придржавати, без обзира на врсту података или сврху

Србији Конвенција 108+, односно наведени Протокол ратификован је 26. маја 2020.

[22] “Charter of Fundamental Rights of the European Union” (2007), Art. 8.

обраде. Чл. 5. GDPR-а и чл. 5 ЗЗПЛ-а наводе седам кључних принципа који су у српско право пренети готово без икаквих измена, чиме је постигнута потпуна терминолошка усклађеност.[23] Прво и основно начело је законитост, поштење и транспарентност. Оно налаже да обрада мора имати основ у закону, али и да се према лицу чији се подаци обрађују поступа поштено, уз јасно информисање о томе ко, зашто и колико дуго користи његове податке. У Европској унији Суд правде је кроз бројне пресуде нагласио да транспарентност није само пуко обавештење на сајту, већ мора бити пружена на језику који је разумљив просечном кориснику.[24] Домаћи ЗЗПЛ преузима овај стандард, обавезујући руковаоце на „кратке, провидне и лако разумљиве" информације.[25]

Друго значајно начело је ограничење сврхе. Оно забрањује да се подаци прикупљени за једну сврху (нпр. достава робе) касније користе за другу, некомпатибилну сврху (нпр. агресивни директни маркетинг). Овде се јавља важна паралела у погледу обраде у сврхе архивирања од јавног интереса или научног истраживања, што оба система дозвољавају као изузетак, под условом да се примене одговарајуће мере заштите. Начело минимизације података, које се често описује изразом „мање је више", директно се супротставља модерној пракси прикупљања што већег броја информација.[26] Руковалац сме да тражи само оне податке који су му неопходни за остварење сврхе. Паралелно са тим, примењује се и начело тачности, које обавезује на ажурирање података, као и начело ограничења чувања, које налаже да се подаци бришу чим престане потреба за њима.

Међутим, најзначајнија иновација коју су и GDPR и ЗЗПЛ увели јесте начело одговорности. Еволуција концепта одговорности у европском праву јасно указује на то да руковаоци и обрађивачи више немају само пасивну обавезу поштовања норми, већ активну дужност доказивања усклађености, што је додатно потврђено и кроз екстензивно тумачење обавеза субјеката у пракси Суда правде у ЕУ.[27] Ово начело је променило

[23] "Regulation (EU) 2016/679" (2016), Art. 5; „Закон о заштити података о личности" (2018), чл. 5.

[24] Peter Carey, *Data Protection: A Practical Guide to UK and EU Law*, Oxford University Press, London, 2018, p. 20.

[25] Андреј Дилигенски *et al.*, *Право заштите података – GDPR*, *op. cit.*, стр. 137.

[26] Cécile de Terwangne, "Article 5. Principles relating to processing of personal data", *The EU General Data Protection Regulation (GDPR): A Commentary*, *op. cit.*, p. 313.

[27] Андреј Дилигенски *et al.*, *Право заштите података – GDPR*, *op. cit.*, стр. 125–127.

терет доказивања. Раније је надзорни орган морао доказивати кршење закона; данас руковалац мора бити у стању да проактивно докаже да је у сваком тренутку усклађен са свим претходно наведеним начелима. То подразумева вођење евиденција о радњама обраде, спровођење техничких мера и едукацију запослених. Управо овде се огледа најснажнија нормативна паралела: наш законодавац је препознао да без овог начела сва остала остају „мртво слово на папиру". Разлика се ипак појављује у свести актера – док је у ЕУ ово начело постало део корпоративне културе, у Републиици Србији се оно и даље често посматра као пука административна препрека.[28]

Правни основи за обраду – изазови легитимног интереса

Да би обрада података била законита, она не сме бити произвољна, већ мора бити утемељена на једном од шест таксативно наведених правних основа. Чл. 6. GDPR-а и чл. 12 ЗЗПЛ-а предвиђају идентичну листу основа: пристанак, извршење уговора, поштовање законских обавеза, заштита животно важних интереса, обављање послова у јавном интересу и легитимни интерес.[29] Иако су нормативно идентични, у пракси се ова два система суочавају са различитим изазовима приликом њихове интерпретације.

Пристанак се често погрешно сматра најважнијим основом, док је он заправо најнестабилнији, јер се може повући у сваком тренутку. И у ЕУ и у Републици Србији, стандард за пристанак је драстично подигнут: он мора бити добровољан, специфичан, информисан и недвосмислен израз воље. Посебна паралела постоји у дигиталној сфери – прећутни пристанак или унапред означена поља (*opt-out*) више нису дозвољени ни у Бриселу ни у Београду.[30]

Највише простора за полемику, али и најширу примену у привреди, оставља легитимни интерес руковаоца или треће стране. Овај основ је специфичан јер захтева спровођење тзв. „теста балансирања". Руковалац

[28] Jakub Míšek, "Data protection as performance-based regulation", Eleni Kosta *et al.* (eds.), *Research Handbook on EU Data Protection Law*, Edward Elgar Publishing, Cheltenham, 2022, p. 53.

[29] "Regulation (EU) 2016/679" (2016), Art. 5; „Закон о заштити података о личности" (2018), чл. 12.

[30] Данило Кривокапић *et al.*, *Водич кроз Закон о заштити података о личности и GDPR: тумачење новог правног оквира*, Мисија ОЕБС у Србији и SHARE Фондација, Београд, 2019, стр. 46.

мора да докаже да је његов пословни или безбедносни интерес претежнији од права и слобода појединца.[31] На пример, видео-надзор у банци ради спречавања пљачке је јасан легитимни интерес, док би видео-надзор у свлачионици био непропорционалан и незаконит.[32]

У Европској унији судска пракса и мишљења Европског одбора за заштиту података (*European Data Protection Board* – EDPB) детаљно су разрадили критеријуме за овај тест. У Републици Србији, с друге стране, приметна је одређена доза опреза код руковалаца. Због недостатка богате домаће судске праксе, српски субјекти се често радије ослањају на пристанак или уговор, чак и када би легитимни интерес био адекватнији основ. Ипак, нормативна подударност омогућава Поверенику у Републици Србији да директно користи смернице из ЕУ приликом тумачења овог појма, чиме се у пракси врши тиха, али ефикасна хармонизација. Такође, значајна паралела постоји и у погледу обраде на основу закона. И у ЕУ и у Републици Србији, уколико посебан закон (нпр. Закон о раду или Закон о банкама) налаже прикупљање одређених података, руковалац нема обавезу да тражи пристанак, јер је сама држава проценила да је та обрада неопходна за функционисање правног поретка.[33] Ова усклађеност осигурава правну предвидивост, која је кључна за функционисање међународне размене података.

Субјективна права лица на која се подаци односе и механизми њихове правне заштите

Средиште нормативне архитектуре и GDPR-а и ЗЗПЛ-а представља корпус права која припадају физичким лицима чији се подаци обрађују. Ова права нису само декларативна, већ представљају активна правна овлашћења којима појединац врши контролу над својим дигиталним идентитетом. Нормативна паралела у овом сегменту је апсолутна, јер је српски законодавац у потпуности преузео каталог права из GDPR-а, чиме је грађанима Републике Србије обезбеђен идентичан ниво правне заштите који уживају грађани ЕУ.[34]

---

[31] Дубравка Доленц, „Легитимни интерес као правни основ обраде особних података“, *Банкарство*, 49, 3, стр. 148–150.

[32] Стефан Андоновић и Драган Прља, *Основи права заштите података о личности*, *op. cit.*, стр. 122.

[33] *Ibid.*, стр. 113.

[34] “Regulation (EU) 2016/679” (2016), Chapter III (Art. 12–23); „Закон о заштити података о личности“ (2018), Глава III (чл. 21–40).

Први стуб ове заштите јесте право на приступ.[35] Оно омогућава лицу да од руковаоца добије потврду о томе да ли се његови лични подаци обрађују, као и детаљне информације о сврси, правном основу и примаоцима података.[36] Ово право је у дигиталној економији кључно, јер представља предуслов за остваривање свих осталих права. Без транспарентног увида у то шта руковалац поседује, заштита остаје илузорна. Два права која су изазвала највише пажње у јавности су право на брисање, односно „право на заборав" и право на преносивост података. Право на брисање омогућава појединцу да захтева уклањање својих података уколико више нису неопходни за сврху због које су прикупљени или уколико је пристанак повучен. Суд правде у ЕУ је у чувеном предмету *Google Spain* (2014) поставио стандарде за ово право, које је сада интегрални део и српског правног поретка.[37]

С друге стране, право на преносивост података представља новину која олакшава прелазак код другог пружаоца услуга (нпр. пренос података са једне друштвене мреже на другу или између банака), чиме се подстиче конкуренција и спречава „закључавање" корисника. Посебно важно у контексту савремених технологија је право на приговор, нарочито у ситуацијама када се обрада врши на основу легитимног интереса или у сврхе директног оглашавања. Уколико лице уложи приговор на обраду у сврхе директног оглашавања, руковалац по закону више нема право да обрађује податке у ту сврху, без могућности доказивања супротног. Коначно, оба система предвиђају строга правила у вези са аутоматизованим доношењем појединачних одлука и профилисање. Појединац има право да не буде предмет одлуке која се заснива искључиво на аутоматизованој обради (нпр. аутоматско одбијање кредита путем алгоритма), уколико та одлука производи правне последице по њега. Ова одредба је од виталног значаја у ери вештачке интелигенције, јер осигурава „људски надзор" над аутоматизованим процесима, што је стандард који Република Србија сада дели са ЕУ.[38] Нормативна

[35] "Regulation (EU) 2016/679" (2016), Art. 15; „Закон о заштити података о личности" (2018), чл. 26.

[36] Maria Tzanou, *The Fundamental Right to Data Protection*, Hart Publishing, Oxford, 2017, p. 114.

[37] Андреј Дилигенски *et al.*, *Право заштите података – GDPR*, *op. cit.*, стр. 173.

[38] Sandra Wachter *et al.*, "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation", *International Data Privacy Law*, 7, 2, p. 78.

подударност у овом сегменту ствара правну сигурност: грађанин Републике Србије који користи апликацију развијену у ЕУ, или грађанин ЕУ чије податке обрађује компанија у Републици Србији, може рачунати на идентичне процесне механизме за заштиту свог интегритета.

4) СУБЈЕКТИ ЗАШТИТЕ И ИНСТИТУЦИОНАЛНИ ОКВИР: НАДЗОРНА ТЕЛА И ЊИХОВА ОВЛАШЋЕЊА

Успех било ког нормативног система не зависи искључиво од квалитета законских одредби, већ од ефикасности институционалног механизма који те одредбе спроводи. У области заштите података о личности улога надзорних тела је од пресудног значаја, јер она делују као регулатори, едукатори, али и као органи који врше репресију над онима који крше права грађана. У овом поглављу анализираћемо нормативне паралеле и оперативне разлике између Повереника у Републици Србији и независних надзорних тела (*Data Protection Authority* – DPA) унутар ЕУ, са посебним освртом на њихову независност и казнена овлашћења.

Статус и улога Повереника у Републици Србији наспрам надзорних тела у државама чланицама ЕУ

Правни положај надзорних тела представља један од најважнијих захтева које поставља GDPR. Према европским стандардима, надзорно тело мора бити потпуно независно од било каквог спољног утицаја, било политичког или комерцијалног, и мора имати сопствене ресурсе за рад.[39] У ЕУ свака држава чланица има своје национално надзорно тело (нпр. *Commission Nationale de l'Informatique et des Libertés* – CNIL у Француској или *Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit* – BfDI у Немачкој), које на нивоу ЕУ координира Европски одбор за заштиту података (EDPB). У Републици Србији ову улогу обавља Повереник. Његов положај је нормативно дефинисан као самосталан и независан државни орган који за свој рад одговара Народној скупштини. Овде уочавамо јасну нормативну паралелу: критеријуми за избор Повереника, његов имунитет и забрана утицаја на његове одлуке, директно су моделовани према захтевима из чл. 52 GDPR-а.[40] Улога Повереника у домаћем правном

[39] "Regulation (EU) 2016/679" (2016), Art. 52; „Закон о заштити података о личности" (2018), чл. 73.

[40] Андреј Дилигенски *et. al.*, *Право заштите података – GDPR*, *op. cit.*, стр. 210–215.

поретку превазилази чисту административну контролу; он делује као кључни гарант очувања дигиталног интегритета појединца, настојећи да кроз своје механизме надзора осигура примену високих европских стандарда заштите, чак и у најкомплекснијим дигиталним окружењима.[41] Ипак, његова улога у Републици Србији је специфична, јер је он „хибридни" орган који штити два различита, мада сродна права: право на приступ информацијама и право на заштиту података. У већини држава чланица ЕУ ове функције су раздвојене, док у Србији Повереник мора балансирати између транспарентности органа власти и приватности појединца.

Када је реч о овлашћењима, GDPR и ЗЗПЛ предвиђају три групе надлежности:

- *Истражна овлашћења*: Право на приступ свим подацима и просторијама руковаоца како би се утврдило чињенично стање.
- *Корективна овлашћења*: Могућност издавања упозорења, налога за усклађивање обраде, или чак привремене и трајне забране обраде података.
- *Саветодавна овлашћења*: Давање мишљења на предлоге закона, одобравање кодекса понашања и едукација јавности.[42]

Највећа функционална разлика, која представља и главни изазов у процесу евроинтеграција, лежи у начину изрицања новчаних казни. Док надзорна тела ЕУ (попут оног у Ирској или Луксембургу) могу директно, у управном поступку, изрицати милионске казне које постају одмах извршне, Повереник у Републици Србији нема то овлашћење. Он може поднети захтев за покретање прекршајног поступка пред надлежним судовима, или изрећи казну путем прекршајног налога у фиксним, знатно мањим износима.[43] Ова асиметрија у „репресивној моћи" значајно утиче на превентивно деловање закона, јер је ризик за кршење прописа у Републици Србији са финансијске тачке гледишта знатно нижи него у ЕУ.[44]

[41] *Ibid.*, стр. 205–210.

[42] "Regulation (EU) 2016/679" (2016), Art. 58; „Закон о заштити података о личности" (2018), чл. 79.

[43] *Ibid.*, стр. 215.

[44] *Ibidem*

Механизми сарадње и концепт „јединствене тачке контакта“ (One-Stop-Shop)

Једна од најзначајнијих иновација коју уводи GDPR, а која представља изазов за државе које нису чланице ЕУ попут Републике Србије, јесте механизам сарадње и конзистентности.[45] У Еврпопској унији циљ овог механизма је да се осигура јединствена примена права на целој територији ЕУ, како би се избегло да различита надзорна тела доносе опречне одлуке о истим питањима. Централни стуб овог система је концепт „јединствене тачке контакта“ (*one-stop-shop*). Он омогућава компанијама које послују у више држава чланица ЕУ (нпр. имају седиште у Ирској, а кориснике у целој ЕУ) да комуницирају првенствено са једним, тзв. водећим надзорним телом. То тело координира истрагу са свим осталим „заинтересованим“ надзорним телима. Уколико дође до неслагања између националних органа, коначну реч доноси EDPB путем обавезујућих одлука. На тај начин, ЕУ делује као јединствен правни простор, што драстично смањује административне трошкове за привреду.[46] У Републици Србији, иако је ЗЗПЛ нормативно преузео терминологију сарадње, овај механизам у пуном капацитету не постоји. Република Србија, као држава изван ЕУ, не учествује у раду EDPB-а са правом гласа нити је део механизма „јединствене тачке контакта“. То значи да компанија из Републике Србије која нуди услуге грађанима ЕУ мора да се придржава одлука сваког појединачног надзорног тела у државама чланицама где су њени корисници, док Повереник у Републици Србији остаје „изолован“ од директног европског ланца одлучивања.[47] Ипак, нормативна повезаност се остварује кроз обавезу Повереника да прати и уважава праксу EDPB-а приликом тумачења одредби ЗЗПЛ-а. Република Србија настоји да кроз билатералне споразуме и чланство у мрежама попут Европске конференције органа за заштиту података (*European Conference of Data Protection Authorities*) надомести овај институционални јаз. Међутим, недостатак учешћа у формалним механизмима сарадње ЕУ остаје једна од главних тачака дисконтинуитета. Док је норма (у смислу текста закона) скоро идентична, процедурални пут до правде се значајно разликује: у ЕУ је он високо интегрисан и

[45] “Regulation (EU) 2016/679” (2016), Art. 63.

[46] Hielke Hijmans, “Article 65. Dispute resolution by the Board”, *The EU General Data Protection Regulation (GDPR): A Commentary*, *op. cit.*, pp. 1042–1043.

[47] Андреј Дилигенски *et al.*, *Право заштите података – GDPR*, *op. cit.*, стр. 218.

централизован, док је у Републици Србији и даље строго националан и зависан од билатералних односа са европским партнерима.[48]

Лице за заштиту података о личности (DPO) – институционални мост између прописа и праксе

Увођење обавезе именовања лица за заштиту података о личности (*Data Protection Officer* – DPO) представља један од најважнијих инструмената проактивне заштите у оквиру GDPR-а и српског ЗЗПЛ-а. Нормативна паралела је у овом сегменту врло изражена, јер оба закона дефинишу идентичне услове за именовање, положај и задатке овог лица, чиме се тежи стварању јединствене професионалне фигуре на европском нивоу.[49] Основна улога DPO је да делује као независни коректив унутар самог руковаоца. Он није одговоран за усклађеност, то је терет руковаоца, већ има улогу саветника и контролора. Кључни нормативни захтев, који Република Србија дели са Европском унијом, јесте независност. Руковалац не сме давати упутства лицу за заштиту података у погледу извршавања његових задатака, нити га сме казнити или отпустити због обављања његове дужности.[50] Ова гарантована независност је од пресудног значаја, јер DPO често мора да укаже на неправилности у раду саме управе предузећа или органа власти.

Задаци DPO-а су вишеструки:

- Информисање и саветовање: Едукација запослених о обавезама које проистичу из закона.
- Праћење усклађености: Контрола спровођења интерних аката и анализа ризика.
- Сарадња са надзорним телом: DPO служи као јединствена тачка контакта за комуникацију са Повереником у Републици Србији, односно надзорним телима у ЕУ.[51]

Ипак, у пракси се уочава одређена асиметрија. Док је у ЕУ професија DPO-а постала високо специјализована грана са јасним стандардима

[48] Paul M. Schwartz, "Global Data Privacy: The EU Way", *NYU Law Review*, 94, 4, p. 774.

[49] "Regulation (EU) 2016/679" (2016), Art. 37–39; „Закон о заштити података о личности" (2018), чл. 56–58.

[50] Peter Carey, *Data Protection: A Practical Guide to UK and EU Law*, *op. cit.*, p. 209.

[51] Cecilia Álvarez Rigaudias and Alessandro Spina, "Article 39. Tasks of the data protection officer", *The EU General Data Protection Regulation (GDPR): A Commentary*, *op. cit.*, pp. 715.

сертификације и струковним удружењима, у Републици Србији је овај институт још увек у фази профилисања. Чест изазов представља тзв. „сукоб интереса", где се у Републици Србији за DPO-а често именују лица која већ обављају руководеће функције, попут шефова у Сектору информационих технологија или правне службе. Оваква пракса директно компромитује њихову независност, јер лице за заштиту података не сме бити у позицији да самостално одређује сврху и начин обраде података које истовремено треба да надзире.[52] Упркос томе, нормативна обавеза да DPO поседује „стручно знање и познавање права и праксе у области заштите података" поставља висок праг који постепено подиже ниво правне свести и у Србији.[53] Ова фигура је постала неопходан „преводилац" комплексних правних норми у оперативне процесе, чиме се осигурава да нормативна паралела између ЕУ и Републике Србије добије свој пуни смисао у свакодневном пословању.

5) ИЗАЗОВИ ПРЕКОГРАНИЧНОГ ПРЕНОСА ПОДАТАКА И „ОДЛУКА О АДЕКВАТНОСТИ"

У глобално повезаном свету, подаци ретко остају унутар националних граница. Проток информација између Републике Србије и ЕУ је интензиван, било да је реч о раду страних компанија у нашој земљи, коришћењу *cloud* сервиса или сарадњи у области безбедности. Међутим, овај проток није безуслован. GDPR и ЗЗПЛ постављају строге баријере за извоз података у треће земље, како би се спречило да се подаци грађана нађу у јурисдикцијама са нижим нивоом заштите. У овом поглављу анализираћемо механизме који омогућавају овај пренос и пут наше државе ка добијању највишег нивоа поверења од стране Европске комисије.

Правни режим преноса података у треће државе и међународне организације

Нормативна паралела у погледу преноса података је веома јасна: GDPR и ЗЗПЛ полазе од опште забране преноса података у друге државе, осим ако су испуњени специфични услови који гарантују „адекватан ниво

[52] Стефан Андоновић, „Лице за заштиту података о личности у правном систему Србије", Стефан Андоновић et al. (ур.), *Заштита података о личности у Србији: зборник радова*, Институт за упоредно право, Београд, 2020, стр. 123, 125–126.

[53] Стефан Андоновић, „Лице за заштиту података о личности у правном систему Србије", *op. cit.*, стр. 121.

заштите“.[54] Циљ ове рестрикције је да се спречи заобилажење закона, односно да руковалац не сме извести податке у земљу где су права појединца мање заштићена него у матичној држави.[55] Оба система предвиђају хијерархију механизама за пренос:

- *Пренос на основу Одлуке о адекватности*: Ово је „златни стандард“. Ако Европска комисија или Влада Републике Србије утврди да одређена држава има систем заштите који је суштински еквивалентан њиховом, пренос података у ту државу може се одвијати слободно, без посебних дозвола. Република Србија је, у том смислу, на своју листу земаља са адекватном заштитом аутоматски уврстила све чланице ЕУ и потписнице Конвенције 108.[56]
- *Пренос уз примену одговарајућих мера заштите*: Ако нема одлуке о адекватности, руковалац мора сам обезбедити гаранције. Најчешћи алат су Стандардне уговорне клаузуле (*Standard Contractual Clauses* – SCC), тј. типска документа која обавезују примаоца података на поштовање правила заштите. Овде постоји занимљива паралела: Повереник у Републици Србији је усвојио сопствене стандардне уговорне клаузуле које су у великој мери усклађене са онима које користи Европска комисија.[57]
- *Обавезујућа пословна правила* (*Binding Corporate Rules* – BCR): Намењена су великим мултинационалним компанијама које преносе податке унутар своје групе широм света.

Главни изазов у овом сегменту је динамика односа. Док наша држава признаје ЕУ као сигурно уточиште за податке, Европска унија Републику Србију још увек третира као „трећу земљу“ без опште Одлуке о адекватности. То значи да сваки пренос података из ЕУ у нашу земљу (нпр. када матична фирма из Берлина шаље податке о запосленима својој кћерки-фирми у Београду) захтева додатне бирократске кораке попут потписивања уговорних клаузула. Такав дисбаланс у ефективној нормативној моћи недвосмислено указује на „парадоксалну ситуацију у којој“, из аспекта домаће легислативе, „нема препрека за изношење података из Републике Србије ка државама чланицама ЕУ, али се може уочити да у случају обрнутог

[54] “Regulation (EU) 2016/679” (2016), Art. 44–50; „Закон о заштити података о личности“ (2018), чл. 63–71.

[55] Orla Lynskey, *The Foundations of EU Data Protection Law*, *op. cit.*, p. 88.

[56] Андреј Дилигенски *et al.*, *Право заштите података – GDPR*, *op. cit.*, стр. 148.

[57] Андреј Дилигенски *et al.*, *Право заштите података – GDPR*, *op. cit.*, стр. 154.

процеса постоје велике и неретко непремостиве препреке".[58] Ова асиметрија је један од главних разлога зашто је потпуна нормативна и фактичка усклађеност императив за српску економију.

Пут ка добијању одлуке о адекватности – препреке и перспективе

Добијање Одлуке о адекватности од стране Европске комисије представља крајњи циљ процеса хармонизације и својеврсни „бели шенген" за проток података. Ова одлука би значила да ЕУ званично признаје да Република Србија нуди ниво заштите који је суштински еквивалентан оном у државама чланицама, чиме би се елиминисале све преостале административне баријере за нашу индустрију информационих технологија и привреду уопште. Потребно је нагласити да питање прекограничног протока информација за нашу земљу није само економско, већ и дубоко политичко питање дигиталног суверенитета, које захтева пажљиво балансирање између националних безбедносних интереса и обавеза преузетих из процеса европских интеграција.[59] Иако је Република Србија усвојила ЗЗПЛ који је верна копија GDPR-а, пут до добијања Одлуке о адекватности није завршен. Европска комисија приликом процене адекватности не разматра само текст закона, већ целокупан правни и друштвени систем.[60] На том путу Република Србија се суочава са неколико кључних препрека:

- *Независност и ресурси надзорног тела*: Европска комисија инсистира на томе да Повереник мора имати не само законску независност већ и довољно кадровских и финансијских капацитета да врши надзор над моћним субјектима, укључујући и државне органе. Сваки притисак на рад Повереника или игнорисање његових одлука од стране власти директно удаљава Републику Србију од позитивне оцене адекватности.[61]

[58] Остоја Калаба, „Прекогранични пренос података о личности у домаћем праву и праву Европске уније", *Европско законодавство*, Година XXII, бр. 84, октобар–децембар 2023, стр. 75.

[59] Данило Кривокапић *et al*., *Водич кроз Закон о заштити података о личности и GDPR: тумачење новог правног оквира*, *op. cit.*, стр. 63.

[60] Paul M. Schwartz, "Global Data Privacy: The EU Way", *op. cit.*, p. 794.

[61] "Commission Staff Working Document – Serbia 2021 Report accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions", pp. 25–26, *European Commission*, SWD(2021) 288 final, Strasbourg/Brussels, 2021.

Приступ органа безбедности личним подацима: Једна од најосетљивијих тачака у дијалогу са Бриселом је начин на који тајне службе и полиција приступају подацима грађана у сврхе националне безбедности, што представља изазов за међународноправне стандарде заштите приватности.[62] Након чувене пресуде Суда правде ЕУ у предмету *Schrems II* (2020), критеријуми за пренос података постали су знатно ригорознији, захтевајући додатне гаранције заштите приватности.[63] Наша земља мора да докаже да је приступ подацима од стране органа безбедности сразмеран, неопходан и подложан независној судској контроли, што је стандард који се често преиспитује у годишњим извештајима Европске комисије о нашем напретку.[64]

Пракса и ефикасност казнене политике: Као што је анализирано у претходним поглављима, немогућност Повереника да директно изриче казне представља системску разлику у односу на европски модел. Ова асиметрија у „репресивној моћи" значајно утиче на превентивно деловање закона, јер је ризик за кршење прописа у Републици Србији, са финансијске тачке гледишта, и даље знатно мањи него у ЕУ. Брисел пажљиво прати да ли су санкције у нашој држави „ефикасне, сразмерне и одвраћајуће".[65] Ако се кршења закона кажњавају минималним износима пред прекршајним судовима, ниво заштите се може оценити као недовољан упркос модерном закону.[66]

Перспектива наше земље у погледу добијања ове одлуке зависи од демонстрације политичке воље да се заштита података третира као приоритетно право, а не као формална препрека. Нормативна паралела је успостављена, па следи фаза доказивања функционалне паралеле. Добијање адекватности не би само олакшало пословање, већ би Републику

---

[62] Marko Milanovic, "Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age", *Harvard International Law Journal*, 2014, 56(1), p. 81.

[63] Ана Човић, „Пренос личних података након одлуке Европског суда правде Schrems II", Драган Вујисић (ур.), *Садашњост и будућност услужног права*, Институт за правне и друштвене науке, Крагујевац, 2022, 418–420.

[64] Дамјан Милеуснић *et al.*, *Приватност и заштита података о личности у Србији: Анализа одабраних секторских прописа и њихове примене*, Партнери за демократске промене Србија, Београд, 2021, стр. 70.

[65] Андреј Дилигенски *et al.*, *Право заштите података – GDPR*, *op. cit.*, стр. 215.

[66] Serbia 2021 Report [SWD(2021) 288 final], p. 25.

Србију позиционирало као регионалног лидера у дигиталној економији и сигурну дестинацију за инвестиције у области високих технологија.[67]

6) ИЗВОРИ

- Álvarez Rigaudias, Cecilia, Spina, Alessandro, "Article 39. Tasks of the data protection officer", Christopher Kuner, Lee A. Bygrave and Christopher Docksey (Eds.), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, Oxford, 2020, стр. 709–716.
- Андоновић, Стефан, Прља, Драган, *Основи права заштите података о личности*, Институт за упоредно право, Београд, 2020.
- Андоновић, Стефан, „Лице за заштиту података о личности у правном систему Србије", Стефан Андоновић, Драган Прља и Андреј Дилигенски (ур.), *Заштита података о личности у Србији: зборник радова*, Институт за упоредно право, Београд, 2020, стр. 117–128.
- Bygrave, Lee A., *Data Privacy Law: An International Perspective*, Oxford University Press, Oxford, 2014.
- Carey, Peter, *Data Protection: A Practical Guide to UK and EU Law*, Oxford University Press, London, 2018.
- Човић, Ана, „Пренос личних података након одлуке Европског суда правде Schrems II", Драган Вујисић (ур.), *Садашњост и будућност услужног права*, Институт за правне и друштвене науке, Крагујевац, 2022, стр. 415–427.
- Дилигенски, Андреј, Прља, Драган, Церовић, Дражен, *Право заштите података – GDPR*, Институт за упоредно право, Београд, 2019.
- Доленц, Дубравка, „Легитимни интерес као правни основ обраде особних података", *Банкарство*, 49, 3, стр. 144–157.
- Greenleaf, Graham, "'Modernising' data protection Convention 108: A safe basis for a global privacy treaty?", *Computer Law & Security Review*, 29, 4, pp. 430–436.
- Hijmans, Hielke, "Article 65. Dispute resolution by the Board", Christopher Kuner, Lee A. Bygrave and Christopher Docksey (Eds.), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, Oxford, 2020, pp. 1041–1052.

[67] Андреј Дилигенски *et al.*, *Право заштите података – GDPR*, *op. cit.*, стр. 341–343.

- Калаба, Остоја, „Прекогранични пренос података о личности у домаћем праву и праву ЕУ“, *Европско законодавство*, Година XXII, бр. 84, октобар–децембар 2023, стр. 41–77.
- Кривокапић, Данило Адамовић, Јелена Тасић, Дуња, Петровски, Андреј, Калезић, Петар, Кривокапић, Ђорђе, *Водич кроз Закон о заштити података о личности и GDPR: тумачење новог правног оквира*, Мисија ОЕБС у Србији и SHARE Фондација, Београд, 2019
- Kuner, Christopher, Bygrave, Lee A., Docksey, Christopher, “Background and Evolution of the EU General Data Protection Regulation (GDPR)”, Christopher Kuner, Lee A. Bygrave and Christopher Docksey (Eds.), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, Oxford, 2020, pp. 1–43.
- Lynskey, Orla, *The Foundations of EU Data Protection Law*, Oxford University Press, Oxford, 2015.
- Milanovic, Marko, “Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age”, *Harvard International Law Journal*, 56, 1, pp. 81–146.
- Милеуснић, Дамјан, Ћурчић, Данило, Тасић, Дуња, Адамовић, Јелена, Калајџић, Кристина, Ковачевић, Милош, Павловић, Михаило, Ницовић, Нина, Мишљеновић, Урош, *Приватност и заштита података о личности у Србији: Анализа одабраних секторских прописа и њихове примене*, Партнери за демократске промене Србија, Београд, 2021.
- Míšek, Jakub, “Data protection as performance-based regulation”, Eleni Kosta, Ronald Leenes, and Irene Kamara (eds.), *Research Handbook on EU Data Protection Law*, Edward Elgar Publishing, Cheltenham, 2022, pp. 50–67.
- Петровић, Драгана, „Сајбер безбедност vs. приватност – општа разматрања и основи заштите“, *Европско законодавство*, Година XXII, бр. 84, октобар–децембар 2023, стр. 177–192.
- Schwartz, Paul M., “Global Data Privacy: The EU Way”, *NYU Law Review*, 94, 4, pp. 771–851.
- Terwangne, Cécile de, “Article 5. Principles relating to processing of personal data”, Christopher Kuner, Lee A. Bygrave and Christopher Docksey (Eds.), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, Oxford, 2020, pp. 301–321.
- Tzanou, Maria, *The Fundamental Right to Data Protection*, Hart Publishing, Oxford, 2017.
- Voigt, Paul, Bussche, Axel von dem, *The EU General Data Protection Regulation (GDPR): A Practical Guide*, Springer, Berlin, 2017.

• Wachter, Sandra, Mittelstadt, Brent, Floridi, Luciano, "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation", *International Data Privacy Law*, 7, 2, pp. 76–99.

7) ЗНАЧАЈ ЗА РЕПУБЛИКУ СРБИЈУ

Анализа нормативне паралеле заштите личних података у ЕУ и Републици Србији показује да је наша земља прешла импресиван пут од иницијалне регулативе до готово потпуне правне асимилације са европским стандардима. Несумњиво, хармонизација права је непрекидан процес, а не једнократан чин.[68] Усвајањем ЗЗПЛ-а домаћи правни поредак је инкорпорирао решења из GDPR-а, чиме је формалноправно обезбеђен висок ниво заштите фундаменталних права грађана у дигиталној сфери. Дакле, Република Србија је успешно извршила нормативно усклађивање, преузимајући не само каталог права лица и начела обраде, већ и сложене концепте попут одговорности и заштите података по дизајну.[69] Ова паралела омогућава српским субјектима да функционишу унутар глобалних ланаца вредности користећи исти правни речник као и њихови партнери из ЕУ. Ипак, наше истраживање је указало и на одређене тачке дисконтинуитета које су првенствено институционалне и процедуралне природе. Главни изазов више није у самом тексту закона, већ у његовој ефективној примени.[70] Док надзорна тела ЕУ располажу директним казненим овлашћењима која служе као снажан превентивни механизам, Повереник у Републици Србији се и даље ослања на посредне прекршајне поступке, што у одређеној мери слаби одвраћајући ефекат прописа. Такође, одсуство наше државе из формалних механизама сарадње унутар EDPB ствара изолованост која се може превазићи тек пуноправним чланством или добијањем Одлуке о адекватности. Ово је кључно јер механизам преноса података у треће земље захтева усклађеност са стандардима који обезбеђују ниво заштите суштински еквивалентан оном у ЕУ.[71] Напослетку, јасан и предвидив правни оквир у овој области представља неопходан предуслов за стране инвестиције и дигитални развој привреде.[72]

[68] *Ibid*., стр. 345.

[69] Данило Кривокапић *et al*., *Водич кроз Закон о заштити података о личности и GDPR: тумачење новог правног оквира*, *op. cit.*, стр. 45–52.

[70] Андреј Дилигенски *et al*., *Право заштите података – GDPR*, *op. cit.*, стр. 345.

[71] Стефан Андоновић и Драган Прља, *Основи права заштите података о личности*, *op. cit.*, стр. 147–152.

Будућност заштите података о личности у Републици Србији нераскидиво је везана за даљу демократизацију и јачање владавине права. Технолошки трендови, попут вештачке интелигенције и масовне обраде података, захтеваће да се нормативна паралела непрестано ажурира кроз праксу и подзаконске акте. Кључни тест за нашу земљу биће балансирање између потреба државне безбедности и неприкосновености приватног живота грађана, што је стандард од којег ЕУ неће одступати. Можемо закључити да је Република Србија изградила модеран и чврст нормативни оквир који је компатибилан са европским. Међутим, да би те паралеле постале потпуно подударне у реалном животу, неопходно је континуирано јачање свести руковалаца, пуна независност надзорног тела и доследна судска пракса. Тек тада ће заштита података о личности у Републици Србији престати да буде само законска обавеза и постати интегрални део дигиталног идентитета и поверења на којем почива савремено друштво.

NORMATIVE PARALLELS OF PERSONAL DATA PROTECTION IN THE EUROPEAN UNION AND IN THE REPUBLIC OF SERBIA

Sergej ULJANOV*

Abstract: In the era of the fourth industrial revolution, personal data has become the most valuable resource of the digital economy, yet also the most vulnerable point for individual privacy. Mass collection, algorithmic processing, and global information flows have necessitated a robust and uniform legal framework to address challenges unforeseen by traditional law. This paper analyses the degree of compliance and key normative parallels between the legal frameworks for personal data protection in the European Union and the Republic of Serbia. The central subject of the research is the relationship between the General Data Protection Regulation (GDPR) and the domestic Law on Personal Data Protection (LPDP) of 2018. The author proceeds from the thesis that the Republic of Serbia, within the European integration process, has carried out extensive harmonisation of its regulations, adopting the basic concepts, processing principles, and data subject rights from the European model. The first part of

[72] *Ibid.,* стр. 205–207.

* Faculty of Business Studies and Law, Union – Nikola Tesla University, Belgrade. E-mail: sergej.uljanov@fpsp.edu.rs. ORCID iD: https://orcid.org/0000-0003-1739-0335

the paper examines the evolutionary processes that led to the adoption of current regulations. The central part provides a comparative analysis of institutes, such as processing principles, legal bases, and the role of supervisory authorities. Special emphasis is placed on the institutional framework, comparing the powers of the Commissioner for Information of Public Importance and Personal Data Protection in the Republic of Serbia with those of supervisory authorities in EU member states, while noting significant differences in penal policy and enforcement mechanisms. The final segment of the paper is dedicated to the challenges of cross-border data transfer and Serbia's prospects for obtaining an Adequacy Decision from the European Commission. Concluding remarks indicate that, despite a high rate of normative alignment, practical application and ensuring the full effectiveness of rights in the Republic of Serbia still face challenges due to specific socio-legal circumstances and administrative capacities.

Keywords: personal data protection, General Data Protection Regulation (GDPR), Law on Personal Data Protection (LPDP), Commissioner for Information of Public Importance and Personal Data Protection, harmonisation of law.