УНИВЕРЗИТЕТ У НИШУ

ПРАВНИ ФАКУЛТЕТ

Право на приватност детета у дигиталном простору

(мастер рад)

Менторка
Проф. др Анђелија Тасић

Студенткиња
Душица Лазић
Број индекса: М004/24-О

Ниш, 2026.

Садржај

1. УВОД 1

2. ПРАВО ДЕТЕТА НА ПРИВАТНОСТ – ПОЈАМ, ПРАВНА ПРИРОДА И МЕЂУНАРОДНИ ОКВИР 3

2.1. Појам и правна природа права на приватност 3

2.2. Специфичност права детета на приватност 5

2.3. Право детета на приватност у Конвенцији о правима детета 8

2.4. Најбољи интерес детета и аутономија у остваривању права детета 9

3. ПРАВО ДЕТЕТА НА ПРИВАТНОСТ У ДИГИТАЛНОМ ПРОСТОРУ 12

3.1. Обрада података о деци у дигиталном простору 13

3.2. Друштвене мреже, шерентинг и дигитални идентитет детета 17

3.3. Дигитално насиље и злоупотреба података детета 22

3.4. Профилисање и други савремени изазови заштите приватности детета 26

4. ПРАВНА ЗАШТИТА ДЕЦЕ У РЕПУБЛИЦИ СРБИЈИ И ДРЖАВАМА БИВШЕ ЈУГОСЛАВИЈЕ 30

4.1. Правни оквир Републике Србије 30

4.1.1. Уставноправни оквир 30

4.1.2. Закон о заштити података о личности 31

4.1.3. Породичноправна заштита приватности детета 35

4.1.4. Кривичноправна заштита приватности детета 37

4.1.5. Пракса заштите права на приватност детета у Републици Србији 39

4.2. Правни оквир држава бивше Југославије 49

4.2.1. Република Словенија 49

4.2.2. Република Хрватска 50

4.2.3. Босна и Херцеговина 52

4.2.4. Република Црна Гора 53

4.2.5. Република Северна Македонија 55

4.3. Упоредноправна анализа 57
5. ЕВРОПСКИ СТАНДАРДИ ЗАШТИТЕ ПРАВА ДЕТЕТА НА ПРИВАТНОСТ 59
5.1. Заштита права детета на приватност у праву Европске уније 59
5.1.1. Општи правни оквир Европске уније 59
5.1.2. Заштита деце у дигиталном окружењу 60
5.1.3. Заштита личних података деце према ГДПР-у 63
5.2. Заштита права детета на приватност према стандардима Савета Европе 65
5.3. Право детета на приватност у пракси Европског суда за људска права 67
6. УПОРЕДНА АНАЛИЗА И МОГУЋИ ПРАВЦИ ЗАШТИТЕ 72
6.1. Заједнички стандарди и положај Републике Србије 72
6.2. Структурне празнине заштите 75
6.3. Могући правци заштите 77
6.4. Могући правци унапређења за Републику Србију 81
7. ЗАКЉУЧНА РАЗМАТРАЊА 83
8. ЛИТЕРАТУРА 87
8.1. Попис коришћене литературе 87
8.2. Остала истраживачка грађа 90
9. САЖЕТАК И КЉУЧНЕ РЕЧИ 96
10. ABSTRACT AND KEY WORDS 97
11. БИОГРАФИЈА АУТОРКЕ 98

1. УВОД

Право на приватност представља једно од основних људских права и важан елемент заштите личности у савременом правном поретку. Развој информационо-комуникационих технологија, масовна употреба интернета и све већа присутност појединаца у дигиталном окружењу довели су до значајних промена у начину остваривања и заштите овог права. Иако су дигиталне технологије омогућиле бржи приступ информацијама, лакшу комуникацију и нове облике учешћа у друштвеном животу, истовремено су створиле и бројне ризике по приватност појединаца, нарочито деце као посебно осетљиве категорије лица.

Деца данас одрастају у окружењу које је у значајној мери обликовано дигиталним технологијама. Интернет, друштвене мреже, мобилне апликације и различите дигиталне платформе постали су саставни део њиховог свакодневног живота, образовања и социјализације. Међутим, лакоћа којом деца користе савремене дигиталне уређаје не значи истовремено и да су у стању да разумеју сложене механизме прикупљања, обраде и комерцијалног коришћења њихових личних података. Истраживања указују да деца често не разумеју у потпуности значај заштите сопствених података, последица објављивања личних информација или ризика који постоје у дигиталном простору,[1] због чега савремени правни системи препознају потребу за посебним облицима заштите приватности деце, заснованим на начелу најбољег интереса детета.

Предмет овог рада је право детета на приватност у дигиталном простору, са посебним освртом на правне механизме заштите приватности и личних података деце у условима све интензивније употребе дигиталних технологија и друштвених мрежа. Истраживањем ће бити обухваћена питања заштите личних података детета, стварања и заштите његовог дигиталног идентитета, обраде података од стране дигиталних платформи, као и однос права детета на приватност према правима и одговорностима родитеља. Посебна пажња биће посвећена остваривању равнотеже између потребе за заштитом детета и развоја његове аутономије у дигиталном простору, с обзиром на његов узраст, степен зрелости и способност да учествује у доношењу одлука које се односе на његову приватност и личне податке.

Полазећи од наведеног, циљ овог рада јесте да се испита у којој мери постојећи међународни, европски, упоредноправни и национални правни механизми обезбеђују ефикасну заштиту права детета на приватност у дигиталном простору, као и да се

[1] M. Stoilova, S. Livingstone, R. Nandagiri, *Digital by Default: Children's Capacity to Understand and Manage Online Data and Privacy*, Media and Communication, Vol. 8, No. 4, 2020, стр. 199.

идентификују постојећи проблеми и могући правци унапређења правне заштите, уз настојање да се допринесе даљем развоју правне теорије и праксе у овој области.

Значај истраживања огледа се у чињеници да интензивна дигитализација свакодневног живота суштински утиче на остваривање права детета и ствара нове изазове за заштиту његове приватности. Деца све раније користе дигиталне платформе и друштвене мреже, док се њихови лични подаци прикупљају, обрађују и користе у различите сврхе. Истовремено, дигитални траг настао током детињства може имати дугорочне последице на приватност, достојанство, идентитет и аутономију детета, укључујући и период адолесценције и одрасло доба.

Посебан проблем представља чињеница да заштита приватности детета у дигиталном простору укључује више међусобно повезаних интереса и субјеката, међу којима су дете, родитељи, држава и приватни субјекти, нарочито пружаоци дигиталних услуга и интернет платформи. Полази се од претпоставке да постојећи правни механизми, иако препознају право детета на приватност и заштиту личних података, не обезбеђују у потпуности ефикасну заштиту овог права, будући да нису у довољној мери прилагођени специфичним ризицима и изазовима савременог дигиталног окружења. Због тога се намеће потреба да се испита у којој мери постојећи правни оквир одговара специфичностима дигиталног окружења и обезбеђује адекватан ниво заштите детета.

У складу са предметом и циљем истраживања, полази се од следећих хипотеза:

I Постојећи међународни, европски и национални правни оквири препознају право детета на приватност у дигиталном простору, али постојећи механизми заштите не обезбеђују у потпуности ефикасну заштиту овог права.

II Ефикасна заштита приватности детета у дигиталном простору захтева успостављање одговарајуће равнотеже између права и одговорности родитеља и права детета на развој сопствене аутономије и одлучивање о питањима која се односе на његову приватност и личне податке, у складу са узрастом и степеном зрелости детета.

III Постојећи правни оквир Републике Србије не обезбеђује адекватан ниво заштите права детета на приватност у дигиталном простору, будући да није у довољној мери прилагођен специфичним ризицима и изазовима савременог дигиталног окружења.

IV Стандарди развијени у праву Европске уније, стандардима Савета Европе и релевантној пракси Европског суда за људска права могу представљати значајан основ за процену и унапређење правног оквира Републике Србије.

V Ефикасна заштита права детета у дигиталном простору захтева јасно дефинисане обавезе и одговорности не само родитеља и државе, већ и пружалаца дигиталних услуга и платформи које прикупљају и обрађују податке деце.

Приликом обраде теме примењени су нормативно-догматски метод, ради анализе релевантних одредаба међународних извора, права Европске уније и Савета Европе, правних система држава бивше Југославије и домаћег законодавства, као и компаративно-правни метод, ради сагледавања сличности и разлика између наведених правних оквира. Анализом садржаја биће испитани релевантни стандарди, док ће методом анализе судске праксе бити испитане одлуке Европског суда за људска права. Телеолошки метод биће коришћен ради утврђивања сврхе и циљева правне заштите детета у дигиталном простору.

Полазећи од наведеног, у раду ће најпре бити анализирани појам, правна природа и међународни оквир права детета на приватност, са посебним освртом на Конвенцију о правима детета, Општи коментар бр. 25 и однос најбољег интереса и аутономије детета. Затим ће бити обрађени специфични изазови и ризици по приватност детета у дигиталном простору, међу којима су обрада података на друштвеним мрежама, феномен шерентинга, дигитално насиље и профилисање. У даљем делу рада биће приказан правни оквир Републике Србије, уз компаративни осврт на правне системе држава насталих на простору бивше Југославије, а потом и европски стандарди заштите права детета на приватност, укључујући и праксу Европског суда за људска права. На основу спроведене упоредне анализе биће формулисани могући правци унапређења правне заштите.

2. ПРАВО ДЕТЕТА НА ПРИВАТНОСТ – ПОЈАМ, ПРАВНА ПРИРОДА И МЕЂУНАРОДНИ ОКВИР

2.1. Појам и правна природа права на приватност

Право на приватност представља једно од основних људских права и важан елемент заштите личности у савременом праву. Реч је о комплексном праву које обухвата широк спектар права, попут права на поштовање приватног и породичног живота, преписке, части и угледа.[2] Управо због сложености и вишедимензионалности овог права, као и чињенице да се његов садржај мењао упоредо са друштвеним и технолошким развојем,

[2]Н. Вучковић Шаховић, Н. Петрушић, *Права детета*, Правни факултет, Центар за публикације, Ниш, 2015, стр. 131.

у правној теорији не постоји јединствена и општеприхваћена дефиниција појма приватности, иако је реч о општеприхваћеној вредности која заслужује правну заштиту.

Генеза права на приватност у модерној правној теорији везује се за рад Ворена и Брандса, који су крајем деветнаестог века приватност дефинисали као „право да се буде остављен на миру“ (*the right to be let alone*).[3] Од првобитног схватања, усмереног превасходно на заштиту појединца од упада у његову физичку и породичну сферу живота, појам приватности се временом проширивао. Тако Вестин у свом делу *Privacy and Freedom* одређује приватност као право појединца да самостално одлучује када, у којој мери и под којим условима ће информације о њему бити доступне другима.[4] Развој информационо-комуникационих технологија додатно је проширио домет овог права. У литератури се стога разликују три међусобно повезана аспекта приватности: информациони, који обухвата контролу над информацијама о лицу, уз напомену да законитост обраде зависи од применљивог правног основа, а не искључиво од сагласности; одлучујући, који се односи на способност појединца да без туђих мешања доноси самосталне животне одлуке; и физички, који штити приватни простор и телесни интегритет.[5] У условима убрзаног развоја дигиталног друштва велике количине података о појединцима свакодневно се прикупљају, обрађују и чувају путем различитих информационих система, што повећава могућност њихове злоупотребе. Тиме је право на приватност доживело суштинску трансформацију из класичног „права да се буде остављен на миру“ у право на контролу над личним подацима који се налазе у дигиталном окружењу и над сопственим дигиталним траговима.[6]

Са становишта правне природе, право на приватност је основно људско право, гарантовано на нивоу Уједињених нација (чл. 12 Опште декларације о људским правима и чл. 17 Међународног пакта о грађанским и политичким правима), на нивоу Савета Европе (чл. 8 Европске конвенције за заштиту људских права и основних слобода и Конвенција 108+) и на нивоу Европске уније (чл. 7 и 8 Повеље о основним правима Европске уније).[7] У унутрашњем праву Републике Србије право на приватност

[3]S. D. Warren, L. D. Brandeis, *The Right to Privacy*, Harvard Law Review, Vol. 4, No. 5, 1890, стр. 193–220, DOI: 10.2307/1321160.
[4]A. F. Westin, *Privacy and Freedom*, New York, 1967, Atheneum, стр. 7.
[5]N. V. Kravchuk, *Privacy of a Child in the Digital Environment: New Risks Unaddressed*, Legal Issues in the Digital Age, Vol. 3, No. 2, 2022, стр. 79, DOI: 10.17323/2713-2749.2022.2.73.89.
[6]Ibid., стр. 80.
[7]Општа декларација о људским правима, Париз, 1948, чл. 12; Међународни пакт о грађанским и политичким правима, Њујорк, 1966, чл. 17; Конвенција за заштиту људских права и основних слобода, Рим, 1950, чл. 8; Савет Европе, Конвенција о заштити лица у односу на аутоматску обраду личних података, са Протоколом о изменама и допунама (Конвенција 108+), *Службени гласник Републике Србије – Међународни уговори, бр. 4/20*; Повеља о основним правима Европске уније, Ница, 2000, чл. 7 и 8.

није именовано као посебно уставно право, него се изводи из више уставних одредаба: чл. 23 (заштита људског достојанства и слободан развој личности), чл. 25 (заштита физичког и психичког интегритета), чл. 40 (неповредивост стана), чл. 41 (тајност писама) и чл. 42 (заштита података о личности).[8] Истовремено, право на приватност испољава се као субјективно грађанско право, које припада групи права личности, а неоснована задирања у њега штите се грађанскоправним, кривичноправним и специјализованим механизмима заштите података о личности. Право на приватност није апсолутно, већ се под одређеним условима може ограничити,[9] али само када је то предвиђено законом, када је ограничење оправдано у демократском друштву и када је пропорционално циљу, што следи из чл. 8 став 2 Европске конвенције за заштиту људских права и основних слобода.[10]

Посебан значај права на приватност као права личности огледа се у томе што његова повреда може имати дугорочне последице по психички развој, социјалне односе и лични интегритет појединца. Ово је нарочито изражено када су у питању деца, чији је развојни процес осетљивији и подложнији негативним утицајима насталим услед повреде приватности, због чега је право детета на приватност предмет посебне анализе у наставку овог поглавља.

2.2. Специфичност права детета на приватност

Иако право на приватност припада сваком лицу, његово остваривање код деце има одређену специфичност која произлази из њиховог узраста, степена зрелости и потребе за посебном заштитом. Дете је носилац свих основних људских права, укључујући и право на приватност, али истовремено представља лице чија способност самосталног доношења одлука није у потпуности развијена, због чега се заштита његове приватности заснива на равнотежи између аутономије детета и одговорности родитеља, старатеља и државе да штите његов најбољи интерес.

У дигиталном простору УНИЦЕФ (UNICEF) разликује четири димензије дечје приватности: физичку (нарушену праћењем, надзором или преносом уживо који открива дететов лик, активности или локацију), приватност комуникације (угрожену

[8]Устав Републике Србије *Службени гласник РС", бр. 98/2006*, чл. 23, 25, 40, 41 и 42.

[9]Када је реч о ограничењу права на приватност, ради се о посебном типу допуштених ограничења, којима се држава овлашћује да, по различитим основима, у општем друштвеном интересу ограничи вршење појединих права и слобода. Ова ограничења допуштена су тзв. рестриктивним клаузулама, које су најчешће наведене у посебним ставовима којима се неко право и слобода штите. Државама је допуштено да у општем друштвеном интересу ограниче вршење ових права, али не и да их суспендују (М. Пауновић, Б. Кривокапић, И. Крстић, *Међународна људска права*, Београд, 2018, Универзитет у Београду – Правни факултет, Центар за издаваштво и информисање, стр. 68).

[10]Конвенција за заштиту људских права и основних слобода, Рим, 1950, чл. 8 став 2.

приступом порукама и разговорима од стране нежељених прималаца), информациону (повређену прикупљањем и обрадом података без разумевања или пристанка детета) и приватност доношења одлука (нарушену аутоматизованим одлучивањем које ограничава самостални развој детета).[11] Ова подела у основи се поклапа са поделом приватности на информациони, одлучујући и физички аспект, изложеном у претходном одељку, уз једну битну разлику: УНИЦЕФ приватност комуникације издваја као самосталну димензију, будући да је у дигиталном окружењу тајност преписке и разговора престала да буде само извод из физичке приватности и стекла самостални значај.

Савремено схватање података о личности детета превазилази оно што дете свесно открива, јер обухвата и податке изведене из његових дигиталних активности, као и податке које о њему, често без његовог непосредног учешћа, објављују родитељи, чланови породице, пријатељи и друга лица. Пошто деца често нису у стању да у потпуности разумеју последице таквог откривања података, изложена су већем ризику од манипулације, злоупотребе и профилисања, а трајан дигитални траг настао на овај начин може остати доступан и након што дете достигне пунолетство. Због тога савремено право детета на приватност обухвата не само заштиту од неовлашћеног откривања података, већ и право на контролу над сопственим дигиталним идентитетом, што захтева правне механизме прилагођене рањивости детета и његовом најбољем интересу.

Питање дефинисања и заштите приватности предмет је сталне научне расправе. Мулиган, Купман и Доти описују приватност као по природи споран појам, о коме се стално расправља и који се брани кроз супротстављене ставове.[12] Те расправе нарочито су актуелне у контексту дигиталног окружења[13] и, конкретније, приватности деце.[14] Развојни приступ у том смислу нуде Лауфер и Вулф, повезујући значај приватности са најранијим периодом детињства. Према њима, способност детета да управља

[11]UNICEF, *Children's Online Privacy and Freedom of Expression: Industry Toolkit*, UNICEF, New York, 2018, стр. 8, преузето 15.9.2026, доступно на: https://www.unicef.org/childrightsandbusiness/reports/childrens-online-privacy-and-freedom-expression.

[12]D. K. Mulligan, C. Koopman, N. Doty, *Privacy is an Essentially Contested Concept: A Multi-Dimensional Analytic for Mapping Privacy*, Philosophical Transactions of the Royal Society A, Vol. 374, No. 2083, 2016, стр. 3, DOI: 10.1098/rsta.2016.0118.

[13]K. Sarikakis, L. M. Winter, *Social Media Users' Legal Consciousness About Privacy*, Social Media + Society, Vol. 3, No. 1, 2017, стр. 1, DOI: 10.1177/2056305117695325.

[14]B. Kidron, A. Evans, J. Afia, *Disrupted Childhood: The Cost of Persuasive Design*, London, 2018, 5Rights Foundation, преузето 15.9.2026, доступно на: https://5rightsframework.com/static/5Rights-Disrupted-Childhood.pdf.; S. Livingstone, *Children: A Special Case for Privacy?*, InterMedia, Vol. 46, No. 2, 2018, стр. 18, преузето 15.9.2026, доступно на: https://researchonline.lse.ac.uk/id/eprint/89706/.

информацијама о себи расте упоредо са способношћу да управља друштвеним интеракцијама, при чему постоји временски размак између спознаје да постоји могућност избора и стварне способности да се тај избор направи. Овај раскорак нарочито је значајан данас, када дигитално окружење деци пружа мало стварног избора или контроле и у великој мери заобилази родитеље.[15]

Пошто ни искључиво индивидуалистички, ни изразито контекстуалистички приступ нису практични за заштиту приватности деце у комерцијализованом дигиталном окружењу, Стоилова, Ливингстон и Нандагири предлажу класификацију која полази од Нисенбаумине концепције приватности као контекстуалног појма[16] и заснива се на три друштвене сфере: интерперсоналној (породица, вршњаци), институционалној (школа, здравствена служба) и комерцијалној (куповина, маркетинг, посредовање подацима),[17] као и на три врсте података: подацима које дете свесно даје, траговима података насталим ненамерно кроз дигиталне активности и изведеним подацима добијеним њиховом анализом (профилисање).[18] Улога података разликује се по сфери: у интерперсоналном контексту типични су подаци које дете свесно даје, а у институционалном се подаци редовно прикупљају, али их не анализирају увек,[19] док се у комерцијалном контексту највреднијим показују управо изведени и обједињени подаци, коришћени за циљано оглашавање у оквиру умрежене економије података.[20]

Регулаторне и образовне политике почивају на претпоставкама о томе шта деца могу да разумеју, због чега не постоји сагласност о узрасту на коме дете стиче способност да самостално одлучује о питањима дигиталне приватности. Питање приватности детета директно утиче и на питање старосних граница, о коме се у литератури и пракси расправља. Хајт препоручује да се са паметним телефонима сачека до средњошколског узраста (око 14 до 16 година), а са друштвеним мрежама до навршене 16. године живота, сматрајући млађу децу подложнијом негативним утицајима.[21] Насупрот томе,

[15]R. S. Laufer, M. Wolfe, *Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory*, Journal of Social Issues, Vol. 33, No. 3, 1977, стр. 22, DOI: 10.1111/j.1540-4560.1977.tb01880.x.
[16]H. Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford, 2010, Stanford University Press; наведено према: M. Stoilova, S. Livingstone, R. Nandagiri, op. cit., стр. 197.
[17]Ibid., стр. 197.
[18]Ibid., стр. 198.
[19]N. Selwyn, *What's the Problem with Learning Analytics?*, Journal of Learning Analytics, Vol. 6, No. 3, 2019, стр. 11–19, DOI: 10.18608/jla.2019.63.3; наведено према: M. Stoilova, S. Livingstone, R. Nandagiri, op. cit., стр. 199.
[20]D. Lupton, B. Williamson, *The Datafied Child: The Dataveillance of Children and Implications for Their Rights*, New Media & Society, Vol. 19, No. 5, 2017, стр. 780–794, DOI: 10.1177/1461444816686328; наведено према: M. Stoilova, S. Livingstone, R. Nandagiri, op. cit., стр. 199.
[21]J. Haidt, *The Anxious Generation: How the Great Rewiring of Childhood Is Causing an Epidemic of Mental Illness*, New York, 2024, Penguin Press; наведено према: M. Niestadt, op. cit., стр. 7.

Ливингстон и Силвандер сматрају да је тешко одредити јединствену старосну границу, будући да се зрелост разликује од детета до детета,[22] а и деца често наводе нетачне податке о свом узрасту.[23]

Сва деца уживају људска права која су самим рођењем гарантована сваком људском бићу,[24] али права детета представљају посебну категорију управо због његовог узраста, зрелости и осетљивости. Из наведеног се стога јасно издваја потреба за посебним правним приступом заштити приватности детета у дигиталном окружењу, чији међународни оквир се разматра у наставку.

2.3. Право детета на приватност у Конвенцији о правима детета

Право детета на приватност изричито је гарантовано чланом 16 Конвенције о правима детета (у даљем тексту КПД), према којем ниједно дете не сме бити изложено самовољном или незаконитом мешању у његову приватност, породицу, дом или преписку, нити незаконитим нападима на његову част и углед.[25] Иако је право на приватност било признато и раније, КПД га је изричито предвидела управо у чл. 16, а његов значај у дигиталном окружењу посебно је дошао до изражаја у последњој деценији.

Текст чл. 16 формулисан је технолошки неутрално, довољно широко да обухвати и физичко и дигитално окружење, али је његова примена на онлајн свет захтевала додатно тумачење. Из тог разлога Комитет Уједињених нација за права детета усвојио је 2021. године Општи коментар бр. 25 о правима детета у дигиталном окружењу.[26] Општи коментар није обавезујући документ, већ званично тумачење КПД-а од стране Комитета, којим се државама чланицама даје смерница како да примењују Конвенцију у дигиталном окружењу.

---

[22]О томе да је зрелост честа тема дискусија о детињству и деци наводе и Шаховић Вучковић и Петрушић у уџбенику *Права детета*. Наиме, ауторке наводе да је веома тешко дефинисати зрелост са психолошког, социолошког и правног становишта, због чега је срж појма развојних могућности деце у градацији, тј. увођење једне врсте постепености. Поштовање еволуције способности детета ставља у равнотежу права родитеља и деце и захтева висок ниво индивидуализације дечијих права и односа између детињства и одраслог доба. Разумевање и поштовање развојних способности детета од кључног је значаја за разумевање одредаба КПД, посебно одредаба које захтевају партиципацију деце (Н. Вучковић Шаховић, Н. Петрушић, *Права детета*, Ниш, 2015, Правни факултет, Центар за публикације, стр. 20).

[23]S. Livingstone, K. R. Sylwander, *There Is No Right Age! The Search for Age-Appropriate Ways to Support Children's Digital Lives and Rights*, Journal of Children and Media, Vol. 19, No. 1, 2025, стр. 6, DOI: 10.1080/17482798.2024.2435015.

[24]„Сва људска бића рађају се слободна и једнака у достојанству и правима.“ Општа декларација о људским правима, Париз, 1948. чл. 1.

[25]Чл. 16 Конвенције о правима детета, *Службени лист СФРЈ – Међународни уговори, бр. 15/90 и Службени лист СРЈ – Међународни уговори, бр. 4/96 и 2/97.*

[26]Комитет за права детета УН, Општи коментар бр. 25 (2021) о правима детета у вези са дигиталним окружењем, CRC/C/GC/25, 2. март 2021.

Комитет у Општем коментару бр. 25 истиче да је приватност од виталног значаја за дечију самосталност, достојанство и безбедност. Према ставу Комитета, претње приватности деце могу произаћи не само из прикупљања података и профилисања од стране јавних институција, предузећа и других организација, већ и из активности чланова породице, на пример када родитељи деле фотографије детета на интернету.[27] Комитет посебно указује на дигиталне праксе које се ослањају на обраду података, као што су профилисање, бихејвиорално циљање, обавезна идентификација и масовни надзор, а које могу представљати самовољно или незаконито мешање у право детета на приватност. [28] У том смислу, државе имају обавезу да усвоје и примењују законе о заштити података који садрже посебну заштиту за децу.[29]

Ипак, како уочава Кравчукова, мере развијане у циљу заштите приватности деце уоквирене су у парадигми подршке родитељима, без наглашавања њихове обавезе да не откривају информације о детету, а став Комитета у Општем коментару бр. 25 потврђује традиционалну перцепцију детета као објекта бриге под родитељском влашћу, уместо да је превазиђе.[30] Наиме, иако Комитет у односу са трећим лицима, попут јавних институција, предузећа и организација, изричито излаже мере које државе треба да предузму, у односу родитеља и детета остаје на констатовању да активности чланова породице могу угрозити приватност детета, не разрађујући конкретне мере у том контексту. Управо та празнина добија пуну тежину у односу родитеља и детета у пракси шерентинга, односно родитељског дељења података о детету на интернету, чија се правна анализа кроз одредабе КПД-а о приватности, учешћу детета и његовом најбољем интересу посебно разрађује у наставку овог рада.

2.4. Најбољи интерес детета и аутономија у остваривању права детета

Најбољи интерес детета, као једно од општих начела КПД-а, представља примарно разматрање у свим активностима које се тичу детета, укључујући и одлучивање о заштити његове приватности.[31] Међутим, у дигиталном окружењу ово начело само по себи не даје одговор на питање када и у којој мери дете може самостално да одлучује о својој приватности. Најбољи интерес није статичан стандард којим би родитељи или држава у име заштите одлучивали уместо детета, него оквир у коме се заштита права детета мора усклађивати упоредно са развојем способности детета да самостално

[27]Ibid., тач. 67.
[28]Ibid., тач. 68.
[29]Ibid., тач. 70.
[30]N. V. Kravchuk, op. cit., стр. 87.
[31]Чл. 3 КПД-а.

доноси одлуке које се односе на њега. Управо ту везу КПД успоставља кроз начело развојних способности, изложено у чл. 5.

Чл. 5 КПД-а обавезује државе потписнице да поштују одговорности, права и дужности родитеља да детету пружају одговарајуће усмеравање у остваривању права признатих Конвенцијом, на начин који је у складу са развојним способностима детета.[32] Ова одредба није неутрална према односу родитеља и детета: усмеравање се захтева, али то не значи да родитељи губе право да доносе одлуке у вези свог детета, с обзиром да су, у највећем броју случајева, управо они лица најближа детету, па сходно томе у позицији да процене шта је најбољи интерес детета. Родитељско право усмеравања постоји у функцији дететовог постепеног остваривања права, а не упоредо са њим. Тиме се признаје да се упоредно са узрастом и зрелошћу обим самосталног остваривања права постепено шири. Зато ни начин доношења одлука које се тичу дететове приватности не може бити исти за сву децу без обзира на године: иста одлука коју родитељ доноси у име детета млађег узраста, код старијег детета може представљати повреду његових права. Општи коментар бр. 25 у том смислу третира развојне способности као начело које детету постепено отвара простор за самостално остваривање права. Државе их морају признати при одлучивању о дигиталној приватности детета, а родитељско праћење дигиталних активности детета мора бити пропорционално и поштовати те способности.[33]

Из развојног начела следи и улога одраслих: они не штите приватност детета уместо детета, него га уче да је штити само. Према тач. 86 Општег коментара бр. 25, подршка родитељима и старатељима треба да им помогне да успоставе одговарајућу равнотежу између заштите детета и његове аутономије у развоју, засноване на узајамној емпатији и поштовању, а не на забрани или контроли, при чему су руководећа начела најбољи интерес детета и његове развојне способности.[34] Комитет истовремено опомиње да деца често прихватају и истражују дигиталне могућности у млађем узрасту него што родитељи очекују, и да су им понекад потребне већа подршка и охрабрење тамо где је одрасли приступ кажњавајући, претерано ограничавајући или неусклађен са њиховим развојним способностима.[35]

Очекивање да дете постепено преузима одговорност за своју приватност почива на претпоставци да дигитално окружење то учење омогућава. Деца могу имати користи од

[32]Чл. 5 КПД-а.
[33]Општи коментар бр. 25, op. cit., тач. 19, 20 и 76.
[34]Ibid., тач. 86.
[35]Ibid., тач. 85.

образовања у области дигиталне писмености, због чега је важно да развијају знања, вештине и способности, како би била сигурна у дигиталном окружењу, па чак и да критички разумеју начин функционисања умрежене економије података. Међутим, уколико дигитално окружење није осмишљено нити регулисано тако да буде разумљиво и да поштује права и најбоље интересе деце, оваква очекивања могу бити нереалистична.[36] Значај приватности за развој потврђују и развојне теорије, према којима је приватност неодвојива од процеса индивидуализације у детињству, будући да се дечје способности управљања информацијама заснивају на развоју способности управљања друштвеним интеракцијама.[37] Раскорак између спознаје да постоји избор и способности да се тај избор учини, указан у претходном одељку, овде добија правни значај: дете учи како да донесе одлуку о заштити приватности кроз стварне, подржане одлуке, а окружење „слепо на узраст“,[38] које нуди мало стварног избора и контроле, то учење отежава.

Из наведеног произлази да се право детета на приватност у дигиталном окружењу остварује сразмерно узрасту и зрелости, уз стално усклађивање заштите и аутономије, на основу развојних способности детета. Равнотежа коју захтевају начело најбољег интереса и начело развојних способности није једнократно решење, него процес сталног усклађивања по принципу да се равнотежа између заштите и аутономије усклађује сходно развојним способностима детета, уз очување обавезе заштите и све већег учешће детета у одлучивању. Међутим, она не престаје да буде обавеза родитеља и државе да учење како да дете донесе одлуке којима штити своју приватност учине могућим. Тај стандард постепености биће у наредним одељцима конкретизован кроз поједине аспекте дигиталног окружења, попут обраде података о деци, шерентинга и профилисања.

[36]D. Buckingham, *Defining Digital Literacy: What Do Young People Need to Know About Digital Media?*, Nordic Journal of Digital Literacy, Vol. 10, 2015, стр. 21–35; S. Culver, A. Grizzle, *Survey on Privacy in Media and Information Literacy with Youth Perspectives*, UNESCO, Paris, 2017; S. Livingstone, M. Stoilova, R. Nandagiri, *Data and Privacy Literacy: The Role of the School in Educating Children in a Datafied Society*, у: D. Frau-Meigs (ур.), Handbook on Media Education Research, London, 2020, Wiley Blackwell, стр. 413–425; J. Buitelaar, *Child's Best Interest and Informational Self-Determination: What the GDPR Can Learn from Children's Rights*, International Data Privacy Law, Vol. 8, No. 4, 2018, стр. 293–308; наведено према: M. Stoilova, S. Livingstone, R. Nandagiri, op. cit., стр. 198.

[37]R. S. Laufer, M. Wolfe, op. cit., стр. 22; наведено према: M. Stoilova, S. Livingstone, R. Nandagiri, op. cit., стр. 198.

[38]M. Stoilova, S. Livingstone, R. Nandagiri, op. cit., стр. 204–205.

3. ПРАВО ДЕТЕТА НА ПРИВАТНОСТ У ДИГИТАЛНОМ ПРОСТОРУ

Дигитално окружење данас је саставни део свакодневног живота деце и значајан простор у коме остварују своја права, посебно у областима образовања, информисања, комуникације и друштвеног учешћа. Међутим, све интензивнија употреба дигиталних технологија поред бројних бенефита доноси и нове облике ризика по остваривање и заштиту тих права. Посебан изазов представља заштита права на приватност, будући да коришћење дигиталних услуга све чешће подразумева прикупљање, обраду, чување, размену и друге облике употребе личних података деце, чега су деца мање или више свесна.

Како је изложено у другом поглављу, право детета на приватност изричито гарантује чл. 16 КПД-а, док је његова заштита у дигиталном окружењу конкретизована Општим коментаром бр. 25 Комитета за права детета УН. Комитет истиче да претње приватности деце могу произаћи не само из прикупљања података и профилисања од стране јавних институција, предузећа и других организација, већ и из активности чланова породице, на пример када родитељи деле фотографије детета на интернету,[39] при чему државе имају обавезу да усвоје и примењују законе о заштити података који садрже посебну заштиту за децу.[40] Тиме је на међународном нивоу означен правни оквир у коме ће у овом поглављу бити анализирани ризици по приватност детета у дигиталном простору.

Организација за економску сарадњу и развој (у даљем тексту: ОЕЦД) развила је у оквиру својих препорука о заштити деце на интернету типологију ризика којима деца могу бити изложена као корисници дигиталних технологија. Почетни оквир, садржан у Препоруци ОЕЦД-а о заштити деце на интернету из 2012. године и заснован на анализи ризика из 2011. године, обухватао је ризике повезане са садржајем, контактом и положајем деце као потрошача, као и ризике по информациону безбедност и приватност.[41] Технолошки напредак је, међутим, значајно изменио начин на који се лични подаци деце прикупљају, чувају, деле и користе, због чега је типологија из 2011. године ревидирана. Ревидирана типологија из 2021. године издваја ризике садржаја, понашања, контакта и потрошачке ризике, а приватност третира као ризик који прожима све наведене категорије.[42] Ова промена важна је за тему овог рада јер показује

[39]Комитет за права детета УН, Општи коментар бр. 25, op. cit., тач. 67.
[40]Ibid., тач. 70.
[41]OECD, *Children in the Digital Environment: Revised Typology of Risks*, OECD Digital Economy Papers, No. 302, Paris, 2021, OECD Publishing, стр. 4–5, DOI: 10.1787/9b8f222e-en.
[42]Ibid., стр. 6.

да се повреда приватности може јавити у различитим облицима дигиталне активности детета, а не само приликом објављивања личних података.

Значај овог проблема потврђују и налази компаративног истраживања *EU Kids Online* из 2026. године, спроведеног међу децом узраста од 10 до 16 година у 19 земаља, међу којима је и Србија. Половина испитане деце забринута је због коришћења својих података за персонализовано оглашавање, четворо од десеторо забринуто је због тога што компаније могу да деле њихове податке са трећим лицима без њихове сагласности, док 39% не верује да компаније безбедно чувају податке прикупљене о њима.[43]

Да би се проценила ефикасност постојећих механизама заштите права детета на приватност, најпре треба разумети ризике по приватност детета у дигиталном простору, о чему ће бити речи у наставку овог поглавља. Одељци који следе поређани су према носиоцу ризика: прво се анализира обрада података од стране пружалаца дигиталних услуга и дигиталних платформи (одељак 3.1), потом друштвене мреже, шерентинг и дигитални идентитет детета (одељак 3.2), затим дигитално насиље и злоупотреба података од стране трећих лица и вршњака (одељак 3.3), а на крају профилисање и други савремени изазови заштите приватности детета (одељак 3.4).

3.1. Обрада података о деци у дигиталном простору

Разумевање појма приватности, као и могућност деце да препознају значај заштите личних података, често су ограничени узрастом. Истовремено, све интензивније коришћење различитих дигиталних платформи, алата и услуга, укључујући и оне засноване на вештачкој интелигенцији, повећава њихову изложеност ризицима. Сматрамо да одговор на ове ризике не треба тражити у ограничавању приступа дигиталном простору, већ у развијању механизама који ће деци омогућити да предности дигиталног окружења користе на безбедан начин, уз одговарајућу заштиту њихових права. Међутим, да би се таква заштита могла обезбедити, неопходно је најпре разумети на који начин се подаци о деци прикупљају и обрађују у дигиталном простору, који су субјекти који у тим процесима учествују и који ризици за приватност детета из такве обраде могу проистећи.

[43] E. Staksrud, E. Helsper, S. Livingstone, B. Lobe, G. Mascheroni, M. Stoilova, K. Ólafsson, *The EU Kids Online 2026 comparative study: Children's views, experiences, opportunities and risks in a digital world*, University of Oslo and London School of Economics and Political Science, стр. 178; преузето 18.9.2026, DOI: https://doi.org/10.21953/researchonline.lse.ac.uk.00140901.

Деца данас представљају важан извор података на изузетно профитабилном тржишту података.[44] Њихове свакодневне, наизглед безазлене активности постају предмет опсежног прикупљања и претварања у дигиталне податке, што се означава појмом „датафикација“. Ова пракса доводи до тога да различити аспекти живота детета постају подложни утицају комерцијалних и политичких интереса на које оно најчешће не може да утиче. Имајући у виду најбољи интерес детета као кровни принцип заштите права детета, поставља се питање на који начин се могу заштитити интереси детета и његово право на самостално одлучивање о сопственим личним подацима.[45] Све наведено отвара важна питања у погледу заштите приватности деце.[46]

Дигиталне активности деце најчешће се одвијају на друштвеним мрежама и онлајн игрицама. Истраживања показују да је најчешћа онлајн активност деце комуникација са пријатељима путем друштвених мрежа и апликација за размену порука (78% свакодневно), потом следи гледање видео-садржаја на друштвеним мрежама (74%), док половина деце (50%) свакодневно игра онлајн игрице.[47] Приликом коришћења друштвених мрежа деца остављају различите личне податке: име, фотографије, податке о образовању, интересовањима и активностима на интернету. Поред информација које корисници добровољно објављују, платформе прикупљају и податке о локацији, претрагама, контактима и навикама коришћења услуга. Посебан проблем представља чињеница да деца често нису у потпуности свесна обима података које откривају нити начина на који се ти подаци користе. Иако већина друштвених мрежа у својим условима коришћења дозвољава отварање профила тек са навршених 13 година, истраживања показују да их користи и много млађа деца. Истраживање *Деца Европе на интернету* показало је да 86% деце узраста 9–17 година у Србији користи интернет свакодневно, да интернету преко мобилног телефона свакодневно приступа 65% најмлађе деце узраста 9–10 година и чак 98% узраста 15–17 година, при чему 74% испитаника има профил на некој друштвеној мрежи или платформи за игрице, укључујући 41% деце узраста 9–10 и 72% узраста 11–12 година, дакле знатно испод узраста који платформе дозвољавају.[48]

---

[44]V. Barassi, *The Child as Datafied Citizen: Critical Questions on Data Justice in Family Life*; y: G. Mascheroni, C. Ponte, A. Jorge (yp.), *Digital Parenting: The Challenges for Families in the Digital Age*, Göteborg, 2018, Nordicom, стр. 169, преузето 18.9.2026, доступно на: https://research.gold.ac.uk/23737/.
[45]Ibid., стр.170 и 173.
[46]J. Buitelaar, наведено према: M. Stoilova, S. Livingstone, R. Nandagiri, op. cit., стр. 198.
[47]E. Staksrud и др., op. cit., стр. 14 и 53.
[48]D. Kuzmanović, Z. Pavlović, D. Popadić, T. Milošević, *Korišćenje interneta i digitalne tehnologije kod dece i mladih u Srbiji: Rezultati istraživanja Deca Evrope na internetu*, Београд, 2019, Institut za psihologiju Filozofskog fakulteta u Beogradu, стр. 24–25 и 76; преузето 30. 9. 2026, доступно на: https://www.lse.ac.uk/media-and-communications/assets/documents/research/eu-kids-online/participant-countries/serbia/EU-Kids-Online-ENG-2019.pdf.

Наведена граница од 13 година, притом, није законска, већ произлази из услова коришћења које сами пружаоци услуга постављају, док се чл. 8 Опште уредбе о заштити података (у даљем тексту ГДПР), у погледу услуга информационог друштва које се детету нуде непосредно, уколико је правни основ обраде сагласност, предвиђа праг од 16 година, уз могућност држава чланица да га законским путем снизе, али не испод 13 година.[49] Из те разлике следи и посебан проблем заштите, јер дете које платформу користи наводећи нетачан узраст, у пракси не остварује заштиту посебног режима сагласности из члана 8 ГДПР-а, док му остала права (информисање, приступ подацима, исправка и брисање, жалба надзорном органу) остају на располагању. Упоредни подаци потврђују озбиљност овог проблема у Србији. Међу децом узраста 9–11 година која свакодневно посећују друштвене мреже, Србија има највећи удео од свих обухваћених земаља (45%, наспрам 11% у Немачкој).[50] Притом, додатну пажњу привлачи и то што је забринутост поводом обраде података код деце у Србији, изгледа, мање изражена него у већем делу Европе. Наиме, истраживање из 2026. године показује да у Србији, као и на Малти и у Португалији, трећина деце сматра да је онлајн праћење њиховог понашања у сврху персонализованог оглашавања легитимно.[51]

У погледу тога како деца разумеју појам обраде података и шта мисле о томе, значајан увид пружа истраживање Ливингстон, Стоилове и Нандагиријеве, спроведено у Уједињеном Краљевству, методом фокус-група са 169 деце узраста од 11 до 16 година. У овом истраживању приватност је испитивана у три дигитална контекста: интерперсоналном (породица, вршњаци, заједница), институционалном (школа, здравствена служба) и комерцијалном (куповина, маркетинг, посредовање подацима).[52] Показало се да је међу институционалним контекстима школа деци најближа и најразумљивија, будући да деца знају да школа држи многе њихове податке, због чега ауторке управо кроз однос детета и школе показују како деца разумеју институционалну обраду података.

Ово истраживање указује на значајан раскорак између обима података које институције прикупљају и обрађују о деци и њиховог разумевања осетљивости тих података и могућих последица њихове (зло)употребе. Деца често не препознају

[49]Чл. 8 Уредбе (ЕУ) 2016/679 Европског парламента и Савета од 27. априла 2016. године о заштити физичких лица у вези са обрадом података о личности и о слободном кретању таквих података (Општа уредба о заштити података), Сл. лист ЕУ, L 119, 4.5.2016; преузето 28.8.2026., доступно на: https://eur-lex.europa.eu/eli/reg/2016/679/oj

[50]S. Livingstone и др. (ур.), *EU Kids Online 2020: Survey results from 19 countries*, London, 2020, EU Kids Online, стр. 50; преузето 30.9.2026, доступно на: https://doi.org/10.21953/lse.47fdeqj01ofo.

[51]E. Staksrud и др., op. cit., стр. 179.

[52]M. Stoilova, S. Livingstone, R. Nandagiri, op. cit., стр. 197.

здравствене и медицинске евиденције, податке о школском успеху и присуству настави, фотографије и друге информације којешкола прикупља као личне податке који могу имати значајне импликације по њихову приватност, а истовремено имају ограничено знање о томе на који начин школа користи њихове податке, да ли их прослеђује трећим лицима и на који начин их штити од неовлашћеног приступа.[53] Са друге стране, деца показују висок степен поверења у школу и углавном очекују да ће њихови подаци бити чувани безбедно и коришћени искључиво у сврху због које су прикупљени. Управо услед ограничених могућности деце да преиспитују и оспоравају одлуке које школа доноси у вези са њиховим подацима, такво поверење може постати проблематично, посебно када се схватање приватности изграђено у институционалном контексту некритички пренесе на комерцијално дигитално окружење, које функционише по посве другачијим принципима и чији су интереси често усмерени на даљу употребу и економско искоришћавање података. Због тога сматрамо да ови подаци указују на посебну одговорност школе да поверење деце не остане само на нивоу очекивања, већ да буде праћено јасним и узрасту прилагођеним информисањем о томе који се подаци прикупљају, у које сврхе се користе, на који начин се чувају и са ким могу бити подељени, чиме школа може значајно допринети развијању свести и критичног промишљања деце о вредности личних података и помоћи им у формирању одговорних дигиталних навика.

Ризици за приватност деце не настају искључиво у оквиру друштвених мрежа. Подаци о деци прикупљају се и кроз коришћење онлајн игрица, паметних играчака, апликација и видео-сајтова намењених деци, што ствара додатне могућности за прикупљање и коришћење њихових података.[54] Један од најзначајнијих ризика за приватност детета јесте трајност дигиталног трага: информације, фотографије и коментари објављени у дигиталном простору могу остати доступни дуги низ година и након што буду обрисани са првобитне платформе. Због тога се право детета на приватност све чешће повезује са правом на контролу сопственог дигиталног идентитета и могућношћу уклањања података који могу негативно утицати на његов будући живот, питањем које ће у правном делу рада бити ближе размотрено кроз право на брисање података (одељак 4.1.2).

Поред поменутих ризика који произлазе из начина рада самих платформи, опасност представља и неовлашћено дељење садржаја од стране других корисника, посебно јер

[53]Ibid., стр. 200–201.
[54]OECD, op. cit., стр. 15.

једном објављени подаци могу бити копирани, прослеђени или поново објављени без знања и сагласности детета, чиме дете губи контролу над њиховим даљим коришћењем.

Савремени правни системи стога настоје да успоставе равнотежу између права детета на учешће у дигиталном окружењу и његовог права на приватност. Заштита приватности при томе не подразумева само пристанак, већ и закониту, поштену и транспарентну обраду података, ограничавање количине прикупљених података, јасно одређену сврху обраде, одговарајуће рокове чувања и могућност брисања или исправке података,[55] а заштита деце на друштвеним мрежама данас представља један од најзначајнијих изазова савременог права детета, који захтева примену посебних правних и институционалних механизама.

3.2. Друштвене мреже, шерентинг и дигитални идентитет детета

Развој друштвених мрежа довео је до појаве нових облика угрожавања приватности деце који не потичу од државних органа или трећих лица, већ од самих родитеља. У правној литератури за ову појаву усталио се термин шерентинг (енгл. *sharenting*), настао спајањем енглеских речи *share*, што значи делити, и *parenting*, што значи родитељство. Овим појмом означава се пракса дељења вести, фотографија и видео-записа о сопственом детету на друштвеним мрежама или интернет страницама, при чему се у литератури посебан нагласак ставља на то да је такво дељење прекомерно или да су информације које родитељи деле, гледано са аспекта детета, срамотне.[56] Истраживање садржаја родитељских профила на друштвеној мрежи *Facebook* показало је да чак 90,5% анализираних профила садржи дететово име, а 83,9% и датум његовог рођења,[57] што показује колико се интензивно родитељи дигиталним путем упуштају у стварање трага који дете најчешће није бирало само. Међутим, специфичност шерентинга огледа се у томе што се ради о појави која се налази на самом пресеку два права: права родитеља на лични и породични живот, укључујући право да објављују информације из свог приватног живота, са једне стране, и права детета на приватност, са друге.[58]

---

[55]Чл. 5, 16 и 17 Уредбе (ЕУ) 2016/679 (Општа уредба о заштити података), op. cit.; Чл. 5 Закона о заштити података о личности, *Службени гласник РС*, бр. 87/2018.

[56]A.Tasić, Rizici „digitalnog“ djetinjstva: Sharenting u praksi Republike Srbije i Republike Hrvatske, Dijete i obitelj u suvremenom društvu, Vol. 3, No. 1, 2026, стр. 86, DOI: 10.25234/dosd/41302, преузето 2. 9. 2026, доступно на: https://hrcak.srce.hr/broj/26955.

[57]A. Brosch, When the Child is Born into the Internet: Sharenting as a Growing Trend among Parents on Facebook, The New Educational Review, Vol. 43, No. 1, 2016, стр. 230, DOI: 10.15804/tner.2016.43.1.19, преузето 5.9.2026., доступно на: https://czasopisma.marszalek.com.pl/images/pliki/tner/201601/tner20160119.pdf.

[58]A. Tasić, op. cit., стр. 86.

У литератури, међутим, не постоји јединствена дефиниција шерентинга. Лендаи, који је систематизовао бројне дефиниције овог појма, предлаже најширу од њих, према којој је шерентинг пракса у којој родитељи, бабе и деде, старатељи или чланови породице јавно деле информације, посебно писане, визуелне, аудио и аудио-визуелне садржаје и податке о личности, о деци, првенствено малолетним лицима, у дигиталном простору.[59] Предложена дефиниција, иако обухвата најшири круг субјеката, у овом раду није прихваћена. Специфичност шерентинга, која га и издваја као самостални правни проблем, управо је у односу између детета и родитеља. Сматрамо да је овде реч о колизији права родитеља на лични и породични живот, односно његовог права да објављује информације из сопственог живота, и права детета на приватност, а та колизија се на исти начин не поставља када податке о детету објављују лица која не врше родитељско право. Дељење информација о детету од стране других чланова породице, дакле, ни по чему није мање штетно по дете, али оно представља питање опште заштите приватности, а не питање граница родитељског права и родитељске бриге, а управо је то питање које шерентинг чини посебним феноменом. У прилог ужем разумевању иду и етимологија самог термина, која у основи има управо родитељство, као и дефиниција прихваћена у радовима који се овим питањем баве и у домаћој литератури.[60] Из тог разлога, у овом раду се под шерентингом подразумева пракса дељења података о детету од стране његових родитеља.

Родитељи данас, дељењем садржаја о свом детету, не обликују само сопствени дигитални идентитет, већ и дигитални идентитет своје деце, често много пре него што деца постану способна да разумеју и контролишу своје присуство у дигиталном простору. У литератури се управо зато шерентинг посматра као радња, дељење информација о детету, а дигитални идентитет детета као исход таквог понашања.[61] Блум-Рос и Ливингстон[62] указују на то да родитељи често почињу да блогују или објављују садржај због себе: да би изразили креативност, сачували део идентитета који није везан искључиво за родитељство или се изборили са осећајем изолације. Ипак, чак и када желе да пишу о сопственом искуству, родитељи готово неизбежно пишу и о

[59]G. F. Lendvai, *Sharenting as a Regulatory Paradox: A Comprehensive Overview of the Conceptualization and Regulation of Sharenting*, International Journal of Law, Policy and the Family, Vol. 38, No. 1, 2024, стр. 6, DOI: 10.1093/lawfam/ebae013.
[60]A. Tasić, op. cit., стр. 86.
[61]V. Berg, D. Arabiat, E. Mörelius, L. Kervin, M. Zgambo, S. Robinson, M. Jenkins, L. Whitehead, *Young Children and the Creation of a Digital Identity on Social Networking Sites: Scoping Review*, JMIR Pediatrics and Parenting, Vol. 7, No. 1, 2024, e54414, DOI: 10.2196/54414.
[62]A. Blum-Ross, S. Livingstone, *„Sharenting," Parent Blogging and the Boundaries of the Digital Self*, Popular Communication, Vol. 15, No. 2, 2017, стр. 110–125, DOI: 10.1080/15405702.2016.1223300.

својој деци, због чега је граница између „мог искуства“ и „дететовог живота“ врло тешко одржива, што представља парадокс уграђен у саму структуру родитељског објављивања садржаја о породичном животу.

Однос адолесцената према шерентингу зависи од објављеног садржаја: адолесценти га доживљавају као позитиван док су приказани у позитивном светлу и док су догађаји које родитељи деле приказани одобравајуће.[63] Показало се, међутим, да 47% родитеља корисника *Facebook*-а има своју децу међу „дигиталним пријатељима“ на тој мрежи,[64] што шерентинг чини посебно проблематичним управо у периоду адолесценције, осетљивом раздобљу у коме млади пролазе кроз емоционалну и социјалну транзицију, изграђују сопствени идентитет и постепено се осамостаљују од родитеља. У погледу заштите приватности у међуљудским односима, деца су свесна да немају потпуну контролу над сопственим подацима управо због феномена који се означава као „умрежена приватност“ (енгл. *networked privacy*): комуникације на интернету су по својој природи јавно доступне готово по аутоматизму, услед чега деца знају да би друга лица могла да деле информације о њима без њихове дозволе или изван првобитно предвиђене сврхе и публике.[65]

Шерентинг, међутим, нема искључиво негативну функцију. Путем друштвених мрежа родитељи размењују искуства, траже и пружају подршку и повезују се са родитељима у сличним животним околностима, чиме доприносе стварању заједница подршке, што је нарочито изражено код родитеља деце оболеле од ретких болести.[66] Због тога правна анализа шерентинга не би требало да полази од претпоставке да је свако објављивање садржаја о детету штетно, већ од потребе да се успостави равнотежа између легитимних интереса родитеља и права и интереса детета. Тај однос већ је назначен кроз однос чл. 16, чл. 12 и чл. 3 КПД-а, као и кроз напомену Општег коментара бр. 25 да претње приватности деце могу произаћи и из активности чланова породице,[67] а разрађен је у одељку 2.3 овог рада. У овом одељку он добија конкретну примену, јер је управо шерентинг пример у коме заштита детета не подразумева

[63]M. Walrave, K. Verswijvel, G. Ouvrein, L. Staes, L. Hallam, K. Hardies, *The Limits of Sharenting: Exploring Parents' and Adolescents' Sharenting Boundaries Through the Lens of Communication Privacy Management Theory*, Frontiers in Education, Vol. 7, 2022, 803393, DOI: 10.3389/feduc.2022.803393.
[64]M. Duggan, A. Lenhart, C. Lampe, N. B. Ellison, *Parents and Social Media*, Pew Research Center, Washington, 2015, стр. 9; преузето 9.9.2026., доступно на: https://www.pewresearch.org/internet/2015/07/16/parents-and-social-media/.
[65]A. E. Marwick, d. boyd, „Networked Privacy: How Teenagers Negotiate Context in Social Media", New Media & Society, Vol. 16, No. 7, 2014, стр. 1051–1067; наведено према: M. Stoilova, S. Livingstone, R. Nandagiri, op. cit., стр. 199.
[66]A. Tasić, op. cit., стр. 87.
[67]Комитет за права детета УН, Општи коментар бр. 25, op. cit., тач. 67.

оснаживање родитеља, већ успостављање одговарајућих обавеза према њима, што је у литератури означено као регулаторни парадокс шерентинга.[68]

У праву Републике Србије не постоји посебна регулатива посвећена шерентингу, те се заштита детета остварује применом општих правила о заштити података о личности, права на приватност и начела најбољег интереса детета. Известан допринос решавању овог питања у домаћој пракси дала је пресуда Врховног касационог суда Републике Србије Рев. 14012/2022 од 6. 10. 2022. године, којом је, у поступку за заштиту права детета, утврђено да објављивање фотографија детета на друштвеним мрежама може представљати опасну активност, те да, након што је родитељ коме је поверено вршење родитељског права изразио противљење објављивању фотографија на којима се лик детета може идентификовати, даље објављивање таквих фотографија није у складу са најбољим интересом детета, због чега је туженом забрањено да их убудуће објављује. Суд при томе није нашао да је раније објављивање, извршено пре израженог противљења, представљало повреду права детета на приватност, тако да је забрана ограничена на будуће објављивање, док већ објављени садржај остаје без судске реакције.[69] Детаљна анализа ове пресуде, укључујући и начине на које је суд применио стандард најбољег интереса детета, износи се у одељку 4.1.5, у оквиру разматрања институционалне праксе Републике Србије, па се овде на њу указује само као на први судски одговор на шерентинг у српском праву.

На регулаторном плану, поједине државе чланице Европске уније (у даљем тексту ЕУ) већ су увеле или предложиле измене закона како би поставиле границе родитељима који јавно деле информације о својој деци на интернету. Француска је у том погледу отишла најдаље, и то у два корака која успостављају заштиту детета путем механизма који право родитеља не укида, већ му поставља конкретне обавезе. Законом из 2020. године заштита малолетника проширена је на активност деце на друштвеним мрежама тако што су родитељи чија деца учествују у активностима која генеришу зараду, дужни да ту зараду уплаћују на рачун отворен на име детета, којима се, док дете не стекне пунолетство, односно еманципацију, управља у његовом интересу.[70] Ово решење је значајно управо зато што није одговор у облику забране; признато је да дељење садржаја са дететом, када прелази у комерцијално коришћење, дете доводи у положај

[68]G. F. Lendvai, *Sharenting as a Regulatory Paradox*, op. cit., стр. 9–10.
[69]Пресуда Врховног касационог суда Републике Србије, Рев. 14012/2022 од 6. 10. 2022. године.
[70]Loi n° 2020-1266 du 19 octobre 2020 visant à encadrer l'exploitation commerciale de l'image d'enfants de moins de seize ans sur les plateformes en ligne, преузето 15.9.2026., доступно на: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000042439054.

заслужног лица, па се заштита више не своди на приватност, већ обухвата и заштиту од економског искоришћавања, при чему су имовински ефекти такве активности осигурани на име будућег носиоца права, а родитељско право на објављивање остало је очувано.

Законом из 2024. године уређене су ситуације у којима се родитељи не слажу око објављивања садржаја на коме се појављује њихово дете, тако што је суду омогућено да, у случају неслагања родитеља о остваривању права детета на лик, забрани једном родитељу објављивање без сагласности другог, док у случају озбиљне повреде достојанства детета вршење права на лик може, под посебно утврђеним условима, бити поверено једном родитељу.[71] Значајно је, притом, да је истим законом чланом 372-1 Грађанског законика Француске уведена обавеза родитеља да дете укључују у остваривање права на лик сразмерно његовом узрасту и степену зрелости,[72] чиме је начело развојних способности детета, разматрано у одељку 2.4 овог рада, директно унето у регулацију шерентинга. Дете се приликом доношења одлуке о употреби сопственог лика третира као учесник, а не искључиво као објекат родитељске одлуке. Ово решење је, у контексту овог рада, посебно занимљиво због два елемента. Прво, оно неразумевање родитеља претвара у судски поступак у коме суд процењује угроженост достојанства детета, а не само вољу родитеља, чиме је стандард најбољег интереса детета издвојен од става родитеља коме је поверено вршење родитељског права, питање које се поставља и у српском праву, али на које је српска пракса тек одговорила у наведеној пресуди Врховног касационог суда (видети одељак 4.1.5). Друго, признањем права сваком од родитеља да тражи забрану, без обзира на то коме је поверено вршење родитељског права, француски законодавац је објављивање дететовог лика извео из искључиве воље родитеља коме је родитељско право поверено. У српском праву, насупрот томе, питање је остало на нивоу судског закључка у којем је заштита детета остварена управо на основу става родитеља коме је родитељско право поверено, а не кроз опште правило о заједничком одлучивању родитеља о објављивању. Италија, са друге стране, тек разматра сродна решења, па су у поступку предлози закона по којима би малолетницима било признато право на уклањање онлајн садржаја у коме се појављују, од навршених 14 година живота, а ако родитељи остварују профит од дељења слика своје деце, били би обавезни да зараду уплаћују на рачун отворен на име детета,

[71]Loi n° 2024-120 du 19 février 2024 visant à garantir le respect du droit à l'image des enfants, преузето 15.9.2026., доступно на: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000049163317
[72]G. F. Lendvai, *Sharenting as a Regulatory Paradox*, op. cit., стр. 14.

којим би оно могло располагати након што постане пунолетно.[73] Упоређивање француског и италијанског приступа, притом, показује и разлику у одабиру момента ослобађања средстава (навршених 16, односно 18 година живота), као и прелазак од приватног дељења ка комерцијалном искоришћавању дететовог лика, у коме се питање приватности детета спаја са питањем његове заштите од економског искоришћавања.

Најновија научна литература потврђује да регулаторни одговори на феномен шерентинга остају фрагментарни и недовољно уједначени, упркос томе што се правна и јавнополитички усмерена литература већ дуже време бави овим феноменом кроз призму приватности, достојанства, најбољег интереса детета и дигиталних права.[74] Истраживање посвећено региону централне и источне Европе показује, у оквиру прегледа држава централне и источне Европе, да је Француска у посматраном кругу држава једина која је донела посебне прописе о шерентингу, док све остале остају при постојећим општим оквирима, који нису довољни за обраду специфичности овог феномена.[75] Управо је та фрагментарност кључни проблем: правна заштита деце од шерентинга нормативно постоји, али се у пракси Републике Србије остварује посредно, кроз постојеће институте породичног, прекршајног и медијског права, без јединственог правног приступа овом феномену. Овај проблем биће разматран у наредним деловима рада, а на основу њега ће се у закључним разматрањима формулисати и предлози за унапређење правне заштите.

3.3. Дигитално насиље и злоупотреба података детета

Право детета на приватност у дигиталном простору угрожено је не само обрадом података од стране интернет платформи или објављивањем садржаја од стране родитеља, већ и различитим облицима дигиталног насиља. Употреба информационо-комуникационих технологија омогућила је нове облике повреде приватности, чије последице могу бити теже од традиционалних облика вршњачког насиља, управо због брзине ширења информација и њихове трајне доступности на интернету. Дигитално насиље (сајбер-насиље) представља намерно и поновљено наношење штете другој

[73]M. Niestadt, *Protecting Children Online: Selected EU, National and Regional Laws and Initiatives*, EPRS, Brussels, 2025, стр.9, 9.9.2026.,доступно на: https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769570/EPRS_BRI(2025)769570_EN.pdf.

[74]O. Akay, *Children's Privacy, Autonomy, and Digital Identity in Sharenting Research: A Scoping Review with Bibliometric Mapping*, Frontiers in Psychology, Vol. 17, 2026, 1845715, преузето 8. 9. 2026, DOI: 10.3389/fpsyg.2026.1845715.

[75]G. F. Lendvai, K. Ambrazevičiūtė, *Parenting in the Digital Age: Addressing the Sharenting Phenomenon in Central and Eastern Europe*; y: Children's Rights in Central and Eastern Europe: A Comparative Analysis with a Spotlight on Lithuania, Cham, 2025, Springer, стр. 349–364, DOI: 10.1007/978-3-032-07092-0_17, преузето 8.9.2026., доступно на: https://link.springer.com/chapter/10.1007/978-3-032-07092-0_17.

особи коришћењем дигиталне технологије, пре свега интернета и мобилних телефона, чиме се она узнемирава, повређује или понижава.[76] Истраживања о дигиталном насиљу истичу да оно поседује одлике које се у традиционалном насиљу лицем у лице не срећу на исти начин, попут могуће анонимности учиниоца, потенцијално неограничене публике, трајности материјала и могућности да жртва буде погођена готово у сваком тренутку. Истраживања такође показују да је насиље чешће резултат интеракције истих вршњака у оба окружења, онлајн и офлајн, тако да се улоге жртве и учиниоца могу мењати и преклапати.[77]

Према налазима истраживања *EU Kids Online* из 2026. године, 39% деце узраста од 10 до 16 година изјавило је да је у току претходне године неко према њима поступао на повређујући или непријатан начин, при чему је такво поступање онлајн пријавило 17% деце, наспрам 29% које је пријавило исто такво поступање лицем у лице. Дигитална окружења су, дакле, постала важан додатни простор таквог понашања, али ван мреже поступање остаје чешће, тако да једно не замењује друго.[78]

Садржај који подстиче мржњу може имати облик слика, речи, видео-записа, игара, симбола, па чак и песама, а може бити мотивисан вером, расом, родом, инвалидитетом, сексуалном оријентацијом или родним идентитетом жртве, или чак наизглед безазленим личним карактеристикама попут акцента, познавања језика, изгледа, хобија или музичког укуса. Изложеност оваквом садржају значајно је порасла у периоду од 2010. до 2019. године: док је 2010. године само 12% деце узраста 11–16 година у Уједињеном Краљевству пријавило изложеност садржају који подстиче мржњу на интернету, до 2019. године то је пријавила половина деце узраста 12–15 година.[79] Налази истраживања *EU Kids Online* из 2026. године показују да је изложеност порукама мржње и даље раширена:30% деце изјавило је да такве поруке види најмање једном месечно, при чему је у Републици Србији забележен највиши удео од свих деветнаест обухваћених земаља (40%).[80]

Одсуство сагласности међу креаторима јавних политика и истраживачима о томе шта тачно представља дигитално насиље довело је до тога да државе овај проблем регулишу на различите начине, у многим случајевима применом мера кривичноправне природе. Међутим, када су учиниоци деца, кривичноправни одговор може бити

[76]S. Hinduja, J. W. Patchin, *Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying*, Thousand Oaks, 2009, Corwin Press, стр. 5.
[77]E. Staksrud и др., op. cit., стр. 109.
[78]Ibid., стр. 111 и 113.
[79]OECD, op. cit., стр. 7–8.
[80]E. Staksrud и др., op. cit., стр. 130.

контроверзан и несразмеран, јер може довести до криминализације деце која нису свесна последица сопствених поступака.[81]

Посебан облик ризичног понашања представља размена сексуално експлицитних порука и садржаја (тзв. *sexting*). Иако се интуитивно чини да ризик постоји само када се такав садржај дели без пристанка приказане особе, у случајевима у којима малолетници учествују у оваквој размени (чак и уз међусобну сагласност) постоји ризик да сами произведу материјал који по правној квалификацији може представљати материјал сексуалног злостављања деце, а који се потом може брзо и трајно проширити дигиталним окружењем. Овакво понашање, стога, не угрожава само приватност, здравље и добробит детета, већ носи и значајан ризик да само дете буде кривично гоњено због „самосталног стварања" материјала који га приказује на порнографски начин.[82]

У циљу боље заштите деце од вршњачког и дигиталног насиља, државе чланице ЕУ у своје законодавство уводе измене које олакшавају пријављивање и спречавање оваквих случајева, при чему се мере против дигиталног насиља често примењују заједно са мерама против вршњачког насиља, будући да се ова два облика насиља неретко јављају истовремено.[83] С обзиром на то да поједине државе различито дефинишу појам вршњачког, односно дигиталног насиља у свом националном законодавству, упоређивање статистичких показатеља између држава чланица знатно је отежано. Француска, на пример, у свом измењеном Закону о образовању (*Code de l'éducation*, 2022) насиље дефинише кроз понашање или коментаре, учињене у образовној установи или ван ње, чији је циљ или последица нарушавање достојанства ученика, односно угрожавање његовог физичког или менталног здравља или услова образовања.[84] Италијански закон из маја 2024. године (Закон бр. 70/2024), насупрот томе, појам дигиталног насиља дефинише знатно шире од појма узнемиравања из француског образовног законодавства, обухватајући, поред узнемиравања, и притисак, агресију, уцену, вређање, омаловажавање, клевету, крађу идентитета и незаконито прибављивање или обраду личних података малолетника учињене електронским путем, укључујући и ширење онлајн садржаја о члановима породице малолетника чија је намерна и претежна сврха изолација малолетника путем озбиљног злостављања,

[81]OECD, op. cit., стр. 9.
[82]Ibid., стр. 9–10.
[83]M. Niestadt, op. cit., стр. 8.
[84]Чл. L. 111-6 Loi n° 2022-299 du 2 mars 2022 visant à combattre le harcèlement scolaire, чланом 1. уведен Code de l'éducation; преузето 20. 10. 2026, доступно на: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000045289043.

штетног напада или исмевања.[85] И у Србији је законодавац, у области образовања, прописао дефиницију дигиталног насиља. Чланом 111 ст. 10 Закона о основама система образовања и васпитања дигитално насиље и злостављање дефинисани су као злоупотреба информационо-комуникационих технологија која може да има за последицу повреду друге личности и угрожавање достојанства, а остварује се слањем порука електронском поштом, смс и ммс порукама, путем веб-сајта, четовањем, укључивањем у форуме, социјалне мреже и другим облицима дигиталне комуникације.[86]

Поједине државе предузеле су и мере усмерене на олакшавање пријављивања дигиталног насиља. Француска, на пример, обавезује платформе друштвених мрежа да објављују поруке којима позивају на борбу против дигиталног насиља и обезбеде телефонски број за пријаву насиља и незаконитог садржаја, при чему су, у хитним случајевима који укључују непосредну и озбиљну претњу по одређену особу, платформе дужне да одговоре на правне захтеве најкасније у року од осам сати.[87] У Србији је изменама Закона о основама система образовања и васпитања из 2023. године предвиђено да се пријаве у вези са насиљем, злостављањем и занемаривањем ученика примају путем Националне платформе за превенцију насиља која укључује децу „Чувам те". Пријава се подноси попуњавањем формулара на платформи, уз могућност да подносилац пријаве прати поступање надлежних институција по својој пријави.[88]

Дигитално насиље није једини начин на који трећа лица угрожавају приватност детета. Посебан ризик представља и злоупотреба личних података деце, која у дигиталном окружењу може довести до крађе њиховог идентитета. Повезивањем различитих података, прикупљених током дечијег коришћења дигиталних услуга, могуће је створити детаљан профил детета, чиме се повећава опасност по његову безбедност и приватност, а ОЕЦД типологија крађу идентитета детета повезује и са

[85]Чл. 1. ст. 2. Закона бр. 71 од 29. маја 2017. године, у тексту измењеном Законом бр. 70 од 17. маја 2024. године (*Disposizioni e delega al Governo in materia di prevenzione e contrasto del bullismo e del cyberbullismo*), *Gazzetta Ufficiale n. 125* од 30. маја 2024; преузето 20. 10. 2026, доступно на: https://www.normattiva.it/atto/caricaDettaglioAtto?atto.codiceRedazionale=24G00086&atto.dataPubblicazioneGazzetta=2024-05-30.

[86]Чл. 111 ст. 10 Закон о основама система образовања и васпитања, *Службени гласник РС, бр. 88/2017, 27/2018 – др. закони, 10/2019, 6/2020 – др. закон, 129/2021 и 92/2023.*

[87]Чл. 5 Loi n° 2023-566 du 7 juillet 2023 visant à instaurer une majorité numérique et à lutter contre la haine en ligne; преузето 1. 10. 2026, доступно на: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047799533; M. Niestadt, op. cit., стр. 9.

[88]Чл. 19 Закон о изменама и допунама Закона о основама система образовања и васпитања, *Службени гласник РС, бр. 92/2023* (чл. 111. ст. 12). Национална платформа за превенцију насиља *Чувам те*, преузето 1. 10. 2026, доступно на: https://cuvamte.gov.rs.

безбедносним ризицима у дигиталном окружењу, попут „фишинг" (енгл. *phishing)* порука које такву злоупотребу олакшавају.[89]

Заштита деце од ових облика угрожавања не може се, међутим, заснивати искључиво на формалним правним механизмима. Поред примене прописа, неопходни су развој дигиталне писмености, едукација родитеља и деце, као и активна улога образовних установа у превенцији дигиталног насиља. Дигитално насиље и злоупотреба података данас представљају значајне претње праву детета на приватност, због чега је неопходно обезбедити свеобухватан систем заштите који обједињује правне, образовне, институционалне и техничке механизме усмерене ка безбедном коришћењу дигиталних технологија од стране деце.

3.4. Профилисање и други савремени изазови заштите приватности детета

Истраживање Ливингстон, Стоилове и Нандагиријеве показује да деца имају најмање разумевања управо о начину на који компаније користе њихове личне податке у комерцијалне сврхе. Иако већина деце препознаје циљано оглашавање и разуме да су рекламе повезане са њиховим претходним претрагама и активностима на интернету, много теже схватају да се током коришћења дигиталних услуга прикупљају и други подаци о њима, попут IP адресе, података о уређају или времена проведеног на одређеној страници, и да се ти подаци могу комбиновати и користити за креирање њиховог дигиталног профила. Истовремено, деца имају ограничену контролу над коришћењем сопствених података, будући да су подешавања приватности често сложена, услови коришћења неразумљиви, а давање података се у пракси често доживљава као услов за коришћење одређене услуге. Посебно је значајно то што деца, услед недовољног разумевања начина на који компаније прикупљају и користе податке, своја схватања поверења из личних односа преносе и на комерцијалне субјекте: компанијама верују на основу њихове познатости, препорака других или сопственог позитивног искуства, чиме могу потценити ризике повезане са комерцијалном обрадом и коришћењем њихових личних података.[90]

Истраживање истих ауторки показује и да деца о приватности и заштити личних података најчешће уче кроз сопствено искуство, методом покушаја и грешака, као и уз помоћ вршњака, породице и интернета.[91] Иако на тај начин развијају практичне вештине сналажења у дигиталном окружењу, њихово знање често остаје фрагментарно

[89]OECD, op. cit., стр. 13.
[90]M. Stoilova, S. Livingstone, R. Nandagiri, op. cit., стр. 200–201.
[91]Ibid., стр. 202.

и праћено погрешним схватањима, посебно када је реч о сложенијим питањима попут профилисања, трагова података, комерцијалне употребе личних података и политика приватности, због чега деца често верују да њихови подаци немају већу вредност или да нису изложени значајнијим ризицима. Ауторке зато указују да самостално сналажење није довољно и да је за развој критичког разумевања приватности неопходно систематично и узрасту прилагођено образовање о дигиталној писмености, уз одговарајућа регулаторна и техничка решења.

Без обзира на то колико је образовање о дигиталној писмености квалитетно, од деце се не може разумно очекивати да у потпуности разумеју и самостално управљају својим подацима и приватношћу у дигиталном окружењу које се непрестано и убрзано развија. Терет заштите стога не може бити пренесен на само дете, већ мора бити подељен са регулаторним и техничким механизмима усмереним на саме пружаоце дигиталних услуга, што представља и једну од полазних теза овог рада, на коју ће се у закључним разматрањима вратити приликом формулисања предлога за унапређење правне заштите.

Ризици повезани са комерцијалним профилисањем настају када оглашивачи користе податке настале коришћењем друштвених мрежа и других дигиталних платформи од стране деце без њиховог информисаног пристанка, односно кршећи прописе о заштити потрошача или заштиту података о личности.[92] Овоме доприноси и чињеница да многа деца немају довољно развијене вештине дигиталне писмености да би разумела обавештења са којима се сусрећу у дигиталном окружењу, нарочито када је реч о коришћењу њихових личних података.[93] У праву Европске уније, тачка 71 преамбуле ГДПР-а изричито наводи да се мере аутоматизоване обраде података, укључујући профилисање, по правилу не би требале односити на дете,[94] чиме се јасно указује да обрада личних података деце у ову сврху не би требало да представља уобичајену праксу. Упркос томе, тренутно не постоји општеприхваћен, јединствен глобални приступ регулисању праксе комерцијалног профилисања деце.[95]

Уређивање комерцијалног профилисања деце већ се, притом, одвија на три нивоа, која показују кретање од препорака законодавца ка обавезујућим прописима и даље, ка предлозима којима се та уређења проширују. Став тачке 71 преамбуле ГДПР-а нема самосталну нормативну снагу, него служи при тумачењу одредаба Уредбе. Чланом 28 ст.

[92]C. Nyst, *Privacy, Protection of Personal Information and Reputation*, Њујорк, 2017, UNICEF, стр. 11–12, преузето 1. 10. 2026, доступно на: https://www.unicef.org/childrightsandbusiness/media/281/file/UNICEF-CRB-Digital-World-Series-Privacy.pdf.
[93]OECD, op. cit., стр. 12.
[94]Тач. 71 преамбуле Уредбе (ЕУ)2016/679 (GDPR).
[95]OECD, op. cit., стр. 12.

2 Акта о дигиталним услугама (ДСА), међутим, пружаоцима онлајн платформи изричито је забрањено приказивање огласа малолетницима заснованог на профилисању, које се заснива на обради њихових личних података.[96] Најзад, предлог EU KIDS Act-а проширује то уређење и на област коју Акт о дигиталним услугама не обухвата у потпуности: поред огласа, предлогом се препоручивање садржаја малолетницима на основу профилисања, односно имплицитних сигнала активности из њиховог понашања онлајн, подразумевано искључује, уз обавезу да приоритет имају изричито изражене жеље самог детета.[97]

Профилисање се, поред комерцијалних сврха, користи и за предлагање садржаја деци, подстицање на одређена понашања, као и за одређивање места, времена и учесталости приказивања тог садржаја.[98] Посебну забринутост при томе изазивају токови садржаја који децу постепено одводе од њихове првобитне области интересовања ка садржају који за њих није примерен, укључујући не само комерцијални садржај, већ и потенцијално штетан садржај који генеришу други корисници интернета или који постаје доступан путем преузимања и других веб-сајтова. Појава таквих токова, познатих као *„rabbit holes“* (токови који корисника све дубље увлаче у непримерен садржај), била је, притом, један од директних подстицаја за одредбе предлога EU KIDS Act-а о препоручујућим системима.[99]

Додатни ризик по приватност деце представљају и уређаји повезани на интернет намењени деци, попут паметних играчака и апликација, који могу бележити локацију, снимати разговоре или омогућити непосредну комуникацију са дететом. У бројним случајевима, прикупљање и коришћење оваквих података одвија се на начин супротан мерама осмишљеним за заштиту приватности деце, услед чега су поједине институције у државама ОЕЦД-а покретале поступке спровођења закона према произвођачима оваквих уређаја и апликација.[100] Тако је, на пример, немачка Савезна мрежна агенција 2017. године забранила продају интерактивне лутке *My Friend Cayla*, сматрајући да њен

[96]Чл. 28. ст. 2. Уредбе (ЕУ) 2022/2065 Европског парламента и Савета од 19. октобра 2022. године о јединственом дигиталном тржишту, измена и допуна Директиве 2000/31/ЕЗ (Акт о дигиталним услугама), Сл. лист ЕУ, L 277, 27.10.2022; преузето 20. 9. 2026, доступно на: https://eur-lex.europa.eu/eli/reg/2022/2065/oj/hrv.

[97]Предлог уредбе Европског парламента и Савета о заштити малолетника на интернету и измену Уредбе (ЕУ) 2022/2065 (EU Keeping Internet Digital Spaces Accountable and Trustworthy, EU KIDS Act), COM(2026) 681, 17. 9. 2026, стр. 49; преузето 20. 9. 2026, доступно на: https://digital-strategy.ec.europa.eu/en/library/proposal-eu-kids-act-eu-keeping-internet-digital-spaces-accountable-and-trustworthy.

[98]OECD, op. cit., стр. 12.

[99]EU KIDS Act, op. cit., стр. 23.

[100]OECD, op. cit., стр. 15 и 17.

уграђени микрофон и несигурна *Bluetooth* веза чине лутку скривеним уређајем за тајно снимање и преношење разговора деце. Америчка Федерална комисија за трговину покренула је 2018. године први поступак против произвођача интернет-повезаних играчака због прикупљања података о деци без обавештења родитеља и њихове сагласности, као и без одговарајућих мера безбедности података, а поступак је окончан поравнањем по којем је произвођач платио новчану казну.[101]

Употреба технологија заснованих на вештачкој интелигенцији, с обзиром на то да се ослањају на велике количине података, може представљати додатне ризике по безбедност и приватност деце, нарочито у контексту начина на који апликације за образовну технологију прикупљају и чувају личне податке деце.[102] Велики скупови података које прикупљају ове технологије могу довести и до озбиљних повреда безбедности података, укључујући незакониту употребу личних података деце. Посебна забринутост односи се на могућност да алгоритми појачавају и репродукују постојеће друштвене предрасуде, на пример оне које инвалидитет приказују на негативан начин, чиме технологије засноване на вештачкој интелигенцији могу негативно утицати и на права деце са инвалидитетом, укључујући право на образовање и заштиту од злостављања.[103]

На наведене ризике профилисања одговорила је најновија регулаторна иницијатива на нивоу Европске уније, предлог EU KIDS Act-a, који је Европска комисија усвојила 17. септембра 2026. године.[104] Овим предлогом се предвиђа да препоручујући токови дају приоритет изричитим изборима детета, да се препоруке засноване на имплицитним сигналима ангажовања подразумевано искључе, уз обезбеђивање контрола над системом препорука и опције рада без профилисања, уводе се обавезни механизми провере узраста и начело „безбедности по дизајну“ (*safety by design*) дигиталних услуга намењених деци.[105] Такође, у погледу терета доказивања, пружалац услуга је тај који мора да докаже да су његове услуге безбедне по дизајну, а не дете, његови родитељи или држава.[106] Оваквим преокретом терета доказивања предлог преузима управо оно што је у овом одељку показано као кључна слабост постојећег оквира: терет заштите не сме да лежи на детету. Иако је реч о предлогу који треба да прође редовни законодавни

[101]Ibid., стр. 16.
[102]Ibid.
[103]Ibid.
[104]Европска комисија, EU KIDS Act to restrict social media platforms' access to children in the EU, саопштење за јавност IP/26/1890, Стразбур, 17. 9. 2026; преузето 1. 10. 2026, доступно на: https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_26_1890/IP_26_1890_EN.pdf.
[105]EU KIDS Act, op. cit., стр. 11 и 13.
[106]Европска комисија, op. cit.

поступак Европског парламента и Савета, овакав приступ представља значајан помак ка регулисању управо оних пракси профилисања које постојећи правни оквир, укључујући и ГДПР, до сада није успевао ефикасно да обухвати. Питање провере узраста, које предлог детаљно уређује, ближе је разматрано у одељку 5.1.2 овог рада.

Профилисање деце, било у комерцијалне, садржајне или безбедносне сврхе, стога представља један од најсложенијих савремених изазова заштите приватности детета у дигиталном простору: изазов који захтева не само јасна законска ограничења, већ и техничка решења по дизајну, стално прилагођавање регулаторног оквира технолошком развоју, као и свест о томе да терет разумевања и заштите сопствених података не може у потпуности бити пренет на дете.

4. ПРАВНА ЗАШТИТА ДЕЦЕ У РЕПУБЛИЦИ СРБИЈИ И ДРЖАВАМА БИВШЕ ЈУГОСЛАВИЈЕ

4.1. Правни оквир Републике Србије

4.1.1. Уставноправни оквир

Основни извор права у којем су садржане најважније норме државног и правног поретка је Устав Републике Србије,[107] донет 2006. године. Као највиши правни акт Србије, Устав садржи норме које се директно тичу права детета и заштите података о личности, међутим, право на приватност није експлицитно прокламовано Уставом. Уставноправни основ за његову заштиту изводи се из уставних гаранација достојанства и слободног развоја личности, права на заштиту података о личности, а када је реч о деци, наведене одредбе потребно је тумачити у светлу посебне заштите детета.

Према Уставу деца узживају људска права примерено свом узрасту и душевној зрелости (чл. 64 ст. 1), свако дете има право на лично име, упис у матичну књигу рођених, право да сазна своје порекло и право да очува свој идентитет (чл. 64 ст. 2). Деца су заштићена од психичког, физичког, економског и сваког другог искоришћавања или злоупотребљавања (чл. 64 ст. 3). Деца рођена изван брака имају једнака права као и деца рођена у браку (чл. 64 ст. 4). Права детета и њихова заштита уређују се законом (чл. 64 ст. 5).[108]

Уставом је зајемчена заштита података о личности (чл. 42 ст. 1). Прикупљање, држање, обрада и коришћење података о личности уређују се законом (чл. 42 ст. 2), забрањена је и кажњива употреба података изван сврхе за коју су прикупљени, у складу

[107]Устав Републике Србије, *Службени гласник РС, бр. 98/2006 и 115/2021.*
[108]Ibid.,чл. 64.

са законом, осим за потребе вођења кривичног поступка или заштите безбедности Србије, на начин предвиђен законом (чл. 42 ст. 3). Свако има право да буде обавештен о прикупљеним подацима о својој личности, у складу са законом и право на судску заштиту због њихове злоупотребе (чл. 42 ст. 4).[109]

Чл. 23 Устава прокламовано је да је људско достојанство неприкосновено и сви су дужни да га поштују и штите (чл. 23 ст. 1). Свако има право на слободан развој личности ако тиме не крши права других зајемчена Уставом (чл. 23 ст. 2).[110]

Према Уставу, дете ужива посебну заштиту у складу са законом (чл. 66 ст. 1).[111]

Наведене одредбе указују да Устав Републике Србије обезбеђује пристојан нормативни оквир погодан за успостављање и даље уређивање заштите приватности детета у дигиталном простору. Ове уставне гаранције даље се разрађују кроз различите законе, међутим за предметну тему од значаја су одредбе Закона о заштити података о личности, Породичног закона и Кривичног законика, који ће бити размотрени у наставку рада.

4.1.2. Закон о заштити података о личности

Заштита података о личности у Србији уређена је Законом о заштити података о личности[112] (у даљем тексту ЗЗПЛ). Актуелни закон донет је 2018. године са циљем усклађивања националног законодавства са Општом уредбом Европске уније о заштити података (у даљем тексту ГДПР), као део процеса усаглашавања законодавства Србије са правним поретком Европске уније (у даљем тексту ЕУ) у контексту њеног статуса кандидата за чланство.

ЗЗПЛ податак о личности дефинише као сваки податак који се односи на физичко лице чији је идентитет одређен или одредив.[113] У погледу предметне теме, овако широко постављена дефиниција посебно је значајна у контексту заштите приватности детета у дигиталном простору. Иако се идентитет детета може утврдити на основу класичних личних података, као што су име, презиме, датум рођења или адреса становања, наизглед безазлени подаци у дигиталном простору такође могу омогућити његову идентификацију.

У том смислу, фотографија, видео-запис или аудио-запис могу, у смислу овог закона, представљати податке о личности уколико се на основу њих, самостално или у

[109]Ibid., чл. 42.
[110]Ibid., чл. 23.
[111]Ibid., чл. 66, ст. 1.
[112]Закон о заштити података о личности, „Службени гласник РС“, бр. 87/2018
[113]Ibid., чл. 4. ст. 1.

комбинацији са другим подацима, идентитет детета може одредити или учинити одредивим. То је посебно важно у дигиталном окружењу, где се такви подаци могу лако објављивати, умножавати и делити, чиме се повећава могућност њихове даље злоупотребе и степен угрожености приватности детета, о чему је више било речи у трећем поглављу овог рада.

За заштиту података деце, од значаја су основни принципи обраде података о личности садржани у чл. 5, према коме се подаци морају обрађивати законито, поштено и транспарентно (чл. 5 ст. 1 тач. 1), прикупљати у сврхе које су конкретно одређене, изричите, оправдане и законите и даље се не могу обрађивати на начин који није у складу са тим сврхама (чл. 5 ст. 1 тач. 2). Прикупљани подаци морају бити примерени, битни и ограничени на оно што је неопходно у односу на сврху обраде (чл. 5 ст. 1 тач. 3), тачни и, ако је то неопходно, ажурирани, узимајући у обзир сврху обраде, морају се предузети све разумне мере којима се обезбеђује да се нетачни подаци о личности без одлагања избришу или исправе (чл. 5 ст. 1 тач. 4)[114] и морају се чувати у облику који омогућава идентификацију лица само у року који је неопходан за остваривање сврхе обраде (чл. 5 ст. 1 тач. 5). Подаци се морају обрађивати на начин који обезбеђује одговарајућу заштиту података о личности, укључујући заштиту од неовлашћене или незаконите обраде, као и од случајног губитка, уништења или оштећења применом одговарајућих техничких, организационих и кадровских мера (чл. 5 ст. 1 тач. 6). За примену ових одредби одговоран је руковалац, и мора бити у могућности да предочи њихову примену (чл. 5 ст. 2).[115]

Наведени принципи представљају значајан механизам заштите деце од прекомерног прикупљања и коришћења њихових података у дигиталном окружењу, посебно имајући у виду њихову старосну доб, развојне способности и чињеницу да, у поређењу са одраслим лицима, нису нужно у могућности да разумеју природу, обим и могуће дугорочне последице обраде и даљег коришћења личних података. У том смислу, захтеви који се односе на законитост, ограничење сврхе и смањење обима података имају посебан значај у дигиталном окружењу, у којем се подаци о деци могу прикупљати, повезивати и даље обрађивати на различите начине.

[114]У контексту заштите приватности деце у дигиталном простору, посебан значај има право на брисање података, имајући у виду да информације које се једном објаве у дигиталном окружењу могу остати доступне и након што престане непосредна сврха њихове обраде, као и бити даље умножаване и дељене. Овај аспект заштите има додатни значај у односу на податке који су прикупљени или објављени у периоду детињства, будући да дете у том узрасту нема знања да у потпуности процени последице које доступност одређених података може имати на његову приватност у каснијем периоду живота.
[115]Ibid., чл. 5.

На известан начин ово је предвидео и сам законодавац, због чега је успоставио дужност руковаоца да предузме одговарајуће мере да би лицу на које се подаци односе пружио информације у погледу прикупљања података, односно информација у вези остваривања права прописана предметним законом, на сажет, транспарентан, разумљив и лако доступан начин, коришћењем јасних и једноставних речи, посебно ако се ради о информацији која је намењена малолетном лицу (чл. 21 ст. 1).[116]

У оквиру чл. 16 посебна пажња посвећена је обради података деце приликом коришћења услуга информационог друштва. Према ЗЗПЛ-у, малолетно лице које је навршило 15 година може самостално да даје пристанак за обраду података о својој личности у коришћењу услуга информационог друштва (чл. 16 ст. 1). Ако се ради о малолетном лицу које није навршило 15 година, за обраду података пристанак мора дати родитељ који врши родитељско право, односно други законски заступник (чл. 16 ст. 2). Према закону руковалац мора предузети све разумне мере у циљу утврђивања да ли је пристанак дао родитељ који врши родитељско право, односно други законски заступник малолетног лица, узимајући у обзир доступне технологије (чл. 16 ст. 3).[117]

Оваквим решењем предвиђен је додатни ниво заштите малолетних лица у дигиталном простору, посебно имајући у виду обавезу руковаоца да предузме све разумне мере како би утврдио да ли је пристанак дао родитељ који врши родитељско право, односно други законски заступник малолетног лица. Иако ово решење сматрамо оправданим и значајним у циљу спречавања детета да се лажно представи као лице које је навршило законом прописани узраст или да се пристанак законског заступника само формално претпостави, непрецизност законодавца у погледу тога шта се подразумева под „разумне мере“, као и непостојање јасно утврђених критеријума или минималног стандарда за проверу идентитета и овлашћења лица које даје пристанак, оставља висок степен дискреционог овлашћења руковаоцима у избору начина провере.

Овакво законско решење може водити до стварања неуједначене праксе у погледу примене ове одредбе, чиме би се њена сврха свела на формално испуњење нормативног захтева, без обезбеђивања њеног суштинског остваривања. Упућивање на технологије које су доступне у тренутку провере омогућава да се начин верификације прилагођава технолошком развоју, што овом законском решењу даје одређени степен флексибилности и оставља простор за његово прилагођавање новим технологијама. Међутим, сматрамо да је неопходно да законодавац утврди барем минимални стандард

[116]Ibid., чл. 21. ст. 1.
[117]Ibid., чл. 16.

поступања, којим би се поставио јасан оквир обавеза руковаоца у погледу провере идентитета и овлашћења лица које даје пристанак. На тај начин обезбедила би се уједначенија примена ове одредбе и додатно унапредио степен заштите деце у дигиталном простору.

Надзор над применом ЗЗПЛ-а врши Повереник за информације од јавног значаја (у даљем тексту Повереник).[118] Повереник је независан државни орган, а његова независност обезбеђена је забраном тражења и примања налога од било кога, забраном обављања друге делатности или јавне функције, као и самосталношћу у избору запослених.[119] У оквиру своје надлежности, Повереник врши инспекцијски надзор, поступа по притужбама лица на које се подаци односе, даје мишљења државним органима о мерама заштите података, а посебно се стара о подизању јавне свести када је реч о обради података малолетних лица (чл. 78 ст. 1 тач. 2, 3 и 6, чл. 79 ст. 1 тач. 2).[120] Ради спровођења надзора, овлашћен је да изриче корективне мере, од опомене и налога за усклађивање обраде, преко привременог или трајног ограничења, па до новчане казне.[121] Лице чија су права повређена може поднети притужбу Поверенику, покренути управни спор против његове одлуке, тражити судску заштиту, као и накнаду штете (чл. 82–86).[122]

Према извештају Европске комисије за Србију за 2025. годину наведено је да је закон у највећој мери усклађен са ГДПР-ом, али да правни оквир заштите података о личности и даље захтева усклађивање са тековима ЕУ, као и да су измене ЗЗПЛ најављене до средине 2026. године.[123] Иако актуелни закон предвиђа старосну границу од 15 година за самостално давање пристанка малолетника за обраду података о својој личности у коришћењу услуга информационог друштва (члан 16. ЗЗПЛ-а),[124] овакво решење не представља одступање од ГДПР-а. Члан 8. ст. 1. ГДПР-а предвиђа праг од 16 година за самостално давање пристанка малолетника, уз могућност да државе законом одреде нижу границу, али не ниже од 13 година,[125] тако да граница од 15 година у важећем закону представља дозвољено коришћење те маргине.

[118]Ibid., чл. 73.
[119]Ibid., чл. 74.
[120]Ibid., чл. 78. ст. 1. тач. 2, 3 и 6, чл. 79. ст. 1. тач. 2.
[121]Ibid., чл. 79.
[122]Ibid., чл. 82–86.
[123]Европска комисија, *Serbia 2025 Report*, Commission Staff Working Document SWD(2025) 755 final, Брисел, 4. 11. 2025, стр. 39, преузето 1. 10. 2026, доступно на: https://enlargement.ec.europa.eu/document/download/6e68ce26-b95b-48e1-921a-c60c12da8f00_en?filename=serbia-report-2025.pdf.
[124]Чл. 16 Закона о заштити података о личности, op. cit.
[125]Чл. 8 ст. 1 ГДПР, op. cit.

Нацрт Закона о заштити података о личности (у даљем тексту Нацрт), у погледу заштите података о личности деце, задржава већ постојећа решења, с тим што као новину изричито прописује да се при процени законитости обраде засноване на легитимном интересу руковаоца или треће стране посебно узима у обзир да ли је лице на које се подаци односе малолетно лице, као околност која захтева нарочиту заштиту његових података о личности.[126] Нацрт такође прописује да овај правни основ није применљив на обраду коју врши орган власти у оквиру своје надлежности.[127] У тренутку завршавања овог рада, јавна расправа о Нацрту, отворена 30. јула 2026. године, била је завршена, а предлог закона још увек није усвојен.

4.1.3. Породичноправна заштита приватности детета

Породични закон (у даљем тексту ПЗ) из 2005. године, са изменама и допунама, је основни правни акт за остваривање права детета у области породичних односа у Србији. Закон користи термин „дете" за свако људско биће до навршених 18 година живота[128], а у одредбама о пословној способности детета (чл. 64 ПЗ) разликује „млађег малолетника" и „старијег малолетника"[129]. Овај закон представља важан корак у имплементацији КПД у домаће право и као такав утврђује права детета као његова лична права, а не као права изведена из дужности родитеља.[130] Суштину родитељског права чине дужности родитеља да се старају о детету, док су права која им законодавац признаје по правилу у функцији испуњења тих дужности.

Иако закон не садржи одредбе које се директно односе на право детета на приватност у дигиталном окружењу, његове одредбе о правима детета и вршењу родитељског права пружају правни основ за заштиту приватности детета и у контексту употребе дигиталних технологија. Породичноправна заштита права детета на приватност заснива се пре свега на начелу најбољег интереса детета,[131] које представља једно од основних начела ПЗ.

Члан65 ПЗ признаје детету право да слободно изражава своје мишљење у свим питањима која га се тичу, при чему се његовом мишљењу мора посветити дужна пажња у складу са његовим годинама и зрелошћу. Истовремено, дете има право да

[126]Чл. 20 Нацрта закона о заштити података о личности; преузето 20. 9. 2026, доступно на: https://www.paragraf.rs/dnevne-vesti/310726/310726-vest13.html.
[127]Ibid.
[128]Чл6 Породичног закон, *Службени гласник РС, бр. 18/2005, 72/2011 – др. закон, 6/2015 и 109/2025 – др. закон*.
[129]Ibid., чл. 64 ст. 1 и 2.
[130]Н. Вучковић Шаховић, Н. Петрушић, op. cit., стр. 68.
[131]Чл. 6 ст. 3., ПЗ.

благовремено добије сва обавештења која су му потребна за формирање сопственог мишљења.[132] Наведено право представља добру полазну тачку у погледу заштите приватности детета, јер се односи не само на поступке пред надлежним органима, већ на сва питања која га се непосредно тичу. Чињеница да је право детета на изражавање мишљења везано за његову способност да формира мишљење, а не искључиво за унапред одређену старосну границу, указује на значај индивидуалне процене узраста и зрелости детета.

Иако у ЗЗПЛ-у законодавац прописује узраст од 15 година као тренутак када малолетно лице може самостално да даје пристанак за обраду података о својој личности, сматрамо да решење које нуди ПЗ у погледу права детета на слободно изражавање мишљења представља значајну полазну основу и у контексту дигиталне приватности детета. Наиме, чињеница да се значај мишљења детета везује за његове године и зрелост, а не искључиво за унапред одређену старосну границу, оставља простор да се његовом мишљењу посвети дужна пажња и пре навршених 15 година. Ово начело требало би имати у виду приликом доношења одлука о прикупљању, коришћењу, објављивању и другом поступању са подацима који се односе на дете, тако да дете, у складу са својим узрастом и степеном зрелости, не буде искључено из одлучивања о питањима која се тичу његове приватности. Напред наведено посебно је важно посматрати у контексту феномена шерентинга о коме је раније било речи.

Посебно је значајно што Породични закон предвиђа да дете које је навршило 10 година може слободно и непосредно да изрази своје мишљење у сваком судском и управном поступку у којем се одлучује о његовим правима.[133] Старосна граница од 10 година, међутим, не представља границу испод које мишљење детета није релевантно. Основно правило из чл. 65 ПЗ везује право детета на изражавање мишљења за његову способност да формира мишљење, док се године и зрелост узимају у обзир приликом одређивања тежине која ће таквом мишљењу бити дата. Овакав приступ је посебно значајан за приватност детета у дигиталном окружењу, у којем се одлуке о употреби података о детету често доносе у свакодневном животу, ван формалног судског или управног поступка. ПЗ, притом, предвиђа да суд и орган управе утврђују мишљење детета у сарадњи са стручним установама, а у присуству лица које дете само изабере (чл. 65 ст. 6).[134] Тиме је обезбеђено да мишљење детета буде изражено слободно, а не

[132]Ibid., чл. 65 ст. 1–3.
[133]Ibid., чл. 65 ст. 4.
[134]Ibid., чл. 65 ст. 6.

под утицајем лица чији интереси могу бити супротстављени интересима детета, што има посебну тежину у контексту шерентинга, где је управо питање да ли је дете слободно изразило мишљење о објављивању сопствених фотографија, уколико је уопште такво питање постављено, често одлучујуће.

Родитељско право, са друге стране, обухвата права и дужности родитеља да се старају о личности, правима и интересима детета,[135] при чему се мора вршити у складу са најбољим интересом детета. Из тога произлази да укључивање детета у одлучивање о питањима његове приватности не значи преношење одговорности са родитеља на дете, већ остваривање права детета да буде информисано и саслушано у мери која одговара његовим степеном зрелости. На тај начин, најбољи интерес детета и право детета на учешће не представљају супротстављене категорије, већ принципе који се међусобно допуњују.

Ипак, у домаћем праву постоји више различитих старосних граница релевантних за питања приватности детета: 10 година за директно изражавање мишљења детета у поступку (чл. 65 ст. 4 ПЗ), 14 година за старијег малолетника (чл. 64 ст. 2 ПЗ) и 15 година за самостално давање пристанка на обраду података у услугама информационог друштва (чл. 16 ЗЗПЛ). Ово показује да законодавац старосну границу не третира као јединствено питање, већ као питање које зависи од конкретне правне ситуације. Посматрано у целини, наведена правила пружају основу за став да се заштита приватности детета не може свести искључиво на обавезу родитеља и других лица да поступају у најбољем интересу детета. Са развојем способности детета да разуме значај и последице одређене употребе његових података, све већи значај добија и његово учешће у одлучивању о тим питањима. Овакво схватање је од посебног значаја у дигиталном окружењу, у којем одлуке о подацима о детету могу имати дугорочне последице по његову приватност и лични развој.

4.1.4. Кривичноправна заштита приватности детета

Поред уставноправне, породичноправне и управноправне заштите, право детета на приватност у Републици Србији ужива заштиту и у оквиру кривичног права. Иако Кривични законик (у даљем тексту КЗ) не предвиђа посебно кривично дело усмерено на повреду приватности детета у дигиталном окружењу, поједине инкриминације пружају непосредну или посредну заштиту приватности малолетних лица.

[135] Ibid., чл. 67 и 68.

У том смислу, од значаја су кривична дела неовлашћеног прислушкивања и снимања из чл. 143 КЗ,[136] неовлашћеног фотографисања из чл. 144 КЗ,[137] као и неовлашћеног објављивања и приказивања туђег списа, портрета и снимка из чл. 145 КЗ.[138] Наведене инкриминације могу бити релевантне за заштиту детета од неовлашћеног снимања, фотографисања и објављивања садржаја који задиру у његов лични живот. Посебан значај ових одредаба у савременом контексту произлази и из чињенице да се фотографије, видео-записи и други садржаји могу веома брзо учинити доступним великом броју лица путем интернета и друштвених мрежа.

Посебно место заузима кривично дело неовлашћеног прикупљања личних података из чл. 146 КЗ, којим се санкционише неовлашћено прибављање, саопштавање или употреба података о личности у сврху за коју нису намењени, као и противправно прикупљање и коришћење података о личности.[139] Имајући у виду све већу количину података о деци који се обрађују путем дигиталних платформи и различитих информационих система, наведена инкриминација представља један од кривичноправних механизама који настоје да обезбеде заштиту од противправног поступања са подацима о личности.

Када је реч о специфичним ризицима којима су деца изложена у дигиталном окружењу, значајна је и одредба чл. 185б КЗ, којом је инкриминисано коришћење рачунарске мреже или комуникације другим техничким средствима за договор о састанку са малолетником, уз намеру извршења одређених кривичних дела против полне слободе, и појављивање на договореном месту.[140] Иако ова одредба није усмерена непосредно на заштиту права на приватност, њен значај за ову тему огледа се у заштити деце од специфичних облика злоупотребе који се остварују коришћењем дигиталних комуникационих средстава, посебно у контексту дигиталног насиља о коме је већ било речи.

Иако наведене одредбе омогућавају кривичноправну заштиту детета од појединих облика повреде приватности и злоупотребе у дигиталном окружењу, кривично право има ограничен домет, јер се активира тек код тежих облика противправног понашања, док се велики број повреда приватности детета у дигиталном простору дешава без достизања прага кривичне одговорности. Специфичности дигиталног окружења, попут

[136]Чл. 143 Кривичног законика, „Службени гласник РС", бр. 85/2005, 88/2005 – испр., 107/2005 – испр. и др. закони, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016, 35/2019, 94/2024 и 63/2026.
[137]Ibid., чл. 144.
[138]Ibid., чл. 145.
[139]Ibid., чл. 146.
[140]Ibid., чл. 185б.

лаког умножавања и даљег дистрибуирања садржаја, њихове потенцијално дуготрајне доступности и различитих начина обраде података, постављају изазове који нису изричито обухваћени посебним кривичноправним одредбама. Због тога се заштита мора посматрати као шири систем који укључује правила о заштити података, породичноправне механизме, образовни систем и институционални надзор.

4.1.5. Пракса заштите права на приватност детета у Републици Србији

Анализа нормативног оквира заштите права детета у дигиталном простору неминовно захтева и осврт на институционалну праксу Републике Србије кроз конкретне случајеве поступања државних институција, судова и независних државних органа, како би се стекао јасан увид у којој мери прокламована правна заштита, онако како је постављена у овом тренутку, заиста функционише у пракси. Имајући у виду напред наведено, у наставку овог рада, методом студије случаја, биће представљени и коментарисани неки од најзначајнијих примера из домаће праксе у циљу формирања објективне оцене нивоа заштите приватности детета у дигиталном простору.

Релевантни примери су издвојени према три критеријума: 1. случајеви који су доспели до највишег суда (одлука Врховног касационог суда), 2. случајеви у којима су надзорни органи процесно деловали у оквиру својих овлашћења и 3. случај масовне повреде права детета на приватност у јавном простору, документован независним истраживањем.

Када је реч о судској пракси, најзначајнији до сада забележен пример у погледу предметне теме представља пресуда Врховног касационог суда Републике Србије (у даљем тексту ВКС) Рев. 14012/2022.[141] У овом случају малолетна тужиља АА покренула је поступак за заштиту од насиља у породици због тога што је њен отац на друштвеној мрежи *Facebook* објављивао фотографије на којима се она налази у купаћем костиму крај базена, као и заједничке фотографије из купатила. Нижестепени судови одбили су тужбени захтев као неоснован, налазећи да објављивањем фотографија на свом *Facebook* профилу отац није учинио повреду права детета, и то права на безбедан живот и права на приватност, наводећи да фотографије и контекст у коме су настале нису непримерени за објављивање. Поступак су нижестепени судови водили као поступак заштите од насиља у породици, док је ВКС утврдио да се ради о поступку заштите права детета, па је по том основу приступио испитивању тужбеног захтева. Поступајући у овом предмету, ВКС је заузео став да тужени отац малолетне тужиље није учинио

[141]Пресуда Врховног касационог суда Републике Србије, Рев. 14012/2022 од 6. 10. 2022. године.

повреду права детета и то повреду права на безбедан живот и повреду права на приватност, превасходно из разлога што је фотографије детета објавио други родитељ, отац, и јер је у поступку утврђено да фотографије, као и контекст у којем су сачињене фотографије, нису непримерене, нису злоупотребљене нити коришћене у недозвољене сврхе, нити је малолетна тужиља трпела душевну бол због објављивања. Такође, ВКС налази да је објављеним фотографијама тужени желео да укаже јавности на срећу и задовољство малолетне тужиље, а као одлучну чињеницу за доношење ове одлуке навео је да су фотографије објављене пре него што је законска заступница тужиље, мајка, изјавила противљење објављивању фотографије детета на друштвеним мрежама, а на којима се може идентификовати њен лик. У даљем образложењу пресуде ВКС је навео да је ревизијом основано указано да су нижестепени судови, одлучујући о захтеву тужиоца да убудуће објављује фотографије детета путем друштвених мрежа, погрешно применили чл. 6 ПЗ, јер се нису руководили најбољим интересом детета.[142] У свом образложењу ВКС је навео следеће: *„Мајци млт. тужиље, ББ поверено је одлукама суда вршење родитељског права над млт. АА. Тужени је родитељ који не врши родитељско право и има право да издржава дете, да са дететом одржава личне односе и да о питањима која битно утичу на живот детета одлучује заједнички и споразумно са родитељем који врши родитељско право (образовање детета, предузимање већих медицинских захтева над дететом, промена пребивалишта детета и располагање имовином детета велике вредности и сл.) Суштински, објављивање фотографија деце на интернету путем сервиса за друштвене мреже може да представља опасну активност. Родитељи, када објављују фотографије своје деце, имају слободу избора да ли ће фотографије да објаве или не, али само док заједнички врше родитељско право и док имају исте ставове по том питању. Родитељи млт. АА имају супротне ставове о објављивању фотографија млт. АА на интернету путем сервиса за друштвене мреже и различита схватања о томе које би то последице могло имати по њу. Малолетна АА није свесна своје приватности, нити права да је заштити. Због тога, о њеној приватности, ради остваривања најбољег интереса детета, треба да брине родитељ коме је поверено вршење родитељског права. Законска заступница млт. АА има став да ради заштите безбедности и приватности не треба објављивати фотографије млт. АА на којима се идентификује њен лик. Стога, од тренутка када је законска заступница млт. тужиље изразила несагласност*

[142]Ibid.

са објављивањем фотографија млт. АА на друштвеним мрежама, на којима се она може идентификовати, нико, па ни други родитељ, којем није поверено вршење родитељског права, нема право да објављује те фотографије.“[143]

Одлучујући по ревизији малолетне тужиље, ВКС је преиначио пресуду Апелационог суда у Крагујевцу Гж2-187/22 од 19. 5. 2022. године и пресуду Основног суда у Крагујевцу П2-239/21 од 11. 3. 2021. године, забранио туженом да убудуће фотографије своје малолетне ћерке објављује на друштвеним мрежама, обавезао га да малолетној тужиљи плати половину трошкове поступка, а ревизију у преосталом делу одбио као неосновану.[144]

Најпре, у оцењивању ове одлуке можемо се сагласити са Тасићевом, која указује да је у овом случају најбољи интерес детета, иако самосталан правни стандард, оцењен не кроз призму околности конкретног случаја, већ кроз призму става родитеља коме је поверено вршење родитељског права.[145] Сагласност са овом оценом, међутим, није крај анализе, већ полазна тачка за три додатна посматрања.

Прво, сама чињеница да је ВКС предмет квалификовао као поступак заштите права детета, за разлику од нижестепених судова, који су га квалификовали као поступак заштите од насиља у породици, представља тачну и вредну одлуку – потврђује да је објављивање фотографија детета од стране родитеља питање заштите права детета, а не питање насиља у породици, чиме је феномен шерентинга добио и процесно упориште у домаћем праву. Управо због тога, недостаци који следе добијају на тежини.

Наиме, у поступку који је суд исправно квалификовао као поступак заштите права детета, садржина одлуке у суштини се своди на разрешење сукоба родитеља око питања ко ће одлучивати о објављивању фотографија. И сам суд наводи да одлучујућа чињеница није ништа што се тиче саме малолетне тужиље и њених интереса, већ тренутак у коме је мајка, као законска заступница, изразила противљење. То је посебно изражено у томе што из образложења пресуде не произлази да су развојне способности детета, као ни његово мишљење у смислу чл. 65 ПЗ, биле предмет самосталног оцењивања, независно од става законске заступнице. Најбољи интерес детета је стандард чија примена претпоставља оцењивање на основу конкретно утврђених чињеница о детету у сваком конкретном случају. У доступном образложењу, међутим, такве чињенице се не наводе, а једини фактички елемент из којег суд изводи закључак о

[143]Ibid.
[144]Ibid.
[145]A. Tasić, op. cit., стр. 92.

најбољем интересу јесте став мајке, као законске заступнице. Иако ревизиони поступак не подразумева утврђивање нових чињеница, управо из тог разлога било би очекивано да ВКС, уколико утврђено стање ствари није омогућавало самостално оцењивање најбољег интереса детета, укаже на то као на повреду примене материјалног права и предмет врати на поновљени поступак, уместо да стандард најбољег интереса детета изведе из воље законске заступнице.

Друго, навод пресуде да „малолетна АА није свесна своје приватности, нити права да је заштити“, не указује где из образложења произлази на који начин је овај став утврђен (стручним налазом, саслушањем детета или другог доказа), а управо се на њему гради закључак да о приватности детета треба да брине родитељ коме је поверено вршење родитељског права. Оваквим решењем се, парадоксално, неспособност детета да заштити своје право користи као разлог да се то право потпуно пренесе на једног од родитеља, уместо да буде околност која захтева појачану државну заштиту. Такав приступ стоји у напетости са начелом развојних способности детета (чл. 5 КПД) и са ставом Општег коментара бр. 25 да државе морају признати значај развојних способности детета у одлучивању о његовој дигиталној приватности.

Треће, резултат одлуке има и последицу коју пресуда не разматра. Оно што је објављено пре противљења мајке остаје легитимно објављено, без било каквог механизма уклањања већ објављеног садржаја. То произлази директно из изреке пресуде, с обзиром на то да је суд ревизију у преосталом делу одбио као неосновану, тако да се забрана односи само на будуће објављивање, док већ објављени садржај остаје без икакве судске реакције. Иако је суд објављивање фотографија деце оценио као могућу „опасну активност“, истовремено је утврдио да повреде права није било, будући да је објављивање вршио родитељ који у том тренутку још није био супротстављен другом родитељу који врши родитељско право. Тиме се потврђује да су заштита и опасност у овој одлуци процењиване у односу на сагласност родитеља, а не у односу на интерес детета као самосталан стандард.

Упркос наведеним резервама, одлука ипак представља важан корак у домаћој пракси, први случај у којем највиши суд директно расправља објављивање фотографија детета на друштвеним мрежама, препознаје објављивање као потенцијално опасну активност, исправно квалификује поступак као поступак заштите права детета и потврђује да родитељско право мора да се врши у складу са правима и интересом детета, а не обрнуто. Управо зато што је исход исправан, а образложење методолошки није разрађено, одлука најбоље илуструје налаз да домаћа пракса још увек нема

разрађену методологију самосталне примене стандарда најбољег интереса детета у случајевима шерентинга, што се у завршном делу рада показује као један од кључних проблема које би будућа регулација требало да реши.

На плану заштите података о личности, репрезентативан пример институционалне праксе представља поступање Повереника поводом портала „Здравитас“, платформе Министарства просвете за праћење физичког развоја и моторичких способности ученика основних и средњих школа.[146] У оквиру портала обрађују се, поред основних идентификационих података (име, презиме, ЈМБГ, датум и место рођења, пол), и подаци о телесној висини, маси, индексу телесне масе и резултатима више физичких тестова (трчање на 20 метара, скок удаљ, издржај у згибу и др.), при чему је реч о масовној обради података ученика основних и средњих школа на нивоу целог образовног система. Како се наводи на порталу Министарства просвете, резултати у овим мерењима се бележе од трећег разреда основне школе до завршетка средње школе, а након тога се уклањају (анонимизују). Даље се наводи да су ови подаци раније били бележени у педагошким свескама предметног наставника, а сада се ти подаци уносе на портал, што значи да се мења само начин евиденције, са папирног на електронски. Напоменуто је да се на порталу не уносе здравствени подаци ученика, нити портал Здравитас може да приступа и дели податке са Информационим системом из области здравства, као и да се подаци не деле са трећим лицима и биће чувани у Државном дата центру, неће се износити из Србије нити преносити у другу државу или међународну организацију.[147] Овај случај наишао је на отпор стручне јавности, Синдиката образовања, али и родитеља ученика. Тим поводом Повереник је у октобру 2024. године спровео ванредни теренски инспекцијски надзор и утврдио да Министарство просвете податке обрађује у складу са Законом о заштити података о личности, налазећи да за ову обраду није потребан пристанак лица, с обзиром на то да Министарство просвете обрађује податке у складу са чл. 12 ЗЗПЛ-а.[148]

Поводом овог саопштења Синдикат образовања Србије упутио је Поверенику захтев за спровођење допунског надзора, доводећи у питање да ли је сврха обраде заиста оправдана, неопходна и сразмерна, односно да ли је поштовано начело ограничења

[146]Министарство просвете, науке и технолошког развоја, *Портал Здравитас је дигитализација вођења евиденције у оквиру предмета Физичко и здравствено васпитање*, преузето 22. 9. 2026, доступно на: https://prosveta.gov.rs/vesti/portal-zdravitas-je-digitalizacija-vodjenja-evidencije-u-okviru-predmeta-fizicko-i-zdravstveno-vaspitanje/.
[147]Ibid.
[148]Повереник за информације од јавног значаја и заштиту података о личности, Саопштење: „Здравитас“, Београд, 28. 10. 2024; преузето 10.9.2026., доступно на: https://poverenik.rs/saopstenje-poverenika-zdravitas/.

обраде у односу на сврху, као и начело интегритета и поверљивости података.[149] Након овога, Министарство просвете је упутило допис основним и средњим школама којим је одложило пуштање у рад корисничког дела портала Здравитас. У допису је наведено да, имајући у виду неслагање и неприхватање једног дела родитеља, одлаже се пуштање корисничког портала, с обзиром на то да ће „одређени кораци захтевати више времена и другачији приступ у објашњавању и промоцији савременог, вишефункционалног инструмента као што је портал Здравитас“. До дана писања овог рада, из доступних извора не произлази да је овај портал пуштен у рад.

Овај случај добро илуструје ограничења чисто формалноправног приступа инспекцијском надзору. Чињеница да за одређену обраду података постоји декларативни правни основ у закону не значи нужно да је обим прикупљених података, укључујући антропометријске податке малолетника, повезане са ЈМБГ-ом, унутар дигиталног регистра, заиста неопходан и сразмеран сврси која се тиме жели остварити, а то је питање које чисто формална провера законитости основа обраде не мора нужно ни да отвори.

Посебно питање, које у саопштењу Повереника уопште није отворено, односи се на квалитет обрађених података. Антропометријски подаци и подаци о физичким способностима ученика, посебно када су повезани са јединственим идентификатором попут ЈМБГ-а, постављају питање да ли спадају у посебне врсте података о личности, као што су подаци о здравственом стању, који по ЗЗПЛ-у уживају појачану заштиту. Ово питање није отворено ни у саопштењима Министарства, које наводи да се на порталу не уносе здравствени подаци, чиме је квалификација података, уместо да буде предмет оцењивања, претпостављена као решена.

Такође, навод Министарства да је реч о дигитализацији постојеће евиденције, вођене до сада у педагошким свескама предметног наставника, не обухвата цео профил ризика. Подаци у педагошким свескама били су расути и физички приступачни у првом реду наставнику који их води, без могућности централизованог претраживања, повезивања и масовне анализе. Електронски регистар у који се истоветни подаци уносе за све ученике система, повезани са ЈМБГ-ом и смештени у јединствену базу у Државном дата центру, ствара ризике агрегације, повезивања и масовне обраде које папирна евиденција

[149]Синдикат образовања Србије, Захтев Поверенику за спровођење допунског надзора примене ЗЗПЛ у оквиру пројекта „Здравитас“, Београд, новембар 2024; преузето 15. 9. 2026, доступно на: https://sind-obr.org.rs/wp-content/uploads/2024/11/Povereniku_ZDRAVITAS.pdf.

није имала, тако да промена медија није неутрална за питање неопходности и сразмерности обраде.

На крају, вреди констатовати да је управо јавна расправа коју је случај изазвала, а не налаз Повереника, довела до прилагођавања праксе – пуштање у рад корисничког дела портала одложено је поводом неслагања дела родитеља,[150] а из доступних извора не произлази да је портал након тога пуштен у рад. Налаз надзорног органа да је обрада законита, дакле, није одредио даљу судбину пројекта, већ је иста обликована родитељским, стручним и медијским притиском. Случај тиме показује да механизам надзора у овој области не производи ефикасну, трајну заштиту података малолетних лица ни када утврди законитост, што је од посебног значаја за оцењивање ефикасности механизама заштите у завршном делу рада.

Пракса Регулаторног тела за електронске медије (у даљем тексту РЕМ) пружа, вероватно, најјаснију илустрацију стварног стања заштите приватности деце у јавном простору Републике Србије.

Приликом анализе институционалне праксе у овој области, полазно ограничење представља недоступност званичне документације. Због тога се анализа институционалне праксе у овом раду у већем делу ослања на извештавање организација које се баве истраживачким новинарством и анализама организација цивилног друштва, уз приписивање сваког податка извештавању. Само стање недоступности званичних докумената о поступању државних органа у питањима која се тичу малолетника сматрамо посебним обликом проблема транспарентности.

У предмету, поводом емисије „ДНК“ која је емитована 30. 11. 2016. године, РЕМ је пружаоцу медијских услуга (у даљем тексту ПМУ) спорне емисије изрекао меру опомене 26. 4. 2017. године због емитовања садржаја у којем је индиректно откривен идентитет малолетних лица, чиме су прекршене одредбе чл. 50 ст. 1 и чл. 68 ст. 11 Закона о електронским медијама, затим чл. 24 ст. 1 и 2 и чл. 26 ст. 3 Правилника о заштити права малолетника у области пружања медијских услуга. ПМУ спорне емисије није испоштовао ни обавезе које се тичу заштите приватног и породичног живота из Правилника о заштити права малолетника у области пружања медијских услуга, чл. 28. ст. 1 и 3.[151] У конкретном случају приказана су малолетна деца, а пред камерама је

[150]Министарство просвете, науке и технолошког развоја, *Одлаже се пуштање у рад корисничког дела портала Здравитас*, преузето 22. 9. 2026, доступно на: https://prosveta.gov.rs/vesti/odlaze-se-pustanje-u-rad-korisnickog-dela-portala-zdravitas/.

[151]Чл. 50 ст. 1 и чл. 68 ст. 11 Закона о електронским медијама, *Службени гласник РС, бр. 83/2014 и 6/2016 –др. закон*; чл. 24. ст. 1. и 2., чл. 26. ст. 3. и чл. 28. ст. 1. и 3. Правилника о заштити права малолетника у

говорио седмогодишњи дечак, ученик првог разреда, чији је лик био замагљен, али глас није био модулиран. Одлучујући по овом предмету, РЕМ је имао у виду да пружалац медијске услуге није водио рачуна о заштити малолетне деце, јер иако имена нису поменута, а лица су била замагљена, на основу учешћа оца и мајке и места становања могуће је утврдити идентитет деце, чиме им је нанета штета, угрожена њихова људска права и достојанство личности, здравствени, морални и социјални развој. У свом извештају РЕМ наводи да појављивање деце у оваквом програму (ријалити садржај), у којем је саопштено низ детаља који задиру у њихову приватност, и поред очигледне дозволе родитеља представља грубо кршење прописа; ПМУ јесте испоштовао форму, евидентно прибавио сагласност родитеља, али није узео у обзир погубност оваквих садржаја по децу, и колико јавно саопштавање података о томе ко су им (или нису) биолошки родитељи, какви су њихови морални поступци, понашање у животу и брачној заједници угрожава малолетнике, излаже их додатном понижењу, омаловажавању, притиску непосредног окружења, вређању или пак осуди. Њихов живот од тог тренутка, од објављивања података, добија нову димензију; угрожен им је интегритет, а њихов правилан развој доведен у питање. Приликом изрицања мере Савет је као отежавајућу околност узео у обзир већ изречену меру пружаоцу медијске услуге због истог програмског садржаја (мера упозорења изречена на седници Савета РЕМ-а од 21. 10. 2015. године). Без обзира на то што су законски заступници, у конкретном случају родитељ детета, дали сагласност за појављивање детета у програму, ова сагласност не искључује одговорност ПМУ за објављивање садржаја, нити обавезу да се приликом учешћа детета у програму посвети посебна пажња заштити његових права. Овом ПМУ изречено је више мера заштите, опомене и упозорења у периоду од 2014. до 2021. године,[152] међутим, већина мера изречених у разматраном периоду брисана је у складу са чл. 29 ст. 9 Закона о електронским медијима (у даљем тексту ЗЕМ), тако да њихов садржај није доступан за анализу. Међутим, оно што се може утврдити јесте да „блаже“ мере нису остварile превентивни ефекат нити утицале на ПМУ да ове повреде не врши. Наведени предмет одлучен је под оквиром важећим у време поступка: Законом о електронским медијама из 2014. године и Правилником о заштити права малолетника у области пружања медијских услуга из 2015. године, који је у међувремену, заједно са

области пружања медијских услуга, *Службени гласник РС, бр. 25/2015*; Регулаторно тело за електронске медије, Извештај о раду за 2017. годину, Београд, 2018, стр. 17, преузето 15. 9. 2026, доступно на: https://www.rem.rs/uploads/files/izvestaj%20o%20radu/Izvestaj%20o%20radu%20REM%202017..pdf.

[152]Регулаторно тело за електронске медије, Регистар пружалаца медијских услуга; преузето 15. 9. 2026, доступно на: https://rem.rs/sr/registar-pruzalaca-medijskih-usluga/575#gsc.tab=0.

самим Законом, замењен Законом из 2023. године и новим Правилником из 2024. године, без измене основног оквира заштите малолетника у медијама.[153]

Иако наведени пример потиче из 2017. године, готово идентичан образац поновио се, и то у знатно тежем и озбиљнијем облику, поводом масовних убиства у Основној школи „Владислав Рибникар“, у Малом Орашју и Дубони, у мају 2023. године, при чему је овога пута дошло и до учешћа највиших државних функционера у кршењу права детета на приватност.

Истраживање организације BIRN Србија, спроведено анализом седам најпосећенијих онлајн медијских портала, утврдило је да је визуелна идентификација малолетне жртве забележена у чак 55 случајева, од чега се 40 односило управо на убиства у Рибникару, Малом Орашју и Дубони, што истраживачи оцењују као једну од најгрубљих пракси кршења права на приватност. Иако су права малолетника посебно заштићена законом и новинарским кодексом, истраживање је показало да су управо деца једна од најугроженијих категорија лица о којима се извештава, при чему је само у периоду од 3. до 7. маја 2023. године у анализираним медијима забележено 237 текстова којима је прекршено право на приватност.[154]

Посебно забрињавајућу димензију овог случаја представља чињеница да право на приватност малолетника нису прекршили само медији, већ и највиши представници државних органа. Свега два сата након што је полиција званично саопштила број убијене деце, начелник Полицијске управе града Београда пред камерама је показао читљив списак деце које је малолетни учинилац „планирао да ликвидира“ и саопштио његово пуно име и презиме, а неколико сати касније, председник Србије јавно је цитирао податке из здравствене документације малолетног учиниоца, навео његов узраст и школу коју похађа његова млађа сестра, као и податке о примањима родитеља, при чему ниједна од ових информација није смела бити изнета јавности.[155] Према анализи BIRN-а, изношењем наведених података дошло је до повреде више прописа који уређују кривични поступак, заштиту малолетника и заштиту података о личности. Неспорно је, по оцењивању у овом раду, да овакво поступање представља повреду наведених прописа, међутим, имајући у виду ограничен обим јавно доступних

[153]Закон о електронским медијама *Службени гласник РС, бр. 92/2023*; Правилник о заштити права малолетника у области пружања медијских услуга *Службени гласник РС", бр. 43/2024*.
[154]BIRN Србија, *Invazija na privatnost: Analiza medijskog izveštavanja*, Београд, 2024, стр. 4, 5 и 22, преузето 15. 9. 2026, доступно на: https://birnsrbija.rs/wp-content/uploads/2024/01/Invazija-na-privatnost-%E2%80%93-Analiza-medijskog-izvestavanja.pdf.
[155]BIRN Србија, *Пуцњава у Рибникару: Како су Вучић и Милић прекршили законе*, 27.6.2023; преузето 18.9.2026., доступно на: https://birn.rs/pucnjava-u-ribnikaru-krsenje-zakona/.

информација и непознате све околности конкретног случаја, ауторка се неће упуштати у коначну правну квалификацију сваке појединачне повреде.

Због сензационалистичког извештавања у јавном простору родитељи убијене деце упутили су, више од три месеца након трагедије, отворено писмо медијима, тражећи да престану са наставком оваквог извештавања, а две породице поднеле су и тужбе против таблоида.[156] Ипак, у тренутку писања рада, из доступних извора не произлази да је ико од носилаца јавних функција сносио последице за изнете податке.

Да се образац наставља и у најскорије време потврђује случај сексуалног насиља над малолетним дететом у једној основној школи, медијски испраћен септембра 2026. године.[157] У интервјуима објављеним на онлајн порталима, у којима је учествовала и малолетна жртва, иако је лик био замагљен, глас није био модулиран, а из објављеног садржаја били су закључиви назив школе коју похађа, локалитет у којем живи и идентитет родитеља, чиме је, у смислу ЗЗПЛ-а, идентитет малолетника учињен одредивим, супротно Закону о јавном информисању и медијима.[158] Накнадно уклањање интервјуа са портала не мења ништа у погледу већ створеног дигиталног трага, чији фрагменти остају доступни на друштвеним мрежама, а родитељи су, како наводе, дали интервју зато што институције не реагују и јавни притисак је једини механизам који сматрају учинковитим, чиме се поново потврђује образац забележен и у случају „Здравитас“ – функцију механизама заштите права у пракси преузимају оштећени и њихове породице.

На основу изложеног, комбиновани преглед законодавног оквира и институционалне праксе у Србији указује на израженији раскорак између нормативно прокламоване и стварно остварене заштите приватности деце у дигиталном простору. Формалноправни оквир, посматран сам за себе, делује релативно разрађено, постоје механизми судске заштите (кроз поступак за заштиту права детета), надзора над обрадом података (Повереник), заштите људских права путем ванредних поступака (Заштитник грађана) и медијске регулације са изричитим овлашћењем за поступање по службеној дужности управо када су у питању деца (РЕМ). Ипак, институционална пракса показује неколико системских слабости: прво, поступање надлежних органа готово увек је реактивно и

[156]BIRN Србија, *Slučaj Ribnikar: Da li će tabloidi snositi posledice za medijsko lešinarenje*,26.12.2024; преузето 15.9.2026., доступно на: https://birn.rs/slucaj-ribnikar-medijsko-lesinarenje/.

[157]Нова С,*Распуст је провео по болницама, 38 ноћи нисмо спавали: Потресна исповест родитеља дечака који је преживео сексуално насиље у школи у Мрчајевцима*, 3. 9. 2026; преузето 15.9.2026., доступно на: https://nova.rs/vesti/hronika/sta-se-dosad-desavalo-u-slucaju-u-mrcajevcima-od-neprimerenog-ponasanja-do-polnog-uznemiravanja/.

[158]Чл. 91 ст. 2 Закон о јавном информисању и медијама, *Службени гласник РС, бр. 92/2023 і 51/2025.*

зависи од иницијативе трећих лица (медијских удружења, синдиката, самих грађана), а не од систематског, проактивног надзора; друго, чак и када се утврди повреда, санкције су по правилу благе, најчешће опомена или упозорење; треће, родитељски пристанак и даље се у пракси третира као довољан основ за објављивање садржаја о детету, упркос томе што правна теорија, пракса Европског суда за људска права (видети одељак 5.3.) и сама пракса РЕМ-а указују на то да такав пристанак не искључује одговорност; четврто, најмасовније повреде остварују се на онлајн порталима, у простору који није у надлежности РЕМ-а, тако да се заштита ослања на појединачне механизме Закона о јавном и информисању и медијим и ЗЗПЛ-а без континуираног надзора; и, најзад, пето, случај „Рибникар“ показује да до најозбиљнијих повреда права детета на приватност може доћи и од стране представника саме државе, укључујући и њене највише функционере, чиме се доводи у питање не само ефикасност постојећих механизама заштите, већ и спремност носилаца јавних функција да их се сами придржавају. Отуда се може закључити да ниво заштите приватности деце у дигиталном простору у Републици Србији, иако нормативно утемељен, у пракси остаје фрагментаран, реактиван и неуједначен, а повремено угрожен и од стране оних институција које би требало да буду носиоци те заштите, због чега сматрамо да је потребно унапређење институционалних механизама заштите, пре свега у правцу проактивнијег надзора, ефикаснијих санкција и јаснијег третмана родитељске сагласности, као и разматрање питања да ли постојећи распоред надлежности уопште покрива простор у којем се највећи део повреда остварује, што ће бити разрађено у завршном делу рада.

4.2. Правни оквир држава бивше Југославије

4.2.1. Република Словенија

Као држава чланица Европске уније, Република Словенија примењује Општу уредбу о заштити података (ГДПР), док национални Закон о заштити личних података (*Zakon o varstvu osebnih podatkov – ZVOP-2*) допуњује и разрађује њене одредбе на националном нивоу. Посебно је значајно правило садржано у чл. 8 ZVOP-2, према којем дете може самостално дати пристанак за обраду података у вези са коришћењем услуга информационог друштва ако је навршило 15 година. За дете млађе од 15 година пристанак даје или одобрава родитељ, старатељ или друго лице које врши родитељску бригу.[159]

[159]Чл. 8. Zakon o varstvu osebnih podatkov (ZVOP-2), *Uradni list RS*, št. 163/22, 40/25 in 10/26, преузето 15. 8. 2026, доступно на: https://pisrs.si/pregledPredpisa?id=ZAKO7959#naslov-parent-463379507.

Посебан значај у систему заштите приватности деце има Информациони повереник Републике Словеније (*Informacijski pooblaščenec*), који поред надзора над применом прописа о заштити података о личности развија и праксу у областима које су непосредно повезане са употребом података о деци у дигиталном окружењу. Његова пракса обухвата, између осталог, питања објављивања фотографија малолетне деце на интернету и друштвеним мрежама, као и питања сагласности родитеља за такво поступање.[160] Посебно је значајно што се у овој пракси питање објављивања фотографија детета повезује са вршењем родитељске бриге и утицајем таквог поступања на дете.

Поред институционалних механизама заштите, у Словенији значајну превентивну и едукативну улогу има и Центар за безбеднији интернет *Safe.si*,[161] који кроз активности усмерене на децу, родитеље и наставнике указује на ризике у вези са приватношћу, заштитом личних података и дигиталним трагом.

Словеначки правни оквир се, према томе, заснива на примени ГДПР-а и националних правила о заштити података о личности, уз посебно уређење пристанка детета за услуге информационог друштва и развијену праксу надзорног органа у погледу обраде и објављивања података о деци. Посебно је значајно што се кроз праксу Информационог повереника питање приватности детета разматра и у контексту вршења родитељске бриге, што је од непосредног значаја за заштиту приватности деце у дигиталном окружењу.

4.2.2. Република Хрватска

У правном оквиру Републике Хрватске (у даљем тексту Хрватска), као државе чланице Европске уније, у области заштите приватности и личних података, непосредно се примењује Општа уредба о заштити података (ГДПР),[162] док је национални оквир допуњен *Законом о проведби Опће уредбе о заштити података*,[163] којим се обезбеђује примена и спровођење њених одредаба у хрватском правном поретку.

---

[160]Вид. нпр. Informacijski pooblaščenec, Objavljanje fotografij mladoletnega otroka s strani enega izmed staršev kljub nasprotovanju drugega, бр. 07121-1/2024/483, 23. 4. 2024; преузето 15.8.2026., доступно на: https://www.ip-rs.si/mnenja-zvop-2/objavljanje-fotografij-mladoletnega-otroka-s-strani-enega-izmed-star%C5%A1ev-kljub-nasprotovanju-drugega-1714390337; као и Informacijski pooblaščenec, Kdo odloča o objavi fotografij otrok, бр. 07121-1/2025/1393, 5. 9. 2025; преузето 15.8.2026., доступно на: https://www.ip-rs.si/mnenja-zvop-2/kdo-odlo%C4%8Da-o-objavi-fotografij-otrok-1764575439.

[161]Safe.si – Center za varnejši internet Slovenije, преузето 15.8.2026., доступно на: https://safe.si/.

[162]Уредба (ЕУ) 2016/679 (ГДПР).

[163]Чл. 1 Zakon o provedbi Opće uredbe o zaštiti podataka, *Narodne novine*, бр. 42/2018; преузето 15.9.2026., доступно на: https://narodne-novine.nn.hr/clanci/sluzbeni/2018_05_42_805.html.

У погледу обраде личних података детета у вези са услугама информационог друштва, чл. 19 Закона прописано је да је, при примени чл. 6. ст. 1. тач. а) ГДПР-а, у вези са пружањем услуга информационог друштва непосредно детету, обрада личних података детета законита ако дете има најмање 16 година.[164] Ставом 2 истог члана прецизирано је да се наведено правило о старосној граници од 16 година примењује на дете чије је пребивалиште у Републици Хрватској, чиме је законодавац уз старосни праг одредио и круг деце на који се ово национално правило примењује.

Надзор над применом прописа о заштити личних података врши Агенција за заштиту особних података (AZOP), која је законом одређена као независно државно тело.[165] За предметну тему од значаја је текст који се налази на званичној интернет страници Агенције „Primjena Opće uredbe o zaštiti podataka u odgojno-obrazovnim ustanovama“, где је истакнуто да деца заслужују посебну заштиту приликом обраде њихових личних података, имајући у виду да могу бити мање свесна ризика, последица и мера заштите, као и својих права у вези са обрадом података, указујући уједно и на значај поштовања најбољег интереса детета у контексту обраде његових личних података.[166]

Поред тога, у пракси хрватских институција заштита приватности деце све више се разматра у контексту специфичности дигиталног окружења. AZOP је у мају 2026. године објавио препоруку посвећену објављивању видео-записа деце и дељењу садржаја на интернету и друштвеним мрежама, у којој указује на посебну потребу заштите деце приликом обраде њихових личних података, као и на ризике повезане са идентификацијом детета, доступношћу и трајношћу објављеног садржаја и могућношћу његовог даљег дељења или злоупотребе.[167] Наведено показује да се заштита приватности детета у хрватском систему не ограничава само на нормативно уређивање обраде личних података, већ обухвата и специфичне ризике који произлазе из дигиталног окружења.

Може се закључити да заштита приватности деце у Хрватској почива на непосредно примењивом европском оквиру заштите личних података, допуњеном националним механизмима за његово спровођење. Посебно је значајно национално одређивање

[164]Чл. 19 ст. 1, Ibid.
[165]Чл. 4 ст. 1 и 2, Ibid.
[166]Агенција за заштиту особних података Републике Хрватске, *Primjena Opće uredbe o zaštiti podataka u odgojno-obrazovnim ustanovama*, преузето 12.9.2026, доступно на: https://azop.hr/primjena-opce-uredbe-o-zastiti-podataka-u-skolskim-ustanovama/.
[167]Агенција за заштиту особних података Републике Хрватске, *Objava videozapisa djece i dijeljenje sadržaja na internetu i društvenim mrežama*, преузето 12. 9. 2026, доступно на: https://azop.hr/objava-videozapisa-djece-i-dijeljenje-sadrzaja-na-internetu-i-drustvenim-mrezama/

границе од 16 година за самостално давање пристанка детета у контексту услуга информационог друштва, као и развој праксе надзорног органа у погледу специфичних ризика за приватност деце у дигиталном окружењу. Ове специфичности представљају основу за касније упоредноправно разматрање положаја детета и степена његове самосталности у одлучивању о личним подацима.

4.2.3. Босна и Херцеговина

Право на приватност и заштиту личних података у Босни и Херцеговини (у даљем тексту БиХ) заштићено је у оквиру уставних гаранција, а посебно уређено *Законом о заштити личних података* из 2025. године, којим је национални систем у погледу заштите података о личности усклађенса одредбама Опште уредбе о заштити података Европске уније (ГДПР).[168] Новим законом уређују се права носилаца података, обавезе контролора и обрађивача, као и надлежности Агенције за заштиту личних података у БиХ као независног надзорног органа.[169]

За заштиту приватности деце у дигиталном окружењу посебно је значајан чл. 10 Закона, којим је уређена обрада личних података детета у вези са непосредним нуђењем услуга информационог друштва. Према овој одредби, дете које је навршило 16 година може самостално дати пристанак за такву обраду, док је за дете млађе од 16 година потребан пристанак или одобрење родитеља, усвојитеља, старатеља или другог законског заступника.[170] Ово решење непосредно следи модел из чл. 8 ГДПР-а, при чему се БиХ определила за границу од 16 година.

У чл. 10 ст. 2 овог Закона успостављена је обавеза контролора да уложи разумне напоре ради провере да ли је пристанак дао или одобрио родитељ, усвојиоц, старатељ или други законски заступник, при чему закон упућује на узимање у обзир доступних технологија.[171]

Поред законодавног оквира, значај има и деловање Агенције за заштиту личних података у БиХ, која као независан надзорни орган прати примену закона и поступа у области заштите права у вези са обрадом личних података.[172]

Заштита приватности деце у БиХ, поред правила о заштити личних података, произлази и из ширег система заштите права детета, укључујући обавезе преузете КПД.

---

[168]Чл. 1 Закон о заштити личних података, *Службени гласник Босне и Херцеговине, бр. 12/25*; преузето 16.8.2026., доступно на: https://www.sluzbenilist.ba/page/akt/aCRNh0ohz4nh78h77P7BE=
[169]Чл.3Ibid.
[170]Чл. 10 ст. 1Ibid.
[171]Чл. 10 ст. 2Ibid.
[172]Чл. 96 ст.1Ibid.

У том контексту значај имају и активности институција за заштиту људских права и права детета, као и организација цивилног друштва које се баве ризицима дигиталног окружења, приватношћу и безбедношћу деце.

Може се закључити да нови Закон о заштити личних података представља значајан корак у унапређењу правног оквира за заштиту приватности у БиХ, посебно имајући у виду његову усклађеност са стандардима ГДПР-а. Са становишта заштите деце у дигиталном окружењу, посебно су значајна правила која се односе на пристанак детета за обраду личних података у вези са услугама информационог друштва. Поред утврђивања границе од 16 година за самостално давање пристанка, закон посебно обавезује контролора да уложи разумне напоре како би проверио да је пристанак дат од стране родитеља, усвојиоца или старатеља, при чему се приликом те провере узимају у обзир доступне технологије. Као и у домаћем праву, овакво решење има посебан значај за заштиту деце у дигиталном окружењу, јер се не задржава само на прописивању старосне границе, већ предвиђа и механизам за проверу лица које пристанак даје у име детета, међутим и у овом случају присутна је непрецизност законодавца у погледу тога шта се подразумева под „разумни напори“, као и непостојање јасно утврђених критеријума или минималног стандарда за проверу идентитета и овлашћења лица које даје пристанак.

4.2.4. Република Црна Гора

Заштита приватности и личних података у Црној Гори уређена је *Законом о заштити података о личности*, којим се прописују услови за обраду личних података, права лица чији се подаци обрађују и надзор над применом закона.[173]

У погледу заштите приватности деце посебно су значајне одредбе које се односе на обраду података малолетних лица. Наиме, сагласност за обраду података малолетног лица може дати родитељ или усвојилац, односно старатељ, осим уколико сагласност није у супротности са интересима малолетног лица.[174] Такође, Закон наводи и да се лични подаци који се односе на малолетно лице обрађују у складу са законом, на начин који је у најбољем интересу малолетног лица.[175]

Овакво законско решење има посебан значај јер је најбољи интерес детета кровни принцип заштите права детета, који прожима различите области правне заштите, али га

[173]Zakon o zaštiti podataka o ličnosti, *Službeni list CG*, br. 79/2008, 70/2009, 44/2012, 22/2017 i 77/2024 – prečišćeni tekst, преузето 16. 8. 2026, доступно на: https://www.gov.me/dokumenta/d65b84b4-14df-43e0-aeb2-aadf44149486.
[174]Ibid., чл. 10 ст. 3.
[175]Ibid., чл. 12.

законодавац овде изричито везује и за обраду личних података малолетника. На тај начин се наглашава да постојање сагласности родитеља, усвојиоца или старатеља само по себи не исцрпљује питање заштите детета, већ да и сама обрада личних података мора бити у складу са његовим најбољим интересом. Овај захтев добија посебну тежину у дигиталном окружењу, у којем се подаци, фотографије и други садржаји који се односе на децу могу лако даље умножавати и дистрибуирати. Питање граница родитељске сагласности и њене усклађености са најбољим интересом детета може послужити као полазиште за решавање једног од најспецифичнијих изазова за остваривање права детета на приватност у дигиталном окружењу, имајући у виду све актуелније питање правне регулације шерентинга и порозне границе између родитељског права и права детета на приватност.

Надзор над применом прописа у области заштите личних података врши Агенција за заштиту личних података и слободан приступ информацијама, као самосталан и независан надзорни орган.[176] Агенција, између осталог, врши надзор над применом закона, поступа по захтевима за заштиту права и даје мишљења и препоруке у области заштите личних података.[177]

Практичан значај заштите приватности деце у дигиталном окружењу потврђује и поступање Агенције у септембру 2024. године поводом неовлашћеног снимања и објављивања снимака малолетника на друштвеним мрежама. Агенција је указала на проблем, али је истовремено констатовала да нема законску надлежност да поступа у односу на обраду података од стране инфлуенсера на друштвеним мрежама.[178] Овај пример указује на одређене границе постојећег институционалног механизма заштите у дигиталном окружењу, али и на важност правовременог институционалног реаговања у ситуацијама када је право на приватност деце у дигиталном простору угрожено.

Заштитник људских права и слобода Црне Горе такође указује на ризике за приватност деце на друштвеним мрежама, укључујући објављивање фотографија и података о деци од стране чланова породице.[179] Тиме се потврђује да се питање приватности детета у дигиталном окружењу не односи само на поступање јавних

[176]Ibid., чл. 49.
[177]Ibid., чл. 50.
[178]Агенција за заштиту личних података и слободан приступ информацијама, Саопштење за јавност бр. 02-125-9970-1/24 од 27. 9. 2024, преузето 16. 8. 2026, доступно на: https://www.azlp.me/me/izvjestaji/20144.
[179]Заштитник људских права и слобода Црне Горе, *Извјештај о раду за 2021. годину*, Подгорица, 2022, стр. 171, преузето 16. 9. 2026, доступно на: https://www.ombudsman.co.me/docs/1652269181_final_izvjestaj_05052022.pdf.

институција и медија, већ и на поступање самих родитеља и других лица из дететовог непосредног окружења.

Може се закључити да правни оквир Црне Горе заштиту приватности деце заснива на општим правилима о заштити личних података, уз посебно уређивање положаја малолетних лица. За предмет овог рада нарочито је значајно што законодавац, поред регулисања питања сагласности за обраду података малолетника, изричито захтева да се њихови подаци обрађују у најбољем интересу детета. Истовремено, пракса надлежних институција показује да се заштита приватности деце непосредно поставља и у контексту друштвених мрежа, што представља важан аспект савремене заштите права детета у дигиталном окружењу, како од стране институција и трећих лица, тако и од стране родитеља и других лица из дететовог непосредног окружења.

4.2.5. Република Северна Македонија

Право на приватност и заштиту података о личности у Републици Северној Македонији уређено је *Законом за заштита на личните податоци*, којим се уређује заштита личних података и право на приватност у вези са њиховом обрадом.[180] Закон је донет са циљем усклађивања националног оквира са Уредбом (ЕУ) 2016/679 (ГДПР), али, према оцени Европске комисије од 4.11.2025. године, пуна усклађеност са ГДПР-ом још није постигнута.[181]

За заштиту приватности деце посебно је значајан чл. 12 Закона, којим је прописано да је, када се услуге информационог друштва непосредно нуде детету, обрада његових личних података заснована на сагласности законита ако дете има најмање 14 година. За дете млађе од 14 година сагласност мора дати или одобрити законски заступник. Поред тога, контролор је дужан да уложи разуман напор како би проверио да је сагласност дата или одобрена од стране законског заступника, узимајући у обзир расположиву технологију.[182][183]

---

[180]Закон за заштита на личните податоци, *Службен весник на Република Северна Македонија*, бр. 42/2020, 294/2021 и 101/2025, преузето 18. 9. 2026, доступно на: https://azlp.mk/wp-content/uploads/2022/11/zakon_za_zastita_na_licnite_podatoci.pdf.

[181]Европска комисија, *North Macedonia 2025 Report*, Commission Staff Working Document SWD(2025) 759 final, Брисел, 4.11.2025, стр. 36, доступно на:https://enlargement.ec.europa.eu/document/download/267b368e-6b55-4a42-bb72-6395593de4da_en?filename=north-macedonia-report-2025.pdf.

[182]Чл. 12 ст. 1 и 2.Закон за заштита на личните податоци.

[183]Идентично решење о обавези провере сагласности законског заступника садржи и нови Закон о заштити личних података Босне и Херцеговине и ЗЗПЛ, о чему је било речи у делу о законодавству Босне и Херцеговине, али са разликом да је граница за самостално давање сагласности постављена на 16 година, односно 15 у Србији. Разлика у старосном прагу показује да преузимање ГДПР стандарда не доводи нужно до истоветних националних решења, с обзиром да државе задржавају простор да самостално одреде узраст на којем дете стиче могућност да самостално даје сагласност за обраду

Надзор над применом прописа врши Агенција за заштиту личних података као самосталан и независан орган.[184] Значај заштите приватности деце у дигиталном окружењу Агенција потврђује и кроз активности усмерене на едукацију младих.[185] У јануару 2024. године представници Агенције одржали су предавања за средњошколце о заштити личних података при коришћењу интернета, при чему су посебно обрађени заштита приватности и идентитета на интернету и безбедност на друштвеним мрежама.[186]

Може се закључити да правни оквир Северне Македоније представља пример преузимања основног ГДПР модела за заштиту детета у дигиталном окружењу, али и пример националне конкретизације тог стандарда. Избор границе од 14 година, за разлику од 16 година у БиХ и 15 година у Србији, показује да заједнички европски стандард оставља простор за различита национална опредељења у погледу узраста за самостално давање сагласности. С друге стране, обавеза контролора да уложи разуман напор ради провере сагласности законског заступника иницијално представља значајнији заштитни механизам од самог утврђивања старосне границе, јер поставља захтев да се формална претпоставка родитељске сагласности замени стварном провером њеног постојања, међутим и у овом случају присутна је непрецизност законодавца у погледу тога шта се подразумева под „разумни напори“, као и непостојање јасно утврђених критеријума или минималног стандарда за проверу идентитета и овлашћења лица које даје пристанак.

Управо у том односу између старосне границе, родитељске сагласности и стварне могућности детета да контролише употребу сопствених података налази се једно од кључних питања за ефикасност заштите права детета на приватност у дигиталном окружењу.

података у вези са услугама информационог друштва (што је пракса и у државама чланицама Европске Уније), док механизам провере родитељске сагласности представља заједнички заштитни елемент.

[184]Закон за заштита на личните податоци, чл. 57; Агенција за заштиту личних података, званична интернет страница; преузето 15.9.2026, доступно на: https://azlp.mk/.

[185]Закон за заштита на личните податоци, *Службен весник на Република Северна Македонија*, *бр. 42/2020*, чл. 65 ст. 1 тач. б). Чланом 65 уређују се задаци Агенције за заштиту личних података, док се под б) посебно предвиђа да Агенција „промовише јавну свест и разумевање ризика, правила, заштитних мера и права у вези са обрадом личних података, а нарочито активности усмерене према деци“.

[186]Агенција за заштиту личних података, *Одржани часови за средношколци на тема „Заштита на личните податоци при користење на интернет“*, објава од 31.1.2024, преузето 16.9.2026, доступно на: https://azlp.mk/одржани-часови-за-средношколци-на-тем/.

4.3. Упоредноправна анализа

Правни системи држава насталих на простору бивше Југославије показују одређени степен нормативне сродности, што је, између осталог, последица заједничког правног наслеђа. Истовремено, савремени процес европских интеграција и потреба за усклађивањем националних правила са стандардима Европске уније, нарочито са ГДПР-ом, допринели су даљем приближавању ових система у области заштите приватности и личних података. Због тога се разлике међу посматраним системима не огледају се нужно у основним принципима заштите, већ пре у појединим нормативним решењима, институционалним механизмима и степену развијености праксе.

Упоредно посматрано, наведени системи се, прво, разликују у старосној граници за самостално давање пристанка детета у услугама информационог друштва. Србија и Словенија одредиле су границу од 15 година, Хрватска и Босна и Херцеговина од 16 година, при чему је хрватско правило ограничено на дете чије је пребивалиште у Републици Хрватској, Северна Македонија је определила границу од 14 година, док Црна Гора није одредила старосну границу. Друго, механизам провере пристанка законског заступника изричито је уведен у Србији, БиХ и Северној Македонији. Руковалац, односно контролор дужан је да предузме разумне мере ради утврђивања да ли је пристанак дао или одобрио законски заступник малолетног лица, узимајући у обзир расположиве технологије. Тиме је формална претпоставка родитељске сагласности у тим системима замењена стварном провером њеног постојања, што представља заштитни елемент независан од саме старосне границе, будући да упућује на питање да ли је пристанак стварно дао оно лице које је за то овлашћено. Иако ово може представљати добро решење, оно што недостаје је прецизно опредељење законодавца шта се подразумева под „разумни напори“, као и непостојање јасно утврђених критеријума или минималног стандарда за проверу идентитета и овлашћења лица које даје пристанак. Треће, јединствено у посматраном кругу држава, законодавство Црне Горе изричито везује обраду података малолетника за његов најбољи интерес, чиме на нивоу закона о заштити података о личности отвара простор за контролу и родитељске сагласности, што је директно релевантно за питање шерентинга. У осталим системима најбољи интерес детета у овој области долази до изражаја пре свега кроз праксу надзорних органа, попут праксе Информационог повереника Словеније у вези са објављивањем фотографија деце или става AZOP-а о значају тог начела при обради података у образовним установама. Четврто, надзор у свим државама врше независни органи за заштиту података о личности, али степен

развијености праксе у питањима дигиталне приватности деце се разликује. Пракса Информационог повереника Словеније и препорука AZOP-а вежу заштиту детета управо за дигитално окружење, у Црној Гори је пракса показала границе надлежности према обради података од стране приватних лица на друштвеним мрежама, док у државама у процесу европских интеграција питање пуне усклађености (Србија, Црна Гора, Северна Македонија), односно текуће примене новог оквира (БиХ), остаје отворено, како показују извештаји Европске комисије о напретку.[187] Најзад, ниједан од посматраних система не уређује феномен шерентинга изричито, тако да се заштита приватности детета у том контексту у свим системима остварује посредно, кроз правила о заштити података, породичноправне механизме и праксу надзорних органа.

Наведени налази чине основу за оцењивање положаја Србије, које ће бити изведено у завршном делу рада. Решење домаћег законодавца када је реч о пристанку малолетника, по старосној граници и по обавези руковаоца да провери сагласност законског заступника, налази се у оквиру заједничког стандарда посматраних система, а разлике у одабиру границе (14, 15, 16 година) показују се као питање националног опредељења у оквирима које ГДПР оставља државама. Истовремено, одсуство изричитог уређења шерентинга и зависност заштите од посредних механизама заједнички су за све посматране системе, што упућује на закључак да празнина у заштити приватности детета у дигиталном простору није везана за појединачни правни систем, него произлази из начина на који су ови системи, под истим европским стандардом, институционално структурирани.

Посебно питање отвара се поводом праксе црногорске Агенције (видети одељак 4.2.4.), која је поводом обраде података малолетника од стране инфлуенсера констатовала да нема законску надлежност да поступа. У таквим ситуацијама заштита података о личности малолетника остаје углавном на кривичноправним механизмима и поступању тужилаштва, органа који је и иначе оптерећен бројним предметима и који у овим питањима делује тек када понашање досегне праг кривичне одговорности, док све оно што се одвија испод тог прага, а по природи ствари највише погађа приватност детета, остаје без ефикасног надзора. Отуда се намеће питање, које ће бити ближе разрађено у завршном делу рада, да ли је ефикасније да надзор над таквом обрадом података буде поверен независном државном органу специјализованом за заштиту

[187]Видети Европска комисија, *Serbia 2025 Report*, op. cit., стр. 39; European Commission, *North Macedonia 2025 Report*, op. cit., стр. 36.

података о личности, коме су овлашћења у дигиталном окружењу изричито обезбеђена, него да се заштита ослања искључиво на накнадно кривичноправно реаговање.

5. ЕВРОПСКИ СТАНДАРДИ ЗАШТИТЕ ПРАВА ДЕТЕТА НА ПРИВАТНОСТ

5.1. Заштита права детета на приватност у праву Европске уније

5.1.1. Општи правни оквир Европске уније

Европска унија је остварила одређени напредак у заштити деце на интернету кроз низ законских аката, иницијатива и кампања за подизање свести. Регулаторни оквир који су успоставиле Унија и њене државе чланице пружа подршку у заштити дигиталних права деце и унапређењу безбедности на интернету. Ипак, још много тога треба учинити како би деца била у потпуности заштићена од ризика и штетних последица дигиталног окружења, а истовремено могла да искористе предности дигиталних алата. Једна од области којој је потребна посебна пажња јесте спровођење постојећих закона, с обзиром да деца имају тенденцију да проналазе креативне начине да заобиђу правила, а неопходна је и већа сарадња између различитих актера и нивоа власти, будући да многи ризици на интернету имају глобални карактер.[188]

Основу правног оквира чине Повеља о основним правима ЕУ (чл. 8 заштита података о личности; чл. 24 права детета), Општа уредба о заштити података (ГДПР), Акт о дигиталним услугама (ДСА), Уредба о европском оквиру дигиталног идентитета (ЕУ) 2024/1183 и, као најновији слој, предлог EU KIDS акта из 2026. године. Овај предлог изричито се тумачи у складу са члановима 7, 8, 11, 21 и 24 Повеље, уз обавезу успостављања равнотеже између сукобљених права сагласно начелу пропорционалности.[189]

На националном нивоу, поједине државе чланице предузеле су и сопствене мере. Француска је законом из 2023. године установила „дигитално пунолетство“ од 15 година, према којем друштвене мреже не смеју да прихвате пријаву малолетника млађег од 15 година без изричите сагласности најмање једног родитеља, уз право родитеља да траже обуставу налога свог детета. Примена тог закона, међутим, до сада није остварена, због одсуства подзаконског акта и поступка пред Европском комисијом.[190] Француски Парламент је, затим, 2026. године усвојио посебан закон којим се приступ

[188]M. Niestadt, op. cit., стр. 1.
[189]EU KIDS Act, op. cit., стр. 40.
[190]*Loi n° 2023-566 du 7 juillet 2023 visant à instaurer une majorité numérique et à lutter contre la haine en ligne*, JORF бр. 157 од 8. 7. 2023; о садржини и непримењивању: Vie publique, Loi du 7 juillet 2023 visant à instaurer une majorité numérique et à lutter contre la haine en ligne, преузето 10. 9. 2026, доступно на: https://www.vie-publique.fr/loi/288274-majorite-numerique-15-ans-reseaux-sociaux-loi-7-juillet-2023.

услугама друштвених мрежа изричито забрањује малолетницима млађим од 15 година; Уставни савет Француске је, међутим, укинуо кључну одредбу тог закона, налазећи да генерална забрана, без узимања у обзир узраста, зрелости и ситуације појединог малолетника, представља несразмерно задирање у слободу изражавања и комуникације и да није обезбедила законске гаранције заштите приватности.[191] Француска се, уосталом, залаже и за увођење јединствене старосне границе од 15 година на нивоу Уније.

У литератури се, међутим, поставља питање да ли европски приступ, који се све више ослања на рестриктивне мере попут одлагања приступа и провере узраста, остаје у оквирима начела пропорционалности. Волц, анализирајући аустралијски модел потпуне забране приступа друштвеним мрежама лицима млађим од 16 година, заступа став да мане опште забране не могу бити оправдане њеном заштитном намером јер се тиме занемарују позитивне функције друштвених мрежа, намећу се озбиљни изазови у спровођењу, а постоји и ризик да деца буду преусмерена у мање регулисана и потенцијално штетнија дигитална окружења, док нерешена питања приватности, аутономије и других основних права додатно доводе у питање легитимитет овакве забране.[192] Овај развој догађаја, притом, потврђује релевантност наведене критике: несразмерност генералне забране, на коју упозорава Волц, остварила се у пракси, управо као уставноправни налаз државе чланице. Овај аргумент директно је релевантан и за оцењивање европског модела одлагања приступа, будући да упућује на то да су пожељније циљане мере прилагођене конкретним ризицима него униформне забране.

5.1.2. Заштита деце у дигиталном окружењу

Акт о дигиталним услугама (енгл. *Digital Services Act*, у даљем тексту: ДСА), односно Уредба (ЕУ) 2022/2065, представља један од најважнијих прописа Европске уније у овој области. Чл. 28 ДСА обавезује пружаоце услуга онлајн платформи којима приступају малолетници да предузму одговарајуће и сразмерне мере ради обезбеђивања високог нивоа приватности, безбедности и сигурности малолетника, док чл. 28 ст. 2 изричито забрањује приказивање огласа заснованих на профилисању малолетника коришћењем њихових личних података.[193] У јулу 2025. године Европска комисија је, у

[191]Loi visant à protéger les mineurs des risques auxquels les expose l'utilisation des réseaux sociaux, усвојена 21. 7. 2026; Conseil constitutionnel, Décision n° 2026-911 DC од 14. 8. 2026; преузето 10. 9. 2026, доступно на: https://www.conseil-constitutionnel.fr/decision/2026/2026911DC.htm.
[192]S. Volz, *Age restrictions as a tool for enhancing children's online safety: an analysis with special reference to Australian law*, Computer Law & Security Review, Vol. 61, 2026, DOI: 10.1016/j.clsr.2026.106278.
[193]Уредба (ЕУ) 2022/2065 (ДСА), чл. 28.

складу са чл. 28 ст. 4 ДСА, усвојила Смернице о мерама за обезбеђивање високог нивоа приватности, безбедности и сигурности малолетника на интернету, које пружају практичан водич о томе шта заправо значи обезбедити висок ниво заштите малолетника.[194]

Спровођење ДСА већ даје конкретне резултате. Комисија је до сада предузела више од 60 активности спровођења, укључујући формални поступак против компаније *Meta* (мај 2024. године), покренут поводом сумње да друштвене мреже *Facebook* и *Instagram* искоришћавају слабости и неискуство малолетника изазивајући зависничко понашање, као и успешно повлачење апликације *TikTok Lite* са тржишта ЕУ, чији је дизајн, кроз систем награђивања за гледање садржаја, подстицао зависничко понашање.[195]

Најновији слој заштите представља Предлог уредбе Европског парламента и Савета о заштити малолетника на интернету и измену Уредбе (ЕУ) 2022/2065 (*EU Keeping Internet Digital Spaces Accountable and Trustworthy*, у даљем тексту: EU KIDS Act),[196] којим се утврђује хармонизована минимална старост од 15 година за самостално отварање налога на друштвеним мрежама и видео-платформама чије карактеристике представљају ризик по приватност, безбедност и сигурност деце.[197] За малолетнике узраста од 13 до 15 година предвиђена је могућност да старатељи отворе налог са ограниченим функцијама, уз активне алате за старатеље, ограничење дневног коришћења на највише један сат и претходно одобравање контаката.[198] За децу млађу од 13 година предвиђен је посебан режим приступа искључиво преко налога старатеља, и то само за услуге прилагођене деци.[199] Предлог, даље, уводи захтеве „безбедности по дизајну" (*safety by design*), подразумевана подешавања приватности и безбедности, као и подразумевано искључење персонализационих функција и система за препоручивање, осим уколико процена покаже да је њихова активација у најбољем интересу детета.[200]

У погледу утврђивања узраста (*age assurance*), предлог поставља изузетно захтевне стандарде: за спровођење одлагања приступа, пружаоци услуга дужни су да користе решења за проверу узраста независна од платформи, у складу са оквиром ЕУ, заснована

[194]Европска комисија, Смернице о мерама за обезбеђивање високог нивоа приватности, безбедности и сигурности малолетника на интернету, у складу са чл. 28 ст. 4 Уредбе (ЕУ) 2022/2065 (C/2025/5519), Сл. лист ЕУ, C серија, 10. 10. 2025; преузето 11. 9. 2026, доступно на: https://eur-lex.europa.eu/eli/C/2025/5519/oj.
[195]M. Niestadt, op. cit., стр. 3–4.
[196]EU KIDS Act, op. cit.
[197]Ibid., стр. 45.
[198]Ibid., стр. 46.
[199]Ibid., стр. 46–47.
[200]Ibid., стр. 47 и 49.

на доказу о узрасту који издаје независно треће лице,[201] уз примену технологије „доказа са нултим знањем" (*zero-knowledge proof*)[202], која онемогућава праћење идентитета корисника.[203] Решења за утврђивање узраста, притом, не смеју омогућити идентификацију, лоцирање, праћење, циљано оглашавање или профилисање корисника ни у коју сврху.[204]

Упркос овом регулаторном напретку, утврђивање узраста остаје најспорнији механизам новог оквира. Ливингстон и сарадници, спајајући правну и емпиријску анализу, показују да је утврђивање узраста у пракси често неефикасно у заштити деце од дигиталног ризика, док истовремено угрожава друга права детета: право на недискриминацију, приватност, право да буде саслушано и грађанска права.[205] Пошто методи утврђивања често претпостављају приступ документима, картицама или алатима дигиталног идентитета, деца која та средства немају могу бити управо она група која остаје изван дигиталног простора, иако би управо она требало највише да имају користи од дигиталне инклузије. Према закључку студије Саса и Милберга, тренутно не постоји метод утврђивања узраста који би адекватно штитио основна права, што додатно заоштрава ово питање.[206] Стала-Бурдијон, посматрајући проблем кроз призму ГДПР-а, поставља питање да ли је европским оквиром уопште постигнут склад између онлајн безбедности и заштите података, доводећи у сумњу да ли предложени оквир утврђивања узраста успоставља одговарајућу равнотежу између супротстављених права.[207] Ипак, аутори признају да постоје снажни разлози за прихватање утврђивања узраста као норме, уз поштовање начела приватности и

[201]Ibid., стр. 62 и 33.
[202]Доказ са нултим знањем (*zero-knowledge proof*) јесте криптографски механизам којим једна страна може другој страни да докаже да је нека тврдња истинита, не откривајући јој никакве друге информације о себи; у овом контексту, корисник може да докаже да је навршио прописану старосну границу, а да пружалац услуге не сазна његов идентитет или тачан узраст. Вид. M. Sas, J. T. Mühlberg, *Trustworthy Age Assurance? A risk-based evaluation of available and upcoming age assurance technologies from a fundamental rights perspective*, Brussels, 2024, The Greens/EFA in the European Parliament, стр. 70.
[203]EU KIDS Act, op. cit., стр. 61.
[204]Ibid., стр. 61.
[205]S. Livingstone, A. Nair, M. Stoilova, S. van der Hof, C. Caglar, *Children's Rights and Online Age Assurance Systems: The Way Forward*, International Journal of Children's Rights, Vol. 32, No. 3, 2024, стр. 721, DOI: 10.1163/15718182-32030001.
[206]M. Sas, J. T. Mühlberg, Trustworthy Age Assurance? A risk-based evaluation of available and upcoming age assurance technologies from a fundamental rights perspective, Brussels, 2024, The Greens/EFA in the European Parliament; стр. 7, преузето 20.9.2026., доступно на: https://extranet.greens-efa.eu/public/media/file/1/8760.
[207]S. Stalla-Bourdillon, *A GDPR Lens on the Draft Article 28 DSA Guidelines and Their Approach to Age Assurance*, European Data Protection Law Review, Vol. 11, No. 2, 2025, стр. 207, DOI: 10.21552/edpl/2025/2/11.

безбедности по дизајну и уколико је она праћена проценом утицаја на права детета, консултацијама са децом и партиципативним дизајном самог решења.[208]

Из изложеног произлази да утврђивање узраста није сама по себи довољан показатељ ефикасне заштите. Њена оправданост зависи од тога да ли мера смањује конкретан ризик, да ли је нужан и најмање интрузиван доступан начин, те да ли су последице по приватност, недискриминацију и приступ деце дигиталним услугама сведене на меру неопходну за постизање циља.[209] Зато процена таквих механизама треба да обухвати и учешће деце у њиховом осмишљавању, а не само техничку могућност провере узраста.[210]

У мају 2022. године Европска комисија је предложила и Уредбу о спречавању и сузбијању сексуалног злостављања деце, којом би пружаоци услуга хостинга и интерперсоналне комуникације били обавезани да откривају, уклањају и пријављују случајеве сексуалног злостављања деце, уз оснивање посебног Европског центра за спречавање и борбу против сексуалног злостављања деце. Овај предлог остаје изузетно контроверзан управо са становишта права на приватност, пре свега због обавезе скенирања приватних комуникација, док је његова коначна судбина још увек неизвесна.[211]

На основу резултата тзв. *Digital Fairness Fitness Check* анализе из 2024. године, Европска комисија је закључила да је потребан посебан Акт о дигиталној праведности, који би требало да обухвати проблеме попут манипулативних образаца дизајна (*dark patterns*), маркетинга путем инфлуенсера, зависничког дизајна дигиталних производа и профилисања рањивих потрошача.[212] У Радном програму за 2026. годину Европска комисија је овај акт навела као законодавну иницијативу планирану за четврти квартал 2026. године.[213]

5.1.3. Заштита личних података деце према ГДПР-у

Општа уредба о заштити података (енгл. *General Data Protection Regulation – GDPR*, у даљем тексту: ГДПР), односно Уредба (ЕУ) 2016/679,[214] полази од становишта да

[208]S. Livingstone и др., *Children's Rights and Online Age Assurance Systems*, op. cit., стр. 738.
[209]Ibid., стр. 730.
[210]Ibid., стр. 738.
[211]Европска комисија, Предлог уредбе Европског парламента и Савета о успостављању правила за спречавање и сузбијање сексуалног злостављања деце, COM(2022) 209 final, 11. 5. 2022; преузето 15. 9. 2026, доступно на: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2022:209:FIN.
[212]M. Niestadt, op. cit., стр. 6.
[213]Европска комисија, Радни програм Комисије за 2026. годину, COM(2025) 870 final; преузето 25.9.2026., доступно на: https://commission.europa.eu/document/download/aa8d20ed-148f-4eaa-b8ea-92be7acdaee6_en.
[214]Тач. 38 преамбуле Уредбе (ЕУ) 2016/679 (Општа уредба о заштити података), op. cit.

„деца заслужују посебну заштиту у погледу својих личних података, јер могу бити мање свесна ризика, последица и заштитних мера које су повезане са обрадом личних података, као и својих права у вези са обрадом личних података“.[215] Оваква заштита примењује се, на пример, када се подаци деце користе за маркетиншке сврхе или профилисање.

Чланом 8 ГДПР-а утврђено је да, када се обрада заснива на пристанку у вези са услугама информационог друштва које се пружају директно детету, таква обрада је законита ако је дете навршило 16 година, при чему државе чланице могу снизити ову границу на 13 година.[216] Више од половине држава чланица искористило је ту могућност, услед чега старосни прагови за давање пристанка знатно варирају широм Уније.[217] Члан 12 ГДПР-а, са друге стране, гарантује да информације и комуникација са децом о обради података буду „сажете, транспарентне, разумљиве и лако доступне, уз јасан и једноставан језик“,[218] што је од кључног значаја за њихово стварно разумевање.[219]

Упркос уведеним заштитним мерама, попут посебне заштите података деце и права на заборав, у литератури се указује и на системска ограничења ГДПР-а: он се посебно не бави приватношћу деце која су предмет шерентинга, нити узима у обзир да родитељи не поступају увек у најбољем интересу детета или можда немају довољно технолошког знања да заштите његову приватност.[220] Практична остваривост права на брисање притом је посебно проблематична, јер деца млађа од 13 година чије фотографије родитељи објављују на интернету немају ни право да отворе налог на платформи на којој су објављене, ни средства да ангажују адвоката, док родитељи можда неће ни пристати да уклоне спорни садржај.[221] У теорији се, најзад, поставља и основно питање да ли је јединствена старосна граница за давање пристанка уопште исправно решење, имајући у виду да свако дете има свој јединствен когнитивни, физички, емоционални и социјални развојни пут.[222]

Уредбом (ЕУ) 2024/1183 од 11. априла 2024. године ажуриран је европски оквир дигиталног идентитета; државе чланице дужне су да најкасније до краја 2026. године

[215]N. V. Kravchuk, op. cit., стр. 80.
[216]M. Niestadt, op. cit., стр. 4.
[217]Ibid., стр. 7.
[218]Чл. 12 ст. 1 Уредбе (ЕУ) 2016/679 (Општа уредба о заштити података), op. cit.
[219]M. Niestadt, op. cit., стр. 4.
[220]S. Donovan, *'Sharenting': The Forgotten Children of the GDPR*, Peace Human Rights Governance, Vol. 4, No. 1, 2020, стр. 53, DOI: 10.14658/pupj-phrg-2020-1-2.
[221]G. F. Lendvai, op. cit., стр. 14.
[222]Општи коментар бр. 25, op. cit., тач. 71.

уведу европски новчаник дигиталног идентитета, путем кога би деца могла да доказују свој узраст приликом приступа платформама, а велике онлајн платформе дужне су да, на захтев корисника и у обиму минимално неопходних података, прихвате новчаник за аутентификацију. *EU KIDS* Act директно се надовезује на овај оквир: самим предлогом прописано је да се дефиниције које се односе на утврђивање узраста тумаче у складу са оквиром Уредбе (ЕУ) 910/2014, измењене Уредбом (ЕУ) 2024/1183, као и са Препоруком Комисије (ЕУ) 2026/1035 о заједничком оквиру за технологије верификације узраста на нивоу ЕУ.[223]

Из наведеног произлази да ГДПР, мада остаје камен темељац заштите података о личности малолетника, своју пуну функцију у дигиталном окружењу остварује само у вези са суседним оквирима, од Акта о дигиталним услугама до европског оквира дигиталног идентитета, у које су његове гаранције уграђене.

5.2. Заштита права детета на приватност према стандардима Савета Европе

Поред права Европске уније, значајан извор заштите права детета на приватност у дигиталном окружењу представљају и стандарди Савета Европе (у даљем тексту СЕ), организације која окупља 46 држава чланица, укључујући и државе које нису чланице ЕУ, попут Србије. За разлику од права ЕУ, које делује кроз директно применљиве уредбе и обавезујуће директиве, инструменти СЕ у највећем броју случајева имају карактер међународних конвенција отворених за приступање, или необавезујућих препорака и смерница упућених државама чланицама, што њиховом деловању даје другачију правну природу, али не и мањи практични значај.

Основни инструмент заштите података о личности на нивоу СЕ представља Конвенција о заштити лица у односу на аутоматску обраду личних података, модернизована Протоколом о изменама и допунама (позната као Конвенција 108+).[224] Србија је страна Конвенције 108+ и Ланзаротске конвенције,[225] које су уврштене у домаћи правни поредак, тако да ови стандарди представљају важну карику повезивања домаћег права са европским стандардима заштите података, укључујући и податке о личности деце.

---

[223]Уредба (ЕУ) 2024/1183 Европског парламента и Савета од 11. априла 2024. године о измени Уредбе (ЕУ) 910/2014 у погледу успостављања европског оквира за дигитални идентитет, Сл. лист ЕУ, L, 2024/1183, 30. 4. 2024, чл. 5a ст. 1 и чл. 5f ст. 3; преузето 19. 9. 2026, доступно на: https://eur-lex.europa.eu/eli/reg/2024/1183/oj; EU KIDS Act, op. cit., стр. 19.

[224]Савет Европе, Конвенција о заштити лица у односу на аутоматску обраду личних података са Протоколом о изменама и допунама Конвенције (Конвенција 108+), *Службени гласник Републике Србије – Међународни уговори, бр. 4/20.*

[225]Закон о потврђивању Конвенције Савета Европе о заштити деце од сексуалног искоришћавања и сексуалног злостављања, *Службени гласник РС – Међународни уговори, бр. 1/2010.*

Посебан значај за заштиту деце од најтежих облика угрожавања у дигиталном окружењу има Конвенција Савета Европе о заштити деце од сексуалног искоришћавања и сексуалног злостављања (тзв. Ланзаротска конвенција), усвојена 2007. године, чија је Србија страна.[226] Овом конвенцијом државе чланице се обавезују да инкриминишу све облике сексуалног искоришћавања и злостављања деце, како ван мреже тако и путем интернета, укључујући и свесно приступање материјалу сексуалног злостављања деце на интернету.

Комитет Ланзаротске конвенције, задужен за надзор над применом овог инструмента, у својим извештајима о мониторингу указује на драматичан пораст феномена сексуалних садржаја које деца сама генеришу и деле (*self-generated sexual material*). Према подацима на које се позива, забележен је пораст од 77% у периоду 2019–2020. године, при чему су у чак 80% случајева жртве биле девојчице узраста од 11 до 13 година,[227] што ову проблематику директно повезује са питањима обрађеним у претходном делу овог рада у контексту секстинга и малолетничке кривичне одговорности.

Кључни необавезујући инструмент специфично посвећен дигиталном окружењу представљају Смернице Савета Европе за поштовање, заштиту и остваривање права детета у дигиталном окружењу, усвојене Препоруком Комитета министара CM/Rec(2018)7.[228] Ове смернице, за које постоји и верзија прилагођена деци, пружају државама чланицама детаљан оквир за примену начела КПД у дигиталном контексту, обухватајући, између осталог, право на приватност и заштиту података о личности, а праћене су и посебним Приручником за креаторе политика, који нуди конкретне практичне кораке за њихово спровођење.

На стратешком нивоу, права детета у дигиталном окружењу представљају један од кључних приоритета важеће Стратегије Савета Европе за права детета (2022–2027), познате и као „Римска стратегија“,[229] која предвиђа синергију са одговарајућом стратегијом Европске уније о правима детета, усвајање политике „нулте толеранције“ према насиљу над децом – укључујући узнемиравање, дигитално насиље, груминг (енг.

[226]Council of Europe, *Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention),* CETS No. 201, Лансароте, 25. 10. 2007.
[227]Lanzarote Committee, извештај о мониторингу феномена сексуалних садржаја које деца сама генеришу (self-generated sexual material), 2022, стр. 42 (позивајући се, поред осталог, на: Internet Watch Foundation, *Annual Report*, налаз о порасту од 77% у периоду 2019–2020. године, при чему су у 80% случајева жртве биле девојчице узраста 11–13 година).
[228]Савет Европе, *Смернице за поштовање, заштиту и остваривање права детета у дигиталном окружењу,* Препорука CM/Rec(2018)7, Стразбур, 2018.
[229]Council of Europe, *Strategy for the Rights of the Child (2022–2027)*„Римска стратегија“, Стразбур, 2022.

grooming) и вршњачко насиље са елементима штетног сексуалног понашања, као и мере превенције зависности деце од дигиталног окружења и технологија, укључујући виртуелну реалност.

Значајну улогу у заштити права детета на приватност у дигиталном окружењу игра и Европска мрежа правобранилаца за децу (ENOC), која је 2019. године усвојила посебан став о правима детета у дигиталном окружењу, позивајући све релевантне актере да предузму одговарајуће мере ради поштовања, заштите и остваривања дечјих права, како би деца и млади могли да уживају предности и могућности које дигитално окружење пружа.[230]

Иако наведени инструменти немају обавезујућу правну снагу, они формирају стандард према коме се оцењује и домаћа пракса, што ће бити искоришћено у завршном делу рада. Стандарди СЕ, посматрани у целини, допуњују и продубљују оквир заштите успостављен на нивоу Европске уније: с једне стране, обухватају шири круг држава (укључујући и Србију, која није чланица ЕУ), а с друге стране, кроз праксу Европског суда за људска права, о којој ће бити речи у наредном одељку, добијају и обавезујућу судску димензију која допуњује претежно програмски и препоручујући карактер осталих инструмената Савета Европе.

5.3. Право детета на приватност у пракси Европског суда за људска права

Право на приватност у систему СЕ гарантује се чл. 8 Европске конвенције о заштити људских права и основних слобода (у даљем тексту: ЕКЉП). ЕКЉП је међународни уговор, али међународни уговор о људским правима, који се склапа између држава у корист индивидуалних корисника (бенефицијара), односно људи који су у надлежности држава уговорница.[231] Конвенција је у Србији ступила на снагу 3. марта 2004. године.[232]

Иако Европски суд за људска права (у даљем тексту: ЕСЉП) није до дана писања овог рада разматрао предмет који се непосредно односи на савремене изазове заштите деце у дигиталном простору, попут профилисања или шерентинга, у његовој пракси постоји низ предмета чија начела имају непосредну важност за ову тему. У наставку ћемо размотрити предмете у којима је ЕСЉП разрађивао садржину чл. 8 ЕКЉП у

[230]Европска мрежа правобранилаца за децу (ENOC), Став о правима детета у дигиталном окружењу, усвојен на 23. Општој скупштини ENOC-а, Белфаст, 27. септембар 2019.
[231]М. Настић, *Уставноправни значај Европске конвенције у правном систему Републике Србије*, у: Право Републике Србије и право Европске Уније – стање и перспективе, Зборник радова, Ниш, 2009, Правни факултет у Нишу, стр. 500–501.
[232]Закон о ратификацији Европске конвенције за заштиту људских права и основних слобода („Службени лист СЦГ – Међународни уговори“, бр. 9/2003, 5/2005 и 7/2005 – испр.; „Службени гласник РС – Међународни уговори“, бр. 12/2010 и 10/2015).

односу на дете, у три правца: заштиту лика детета, позитивне обавезе државе у дигиталном окружењу и заштиту података о личности. Постојећа пракса, мада не пружа непосредан одговор на наведене нове изазове, нуди начела која се могу извести и на њих непосредно применити.

Суд је изложио схватање да је појам приватног живота веома широк концепт, који може обухватити бројне аспекте физичког, психолошког и друштвеног идентитета, и да се нарочито односи на име и слику личности, као веома важне аспекте личног идентитета.[233]

Прву линију праксе чини заштита лика детета.

У предмету *Reklos u Davourlis против Грчке* ЕСЉП је утврдио да ефикасна заштита права на контролу сопственог лика претпоставља прибављање сагласности лица на које се то право односи већ у тренутку када се фотографија снима, а не тек када дође до њеног евентуалног објављивања. У конкретном случају, професионални фотограф клинике фотографисао је новорођенче у болничкој соби, без пристанка родитеља, и задржао негативе упркос њиховом изричитом захтеву да им се предају, тако да је лик детета остао код фотографа у форми која омогућава накнадну злоупотребу. По налажењу суда, кључно у овом предмету није било то да ли је сам фотографија била вредна или нешкодљива, него чињеница да је снимљена и задржана без сагласности родитеља, што представља повреду чл. 8 ЕКЉП.[234]

Ово начело даље је разрађено у предмету *Bogomolova против Русије*, у коме је Суд утврдио повреду чл. 8 услед објављивања фотографије детета на насловној страни брошуре центра за психолошку, медицинску и социјалну подршку, дистрибуиране у 200 примерака, без сагласности мајке. Суд је навео да чињеница да је сагласност дата само за фотографисање детета, не подразумева аутоматски и пристанак на објављивање фотографије, посебно нагласивши да објављени садржај може створити лажан утисак о породичним односима детета и тако нарушити јавну перцепцију породичне везе, будући да је фотографија објављена у брошури која позива на усвајање и да је као таква, код читалаца могла створити утисак да је дете остало без родитеља или да су га родитељи напустили.[235] Управо ова дистинкција између пристанка на снимање и пристанка на

[233]М. Вучковић, *Појам приватности у пракси Европског суда за људска права*, у: Заштита људских и мањинских права у европском правном простору, Тематски зборник радова Правног факултета у Нишу, књ. 14, Ниш, 2025, Правни факултет Универзитета у Нишу, стр. 178.
[234]*Reklos u Davourlis против Грчке*, представка бр. 1234/05, пресуда од 15. јануара 2009, пр. 40, 42, 43.
[235]*Bogomolova против Русије*, представка бр. 13812/09, пресуда од 20. јуна 2017, пр. 54.

објављивање представља правни принцип директно применљив на проблематику шерентинга, чак и ван контекста у коме је првобитно установљен.

У предмету *Dupate против Летоније* Суд је утврдио повреду чл. 8 ЕКЉП због објављивања тајно снимљених фотографија мајке са новорођенчетом док је напуштала породилиште, нагласивши инхерентно приватан карактер порођаја и довођења детета кући, због чега објављивање у конкретном случају далеко превазилази оно што се од подносиоца, и по питању познатости, могло очекивати.[236]

Линију заштите лика детета крунише пресуда у предмету *I.V.T. против Румуније*. Једанаестогодишња девојчица интервјуисана је испред своје школе поводом смрти ученице која је погинула падом из воза на школском излету, без сагласности родитеља и без присуства родитеља, пунолетног члана уже породице или наставника. Њен интервју емитован је на телевизији са националном фреквенцијом, такође без сагласности родитеља. Државни судови сматрали су да приватна телевизијска компанија која је емитовала њен интервју није прекршила њено право на приватан живот, налазећи да новинари нису поступали противправно, већ су само извештавали о случају који је био од јавног интереса.[237]

Поводом овог случаја ЕСЉП је навео да, иако је суштински циљ чл. 8 ЕКЉП заштита појединца од произвољног мешања јавних власти у право на приватан и породични живот, он не обавезује државу да се само уздржи од тог мешања. Поред ове негативне обавезе, на страни државе могу постојати и позитивне обавезе, које су неодвојиви део делотворног поштовања права на приватан и породични живот и могу подразумевати усвајање мера чији је циљ обезбеђивање поштовања приватног живота, чак и у сфери односа између самих појединаца.[238] Суд даље наглашава да су деца посебно рањива категорија лица, због чега чл. 8 и друге одредбе ЕКЉП намећу држави обавезу да узме у обзир посебну рањивост младих људи.[239] Суд је нашао да су поступајући национални судови пропустили да испитају да ли је лик подноситељке представке био делотворно заштићен, те да је претходну сагласност родитеља требало посматрати као гаранцију заштите лика подносиоца представке, а не као пуки формални захтев, јер би мајка, да је била обавештена о интервјуу, имала могућност да се успротиви.[240] Суд је при томе истакао да, чак и када извештавање доприноси расправи

[236] *Dupate против Летоније*, представка бр. 18068/11, пресуда од 19. новембра 2020, пр. 40, 56.
[237] *I.V.T. против Румуније*, представка бр. 35582/15, пресуда од 1. марта 2022, пр. 8–11, 12–17.
[238] Ibid., пр. 45.
[239] Ibid., пр. 46.
[240] Ibid., пр. 55.

од јавног интереса, откривање приватних информација, попут идентитета малолетника који је био сведок драматичног догађаја, не сме премашити границе уређивачке процене и мора бити оправдано.[241]

Овај став суда посебно је занимљив за предмет овог рада са два аспекта. Прво, у погледу шерентинга, јер суд сагласност родитеља види као гаранцију заштите лика детета, па се поставља питање шта када су управо родитељи ти који користе лик детета за снимање и објављивање садржаја на друштвеним мрежама. Друго, овај став указује да је и у случају интервјуисања малолетне деце која су била ученице школе „Владислав Рибникар“ у Београду, а који су непосредно након пуцњаве интервјуисани испред школе (види одељак 4.1.5), дошло до потенцијалне повреде чл. 8 ЕКЉП. По нашем мишљењу, у конкретним околностима извештавања о пуцњави постојала је основана сумња да је извештавање погодило право на приватност укључених малолетника у смислу чл. 8 ЕКЉП, имајући у виду да суд налази да извештавање о драматичним догађајима који се дешавају око малолетника или их непосредно укључују захтева од пружалаца услуга аудиовизуелних медија да испуне своју дужност информисања јавности уз истовремену заштиту идентитета укључених малолетника.[242] Наведени захтеви су од највећег значаја у случајевима медијског извештавања који се односе на малолетну децу, будући да би откривање информација о њиховом идентитету могло угрозити достојанство и добробит детета у још већој мери него у случају пунолетних лица, имајући у виду њихову већу рањивост, због које је потребна посебна правна заштита.[243]

Наведени предмети утврђују да заштита лика детета не почиње тек при објављивању садржаја, него у тренутку снимања, и да родитељска сагласност, где је она потребна, има функцију стварне заштите детета, а не формалности.

Другу линију праксе чине позитивне обавезе државе у дигиталном окружењу. У предмету *K.U. против Финске*[244] Суд је утврдио повреду чл. 8 због тога што домаћи законодавни оквир није омогућио идентификовање лица које је анонимно објавило сексуално оријентисани оглас о дванаестогодишњаку на сајту за упознавање, истичући да деца и друга рањива лица имају право на државну заштиту у облику ефикасне одвраћајуће заштите од тешких задирања у суштинске аспекте приватног живота, те да

[241] Ibid., пр. 56.
[242] Ibid., пр. 56.
[243] Ibid., пр. 58–59.
[244] *K.U. против Финске*, представка бр. 2872/02, пресуда од 2. децембра 2008.

државе не могу да се позивају на то да нису имале прилику да обезбеде механизам идентификовања починиоца, узимајући у обзир анонимни карактер интернета.[245]

У предмету *Söderman против Шведске*, пресудом Великог већа од 12. новембра 2013. године, ЕСЉП је утврдио да законодавни оквир у времену настанка догађаја није обезбедио заштиту четрнаестогодишњакиње, чији је очух у купатилу породичног стана скривено поставио видео камеру у намери да је сними током пресвлачења, будући да ни кривичне ни грађанске одредбе тадашњег шведског права нису покривале тајно снимање без сагласности. Суд је поновио да мере државе за заштиту деце, као посебно рањиве групе, морају да буду ефикасне и да укључују разумне кораке превенције и ефикасну одвраћајућу заштиту од озбиљних прекршаја личног интегритета.[246]

Да се позитивне обавезе државе протежу и на насиље остварено дигиталним средствима, ЕСЉП је потврдио у предмету *Volodina (бр. 2) против Русије*. Подноситељка представке, пунолетно лице, годинама је била изложена дигиталном насиљу свог бившег партнера, који је без њене сагласности објављивао њене интимне фотографије, пратио је помоћу ГПС-а и креирао лажне профиле на друштвеним мрежама под њеним именом. ЕСЉП је у овом случају утврдио да се позитивна обавеза државе примењује на све облике насиља, без обзира да ли се дешавају офлајн или онлајн, те да је у конкретном случају држава пропустила да ефикасно заштити подноситељку представке и истражи пријављене радње, позивајући се при том и на предмет *K.U. против Финске* у делу којим се позитивне обавезе државе протежу и на делотворност кривичне истраге.[247]

Трећу линију пресуда чини заштита података о личности. У предмету *Авилкина и др. против Русије*, приликом истраге о законитости рада верске организације, тужилаштво је затражило од болница у региону да га обавести о сваком случају одбијања трансфузије крви из верских разлога, након чега су болнице открите медицинску документацију подносилаца представке, међу којима је било и малолетника. Суд је заштиту личних, укључујући и медицинских, података квалификовао као питање од фундаменталног значаја за уживање права на приватни и породични живот, а откривање таквих података у конкретном случају оценио као непропорционално.[248]

Наведене линије праксе обухватају најразличитије појаве угрожавања приватности детета у дигиталном простору: анонимно објављивање података о детету на интернету,

[245]Ibid., пр. 46-49; о предмету видети: N. V. Kravchuk, *op. cit*., стр. 80.
[246]*Söderman против Шведске*, представка бр. 5786/08, пресуда од 12. новембра 2013, пр. 81–82, 117.
[247]*Volodina (бр. 2) против Русије*, представка бр. 40419/19, пресуда од 14. септембра 2021, пр. 49.
[248]*Авилкина и др. против Русије*, представка бр. 1585/09, пресуда од 6. јуна 2013, пр. 27, 32, 45.

тајно снимање, снимање и објављивање лика детета од стране трећих лица и институција, дигитално насиље и обраду података о личности. Ипак, у литератури се указује на то да пракса Суда, посматрана у целини, још увек нема кохерентан, свеобухватан приступ интернету као новом простору за остваривање људских права и да показује значајне празнине управо у областима заштите података о личности и понашања приватних (недржавних) актера; у том смислу се указује да би државе, на основу чл. 8, могле да одговарају и за понашање приватних лица, укључујући пружаоце дигиталних услуга и родитеље, при злоупотреби података о деци.[249] Празнина је нарочито видљива у односу на новије појаве, међу којима је најизраженија родитељско дељење садржаја о деци путем друштвених мрежа (шерентинг), која до сада није била предмет непосредног разматрања ЕСЉП-а. Отуда се поставља питање да ли се начела успостављена у наведеним предметима, пре свега неопходност пристанка на објављивање, независно од пристанка на снимање, и заштита јавне перцепције породичних односа детета, могу по аналогији применити и на ту праксу, уколико би се пред Судом нашао одговарајући предмет.

Из наведеног произлази да Европски суд за људска права доследно потврђује постојање позитивних обавеза државе у погледу заштите приватности детета у дигиталном простору, али да је пракса Суда, у односу на брзину технолошког развоја и нове облике угрожавања приватности, још увек у изградњи, што оставља простор и за даљу научну анализу и за развој те праксе у наредном периоду.

6. УПОРЕДНА АНАЛИЗА И МОГУЋИ ПРАВЦИ ЗАШТИТЕ

6.1. Заједнички стандарди и положај Републике Србије

Упоредни преглед спроведен у претходним поглављима омогућава да се положај Републике Србије оцени у три равни: у односу на правне системе држава бивше Југославије, у односу на стандарде Европске уније и Савета Европе и у односу на праксу Европског суда за људска права.

У првој равни, решење домаћег законодавца налази се у оквиру заједничког стандарда посматраних система: старосна граница од 15 година за самостално давање пристанка обухваћена је простором који ГДПР оставља државама, а обавеза руковаоца да провери да ли је пристанак дао законски заступник приближава српско право решењима Босне и Херцеговине и Северне Македоније, у којима је формална

[249]R. Greco, *Children's Right to Privacy in the Digital Age: Is the ECtHR's Current Approach up to the New Challenges?*, Diritti umani e diritto internazionale, бр. 3, 2024, стр. 573, DOI: 10.12829/115907.

претпоставка родитељске сагласности замењена обавезом провере њеног постојања, мада, како је уочено, без јасно утврђених критеријума (видети одељак 4.3.). Разлике у одабиру границе, како је већ закључено, показују се као питање националног опредељења, а не питање нивоа заштите. Истовремено, одсуство изричитог уређења шерентинга заједничко је за све посматране системе, што упућује на закључак да празнина у заштити приватности детета у дигиталном простору није везана за појединачни правни систем, него произлази из начина на који су ови системи, под истим европским стандардом, институционално структурирани.

У односу на право ЕУ, слика је мање једноставна него што би сугерисао висок степен нормативне усклађености ЗЗПЛ-а са ГДПР-ом, који потврђује и извештај Европске комисије за 2025. годину, при чему је измена закона већ у поступку (видети одељак 4.1.2.).[250] Наиме, европски оквир више није само оквир заштите података о личности: на првобитни слој, у којем се заштита детета постиже кроз правила о законитости обраде и услове пристанка, надоградили су се обавезе пружалаца услуга онлајн платформи по чл. 28 ДСА, укључујући и забрану огласа заснованих на профилисању малолетника, а најновији слој представља EU KIDS Act, са хармонизованом старосном границом од 15 година, режимом одлагања приступа и захтевима за утврђивање узраста. Правни оквир Србије остаје, по основним цртама, у оквиру првог слоја, тако да питања попут профилисања деце, зависничког дизајна и обавеза платформи према малолетницима у домаћем праву немају посебан режим, већ се, уколико су уопште обухваћена, решавају општим правилима о заштити података, породичноправним и медијским механизмима, а тек када досегну праг кривичне одговорности, кривичноправним механизмима. У том смислу, разлика између српског и европског оквира не огледа се пре свега у степену усклађености постојећих закона, већ у томе што европски оквир детету нуди више различитих механизама заштите, од забране профилисања до одлагања приступа, док домаћи оквир на то питање одговара само основним правилима о заштити података.[251]

Стандарди СЕ, за разлику од права ЕУ, делују пре свега кроз конвенције отворене за приступање и необавезујуће инструменте, а Србија је, као страна и Конвенције 108+ и Ланзаротске конвенције, у њихов систем укључена. Одсуство обавезујуће снаге смерница СЕ за права детета у дигиталном окружењу не значи, међутим, да оне немају правну функцију: пружају детаљан оквир за примену начела КПД у дигиталном

[250]Европска комисија, Serbia 2025 Report, op. cit., стр. 39.
[251]M. Niestadt, op. cit., стр. 4; EU KIDS Act, op. cit., стр. 45–49 и 61–63.

окружењу, укључујући право на приватност и заштиту података о личности детета – начела која у сродним правцима разрађује и пракса ЕСЉП кроз чл. 8 ЕКЉП, а која Општи коментар бр. 25 конкретизује: тачка 71 везује пристанак за узраст и еволуирајућу способност детета, а тачка 72 за право детета да приступи, исправи и избрише податке о себи. Практични значај тих инструмената за Србију лежи управо у томе што нуде спреман оквир за процену домаћег решења без потребе да се домаћи законодавац ослања искључиво на модели других држава чланица ЕУ.

Пракса ЕСЉП додаје овом оквиру и обавезујућу судску димензију (видети одељак 5.3.). Начела разрађена у линији заштите лика детета, пре свега да заштита лика не почиње тек приликом објављивања садржаја него у тренутку снимања и да родитељска сагласност има функцију стварне заштите детета, а не формалности, по аналогији су директно применљива на шерентинг, иако ЕСЉП није разматрао предмет који би тај феномен непосредно обухватио. У том погледу, пресуда Врховног касационог суда Рев. 14012/2022, којом је, након израженог противљења родитеља коме је поверено вршење родитељског права, даље објављивање фотографија детета оцењено као несагласно са најбољим интересом детета, налази се у истом правцу са праксом ЕСЉП, али и показује њену границу: српски суд је заштиту остварио на основу става родитеља коме је родитељско право поверено, док француско законодавно решење, којим је дете укључено у одлучивање о свом лику сразмерно његовом узрасту и зрелости, то питање већ изводи из искључиве воље једног родитеља.[252] Уз то, линија позитивних обавеза државе, од предмета *K.U. против Финске* до *Volodina (бр. 2) против Русије*, налаже да ефикасна одвраћајућа заштита обухвати и насиље остварено дигиталним средствима, а институционална пракса Србије, од случаја „Здравитас“ до извештавања о трагедији у Основној школи „Владислав Рибникар“, показује да та обавеза у пракси остаје најслабије испуњена управо тамо где за повреду нису одговорни само приватни актери, већ и носиоци јавних функција.[253]

Из три наведене равни произлази слика положаја Србије која је, на нормативном плану, блиска посматраним системима, али која у погледу механизама који би тај стандард учинили стварним остаје у оквиру првог, најосновнијег слоја европског развоја, оквира заштите података, без посебних механизама за платформе. Које су то конкретне празнине и како би се могле затворити, биће показано у наставку.

[252]R. Greco, op. cit., стр. 573; Пресуда Врховног касационог суда Републике Србије, Рев. 14012/2022 од 6. 10. 2022. године.
[253]Повереник за информације од јавног значаја и заштиту података о личности, Саопштење: „Здравитас“, op. cit.; BIRN Србија, Invazija na privatnost: Analiza medijskog izveštavanja, op. cit., стр. 4, 5 и 22.

6.2. Структурне празнине заштите

Најпре, прву празнину чини одсуство изричитог уређења шерентинга, а њено најважније обележје јесте то што није празнина појединачног система, него свих посматраних система. ГДПР, кроз изузетак обраде у оквиру личних или породичних активности, практично оставља дељење садржаја о детету од стране родитеља изван свог делокруга, и одлуку о подацима који се о детету објављују препушта у потпуности родитељима, без механизма којим би се у конкретном случају проверавало да ли је таква одлука у складу са најбољим интересом детета; у литератури се притом указује и да оквир уопште не узима у обзир да родитељи не поступају увек у том интересу. Није, дакле, у питању да се родитељима одузме могућност одлучивања о сопственом детету, него да онда када објављивање није у складу са његовим најбољим интересом постоји расположив механизам заштите, и управо такав механизам недостаје. Право на брисање, које се у литератури најчешће наводи као одговор на овај феномен, у пракси је детету у најрањивијем узрасту недоступно: дете млађе од старосне границе коју платформа поставља не може законски да отвори налог на којем би то право остварило, нити располаже средствима да заштитним механизмима приступи самостално. Посматрано у целини, у посматраном кругу држава ниједан законодавац није увео изричито уређење шерентинга, без обзира да ли користи сам појам; једино познато изузетно решење остаје француско, које, међутим, није било предмет упоредног прегледа (видети одељак 3.2), а ни пракса ЕСЉП-а овај феномен није непосредно обухватила, тако да се у највећем делу посматраног простора заштита приватности детета код шерентинга зависи од воље онога ко тај ризик најчешће и ствара, родитеља.[254]

Другу празнину чини одсуство ефикасног надзора над обрадом података малолетника коју врше приватна лица, у ситуацијама у којима понашање не досеже праг кривичне одговорности. Пракса црногорске Агенције, која је поводом обраде података малолетника од стране инфлуенсера констатовала да нема законску надлежност да поступа (видети одељак 4.2.4.), показује да се у таквим ситуацијама заштита ослања углавном на кривичноправне механизме и поступање тужилаштва, органа који делује тек када понашање досегне праг кривичне одговорности. Све оно што се одвија испод тог прага, од свакодневног родитељског дељења до објављивања садржаја о детету од стране лица која нису његови законски заступници, чини најмасовнији део проблема и

[254]S. Donovan, op. cit., стр. 53; G. F. Lendvai, op. cit., стр. 14; G. F. Lendvai, K. Ambrazevičiūtė, op. cit.; O. Akay, op. cit.; N. V. Kravchuk, op. cit., стр. 2 и 15.

остаје без ефикасног надзора. Тиме се, међутим, не пориче постојање надзорних органа нити њихових општих овлашћења; празнина се састоји у томе што та овлашћења на пољу обраде података од стране приватних лица у дигиталном окружењу нису конкретизована ни остварена као устаљена пракса, тако да је надзор у том делу епизодичан и углавном реактиван.

Трећа празнина односи се на најновији слој европске заштите, изграђен на одлагању приступа и утврђивању узраста, чија је усклађеност са основним правима детета још увек неутврђена. Од Смерница усвојених у складу са чл. 28 ст. 4 ДСА до EU KIDS Act-а, овај слој се ослања управо на та два механизма, док литература показује да је утврђивање узраста у пракси често неефикасно у заштити деце од дигиталног ризика, а да истовремено угрожава њихова друга права: право на недискриминацију, приватност, право да буде саслушано и грађанска права, погађајући најтеже управо децу која не располажу документима, картицама или средствима електронске идентификације. Налаз студије Саса и Милберга да тренутно не постоји метод утврђивања узраста који би адекватно штитио основна права доводи у сумњу и да ли је европским оквиром уопште постигнут склад између онлајн безбедности и заштите података, а уставноправни налаз државе чланице о несразмерности генералне забране потврђује да граница тог механизма није теоријска, него практична. Отуда следи закључак који ће бити од значаја за наставак излагања: усклађивање са најновијим слојем европског развоја не може се третирати као самостална гаранција заштите, будући да је и сам тај слој у напетости са правима чију заштиту проглашава.[255]

Четврту празнину чини пракса, која реагује, али не гради стандард. Пресуда Врховног касационог суда Рев. 14012/2022 заштиту лика детета остварила је кроз општа начела породичног права и начело најбољег интереса детета, без разрађеног стандарда који би наредним случајевима давао предвидив оквир, а институционална пракса Србије, како је утврђено у одељку 4.1.5., остаје фрагментарна, реактивна и неуједначена, при чему се заштита активира тек када је покрену дете или његова породица. Заштита која чека иницијативу оштећеног, у области у којој је оштећено лице најчешће малолетно и без правних средстава да поступа, по свом дејству се не разликује од одсуства заштите.[256]

[255]S. Livingstone и др., op. cit., стр. 721 и 730; M. Sas, J. T. Mühlberg, op. cit., стр. 7; S. Stalla-Bourdillon, op. cit.; S. Volz, op. cit.; Conseil constitutionnel, Décision n° 2026-911 DC, op. cit.
[256]Пресуда Врховног касационог суда Републике Србије, Рев. 14012/2022 од 6. 10. 2022. године.

Из наведених празнина произлази закључак који носи овај одељак: празнине у заштити приватности детета у дигиталном простору нису појединачни недостаци појединих прописа, него последица самог начина на који су посматрани системи, под истим европским стандардом, организовани. Постојећи механизми нису намењени деловању према приватним актерима, нити се активирају без иницијативе самих оштећених, док најновији слој европског развоја, управо у тренутку када га усклађивање преноси у домаће право, носи напетост између заштите и основних права детета. Тиме се потврђује прва хипотеза овог рада: постојећи механизми препознају право детета на приватност, али не обезбеђују у потпуности ефикасну заштиту тог права. Питање које следи није, дакле, да ли стандарди постоје, него како се њихова преносивост у домаћи правни поредак може остварити тако да празнине буду затворене, а не пренете.

6.3. Могући правци заштите

Из празнина изложених у претходном одељку изводе се правци заштите који почивају на материјалу разматраном у поглављима 4 и 5, при чему прва четири правца одговарају на конкретне празнине, а пети их допуњава као системски слој.

Први правац односи се на изричито уређење шерентинга, као одговор на прву празнину. Искуство Француске показује да решење не захтева укидање родитељског права, него његово уоквиравање обавезама: право родитеља остаје очувано, али се одлучивање о употреби лика детета веже за учешће детета сразмерно његовом узрасту и зрелости, сваки од родитеља добија право да од суда затражи забрану објављивања које угрожава достојанство детета, а зарада од комерцијалног коришћења лика детета уплаћује се на рачун отворен на име детета (видети одељак 3.2.). У прилог таквом правцу иду и Лендваијеве смернице, упућене родитељима и регулаторним органима, које овај рад између осталог прихвата: механизам за уклањање интимних, неадекватних или срамотних фотографија које објављују родитељи, и пооштрење регулативе шерентинга инфлуенсера, поља на којем се комерцијално искоришћавање лика детета одвија практично без ограничења, без учешћа детета у одлуци и без удела у добити. На ту линију се надовезује и надзорна пракса Словеније и Хрватске: Информациони повереник Словеније у својим мишљењима расправља објављивање фотографија малолетне деце на интернету, повезујући то питање са вршењем родитељске бриге, а AZOP је објављивању видео-садржаја о деци посветио посебну препоруку (видети одељке 4.2.1. и 4.2.2.), док италијански предлози покушавају са уклањањем садржаја

(видети одељак 3.2.). Ни у једном посматраном систему, међутим, овај низ није затворен у целини: француско решење покрива одлучивање, словеначка и хрватска надзорна пракса покривају питање објављивања фотографија и видео-садржаја о деци, а италијански предлози покушавају са уклањањем, тако да упоредни материјал нуди решење за сваки појединачни елемент, али не и модел целине, из чега произлази да би уређење шерентинга, где год га будући законодавац прихватио, морало бити састављено из појединачних модела, а не преписано из једног система.[257]

Други правац односи се на обавезе пружалаца дигиталних услуга и платформи, као одговор на другу празнину, одсуство ефикасног надзора над обрадом података малолетника коју врше приватна лица. Пракса примене чл. 28 ДСА, поткрепљена Смерницама о примени тог члана и конкретним резултатима спровођења, показала је да обавезе пружаоцима могу имати стварни ефекат, од забране огласа заснованих на профилисању малолетника до поступака против највећих друштвених мрежа поводом зависничког дизајна. По оцењивању у овом раду, смисао тог развоја јесте померање терета одговорности: одговорност за заштиту малолетника преноси се са, које се не може самостално заштитити, на платформу, која услове обраде поставља самим дизајном својих услуга. Тамо где такве обавезе немају изричито место у националном праву, из ове праксе изводе се два стандарда: мере безбедности и приватности малолетника уграђене у дизајн услуге и подразумевана подешавања на највишем нивоу заштите, уз уздржавање од профилисања малолетника у комерцијалне сврхе. Увођење обавеза, међутим, није довољно само по себи: обавеза остаје програмска ако санкција не одвраћа, а највећи пружаоци услуга казну често плаћају као трошак пословања у ситуацијама кад профит који остварују надмашује њен износ. Надаље, надзорни органи располажу знатно мањим људским и техничким ресурсима од највећих пружалаца услуга, тако да ће тек њихово стварно деловање показати колики је стварни домет тог механизма. Зато правац унапређења није само у увођењу обавеза, него и у санкционисању које би било ефикасно, сразмерно и одвраћајуће.[258]

Трећи правац односи се на утврђивање узраста на основу заједничких европских решења, као одговор на трећу празнину. Уредбом (ЕУ) 2024/1183 државе чланице дужне су да најкасније до краја 2026. године уведу европски новчаник дигиталног идентитета, путем кога би деца могла да доказују узраст приликом приступа

[257]G. F. Lendvai, op. cit., стр. 15–17; Loi n° 2024-120, op. cit.; Loi n° 2020-1266, op. cit.
[258]M. Niestadt, op. cit., стр. 4; Европска комисија, Смернице о мерама за обезбеђивање високог нивоа приватности, безбедности и сигурности малолетника на интернету, op. cit.

платформама. Предлог EU KIDS Act-а за спровођење одлагања приступа предвиђа коришћење сертификованих решења независних од платформи, укључујући ЕУ апликацију за проверу узраста и европски новчаник дигиталног идентитета: доказ о узрасту издаје независно треће лице, примењује се технологија доказа са нултим знањем, а таква решења не смеју да послуже за идентификовање, праћење или профилисање корисника. Заједнички оквир за технологије верификације узраста уређен је, притом, Препоруком Комисије (ЕУ) 2026/1035. Законодавац, дакле, без обзира да ли делује на националном нивоу или на нивоу ЕУ, не би требало да преписује техничка решења која још нису у примени, него да у правни стандард унесе оно што из њих следи: да утврђивање узраста не сме да буде мање заштитно од саме забране обраде података без пристанка и да решења утврђивања узраста не постану нови канал за обраду података детета. Овај правац, притом, мора да носи и напомену о пропорционалности, разрађену у одељку 5.1.2.: мера утврђивања узраста оправдана је само ако стварно смањује конкретан ризик, ако је неопходна и најмање инвазиван од расположивих начина и ако су последице по приватност, недискриминацију и приступ деце дигиталним услугама сведене на најмању меру, уз процену утицаја на права детета и учешће деце у осмишљавању самог решења.[259]

Четврти правац односи се на позитивне обавезе државе према приватним актерима, као одговор на то да се механизми заштите не активирају без иницијативе оштећених. Линија праксе ЕСЉП-а од предмета *K.U. против Финске* до *Volodina (бр. 2) против Русије* налаже да ефикасна одвраћајућа заштита обухвати и насиље остварено дигиталним средствима, а у литератури се изводи да би државе, на основу чл. 8 Конвенције, могле да одговарају и за понашање приватних лица, укључујући пружаоце дигиталних услуга и родитеље, при злоупотреби података о деци. Овај правац, притом, има и унутрашњу димензију коју је показала домаћа пракса: када су за повреду приватности малолетника одговорни и носиоци јавних функција, као у случају „Здравитас“ и извештавања о трагедији у Основној школи „Владислав Рибникар“, питање није само у обавезивању приватних лица, него и у доследности државе према стандардима које сама проглашава, јер заштита коју држава не остварује према себи тешко ће бити остварива према другима.[260]

[259]Уредба (ЕУ) 2024/1183, op. cit.; EU KIDS Act, op. cit., стр. 61–63; Препорука Комисије (ЕУ) 2026/1035, op. cit.; S. Livingstone и др., op. cit., стр. 730 и 738; S. Stalla-Bourdillon, op. cit.
[260]R. Greco, op. cit., стр. 573–599; K.U. против Финске, op. cit.; Volodina (бр. 2) против Русије, op. cit.

Пети правац односи се на едукацију, као слој који није посебан правни механизам, него системски услов да остали правци делују. По оцењивању у овом раду, ни најстрожа забрана ни најсавршенија регулатива не могу сами по себи да обезбеде трајну заштиту. Колико год правила била прецизна, она остају екстерно ограничење све док деца и лица у њиховом окружењу не схвате да су подаци о личности у дигиталном свету трајни, рањиви и лако злоупотребљиви, и да се њима мора управљати свесно, у складу са стандардима заштите. Управо зато што деца, како је утврђено у одељку 5.1.1., проналазе креативне начине да заобиђу наметнута правила, забрана без едукативног слоја не уклања ризик, него га помера у мање заштићене просторе. Едукација, притом, у овом раду није начин да се терет заштите пренесе на дете. Како је изложено у трећем поглављу, од деце се не може разумно очекивати да у потпуности разумеју и самостално управљају својим подацима, па терет остаје подељен између регулаторних и техничких механизама и едукативног слоја. Правац едукације обухвата, стога, не само децу, него и родитеље, старатеље и институције које долазе у непосредни контакт са децом, пре свега школу, којој је у трећем поглављу приписана посебна одговорност за узрасту прилагођено информисање деце о подацима који се о њима прикупљају. За такав слој постоји и спреман међународни оквир: Смернице Савета Европе за права детета у дигиталном окружењу, које постоје и у верзији прилагођеној самим деци, уз Приручник за креаторе политика, став Европске мреже правобранилаца за децу и Стратегију Савета Европе за права детета, уз захтев Општег коментара бр. 25 да информисање деце буде на језику прилагођеном њиховом узрасту. Налаз одељка 5.2. остаје у снази: едукација није алтернатива регулативи, него њена неопходна допуна.[261]

Најзад, сви наведени правци морају да прођу кроз начело пропорционалности, јер развој последњих година показује и смер који треба избећи. Неизвршавање француског закона о дигиталном пунолетству и укидање кључне одредбе закона из 2026. године пред Уставним саветом Француске потврдили су у пракси оно на шта је литература упозорила: генерална забрана приступа, без обзира на узраст, зрелост и ситуацију појединог детета, несразмерна је и не даје законске гаранције заштите приватности(видети одељак 5.1.1.). Заштита детета која потискује његову аутономију није решење, него друга врста истог проблема, и управо зато правци унапређења иду у правцу циљаних, ризику прилагођених мера, уз узрасту прилагођено информисање

[261]Смернице Савета Европе за поштовање, заштиту и остваривање права детета у дигиталном окружењу, op. cit.; C. Nyst, op. cit., стр. 11–12; Европска мрежа правобранилаца за децу (ENOC), op. cit.; Стратегија Савета Европе за права детета (2022–2027), op. cit.; Општи коментар бр. 25, op. cit.

деце о обради њихових података, учешће деце у одлукама које их се тичу и образовање које развија свест о вредности личних података, чиме се постиже оно што генералне забране не могу: заштита детета која не потискује његову аутономију, него је постепено оспособљава. Како би наведени правци могли да се остваре у домаћем правном поретку, биће показано у наставку.

6.4. Могући правци унапређења за Републику Србију

Правци изложени у претходном одељку остварују се у домаћем правном поретку кроз конкретне мере, при чему се утврђене празнине у домаћи оквир не преносе, него затварају.

Први правац односи се на измене ЗЗПЛ-а у правцу конкретизације провере пристанка законског заступника. Како је утврђено у одељку 4.1.2., упућивање на „разумне мере“ оставља руковаоцима висок степен дискреционог овлашћења и може довести до неуједначене праксе у којој се сврха одредбе сведе на формално испуњење нормативног захтева, због чега сматрамо да законодавац треба да утврди барем минимални стандард поступања у погледу провере идентитета и овлашћења лица које даје пристанак. Оцена извештаја Европске комисије из 2025. године да је закон углавном усклађен, уз најаву измена, чини ту измену најприроднијим местом за такав стандард, нарочито будући да и Нацрт измена ЗЗПЛ-а, који је у поступку усвајања, већ изричито посебно третира малолетна лица и право на брисање података (видети одељак 4.1.2.). Сматрамо да измена не би требало да преписује техничка решења која још нису у примени, него да унесе оно што из њих следи као правни стандард, разрађен у претходном одељку: да провера пристанка не сме бити мање заштитна од саме забране обраде без пристанка. Пропуштање те измене не би само одложило уређење, него би одржало и онај део празнине који се праксом не може надоместити.[262]

Други правац односи се на изричито уређење шерентинга, које, како је показано, мора бити састављено из појединачних модела, а не преписано из једног система. Француско решење нуди елемент одлучивања: дете се укључује у одлучивање о употреби свог лика сразмерно свом узрасту и зрелости, што је у директној вези са начелом развојних способности из чл. 65 ПЗ, које Општи коментар бр. 25 разрађује за дигитално окружење. У исто време, овакво решење ублажава границу домаћег приступа коју је показала пресуда Врховног касационог суда, а која се огледа у зависности

[262]Нацрт Закона о заштити података о личности, op. cit.; чл. 16. Закона о заштити података о личности, *Службени гласник РС, бр. 87/2018.*

заштите детета од става родитеља коме је поверено вршење родитељског права. Механизам уклањања интимних, неадекватних или срамотних фотографија које објављују родитељи, уз пооштрење регулативе шерентинга инфлуенсера, пружа елемент уклањања, а словеначка и хрватска надзорна пракса показују да елемент преобликовања обраде може постојати и без измене закона, кроз тумачење надзорног органа. Најмање инвазиван корак, који ниједан посматран систем осим Црне Горе није учинио, представља пренос црногорског критеријума: изричито везивање обраде података малолетника за његов најбољи интерес, чиме би се на нивоу ЗЗПЛ-а отворио простор за контролу и родитељске сагласности у случајевима шерентинга. Састављено тако, уређење би обухватило одлучивање, уклањање и преобликовање, а био би и први покушај систематског уређења тог феномена у посматраном кругу држава, будући да је управо у том пољу упоредни материјал показао да ниједан посматран систем није затворио целину.[263]

Трећи правац односи се на јачање институционалног механизма заштите. Поука из црногорске праксе, да надзорни орган без изричитих овлашћења према приватним актерима остаје без законског инструмента да поступи управо на пољу на којем се угрожавање приватности детета највише одвија, указује да треба изричито утврдити обим Поверенкових овлашћења у дигиталном окружењу, пре свега поступање по питањима обраде података малолетника од стране приватних лица, јер управо тај орган, а не тужилаштво, располаже средствима за деловање испод прага кривичне одговорности. Тиме се не стварају нове надлежности, него изричито уређује оно што ЗЗПЛ већ покрива општим правилима, а што, како је утврђено у одељку 6.2., у пракси остаје епизодично и реактивно. У том правцу спада и оно што је анализа случаја „Здравитас" показала као питање инспекцијског надзора: формална провера законитости обраде не обухвата неопходност и сразмерност обраде, тако да надзор остаје без ефикасног инструмента и када су формални услови испуњени. Најзад, правац унапређења у делу медијског извештавања о малолетницима није у изградњи нових механизама него у доследној примени постојећих (видети одељак 4.1.5.): ЗЕМ-а, Правилника о заштити права малолетника у области пружања медијских услуга, праксе РЕМ-а и захтева за спровођењем допунског надзора, уз стварне последице по оне који одредбе крше. Линија позитивних обавеза из праксе ЕСЉП-а и налаз о извештавању

[263]G. F. Lendvai, op. cit., стр. 14, 15 и 17; чл. 65. ПЗ; Комитет за права детета УН, Општи коментар бр. 25, op. cit., тач. 19, 20 и 76; чл. 10 ст.2 и чл. 12 Закона о заштити података о личности (*Службени лист Црне Горе, бр. 79/2008 и 77/2024*).

после трагедије у Основној школи „Владислав Рибникар“ чине ово питањем ефикасности, а не одсуства прописа.[264]

Четврти правац односи се на едукативни слој заштите, као услов делотворности свега наведеног. Правни механизми, колико год били савршено уређени, не затварају празнину коју креативност корисника ствара, деца проналазе начине да заобиђу наметнута правила, а родитељи, старатељи и институције у непосредном контакту са децом, од школа до здравствених служби, често не располажу ни знањем ни алатима да препознају ризике обраде података детета. Зато едукација мора да обухвати све ове субјекте, а не само децу, и да иста буде узрасту прилагођена, у складу са захтевом из Општег коментара бр. 25 да информисање деце буде на језику прилагођеном њиховом узрасту, као и са Смерницама Савета Европе, које за то постоје и у верзији прилагођеној деци. Најзад, по оцењивању у овом раду, едукативни слој треба да обухвати и правосудне органе. Пресуда Врховног касационог суда показала је да судови реагују кроз општа начела, делимично управо зато што не располажу разрађеним стандардом за питања приватности детета у дигиталном простору, тако да изградња тог стандарда, кроз праксу, смернице или стручно усавршавање, није техничко питање него услов да судска заштита престане да буде реактивна и неуједначена, како је утврђено у одељку 4.1.5.[265]

Из наведеног произлази да унапређење српског правног оквира не захтева нови партикуларни закон за сваку појаву, него неколико усмерених измена: стандард провере пристанка, уређење шерентинга састављено из појединачних модела, изричито уређење Поверенкових овлашћења у дигиталном окружењу и едукативни слој који обухвата и правосудне органе. Свака од тих мера има узор у посматраним системима, а ниједна не зависи од технолошког развоја или будућих европских аката. Домаћи законодавац, дакле, не чека на изворе права, него на одлуку.

7. ЗАКЉУЧНА РАЗМАТРАЊА

Истраживање у овом раду полазило је од питања у којој мери постојећи међународни, европски, упоредноправни и национални правни механизми обезбеђују ефикасну заштиту права детета на приватност у дигиталном простору, и који су могући

[264]Повереник за информације од јавног значаја и заштиту података о личности, Саопштење: „Здравитас“, op. cit.; Синдикат образовања Србије, Захтев Поверенику за спровођење допунског надзора примене ЗЗПЛ у оквиру пројекта „Здравитас“, op. cit.; BIRN Србија, op. cit., стр. 4, 5 и 22.

[265]Комитет за права детета УН, Општи коментар бр. 25, op. cit.; Смернице Савета Европе за поштовање, заштиту и остваривање права детета у дигиталном окружењу, op. cit.; A. Tasić, op. cit., стр. 96–97; Пресуда Врховног касационог суда Републике Србије, Рев. 14012/2022 од 6. 10. 2022. године.

правци унапређења те заштите. Одговор који анализа омогућава може се изложити у једној реченици: механизми заштите постоје на свим посматраним нивоима, али нису прилагођени оним ризицима који приватност детета у дигиталном простору данас највише угрожавају, нису намењени деловању према приватним актерима и најчешће се активирају по иницијативи самог оштећеног.

Прва хипотеза рада, да постојећи правни оквири препознају право детета на приватност у дигиталном простору, али да механизми заштите не обезбеђују у потпуности ефикасну заштиту тог права, потврђена је у целости. Посматране системе повезује висок степен нормативне усклађености са ГДПР-ом, а одвајају их старосне границе које су питање националног опредељења у оквирима које Уредба оставља државама. Празнине, међутим, нису појединачни недостаци прописа, него последица самог начина на који су посматрани системи, под истим европским стандардом, организовани: шерентинг није изричито уређен ни на једном нивоу, надзорни органи располажу општим овлашћењима, али она према обради података од стране приватних лица у дигиталном окружењу нису конкретизована ни остварена као устаљена пракса, утврђивање узраста, на које почива најновији слој европског развоја, носи напетост између заштите и основних права детета, а судска и институционална пракса реагују, али кроз општа начела и тек по иницијативи оштећеног.

Друга хипотеза, да ефикасна заштита захтева равнотежу између права и одговорности родитеља и права детета на развој аутономије и одлучивања сразмерно узрасту и зрелости, потврђена је, и то у свом најстрожем значењу. Равнотежа се не успоставља оснаживањем детета само по себи, нити повећањем старосне границе, него оквиром у којем одлука родитеља није последња реч: кроз укључивање детета у одлучивање о употреби свог лика сразмерно његовом узрасту и зрелости, како француско решење то већ чини, и кроз везивање обраде података малолетника за његов најбољи интерес, како је јединствено учинило црногорско законодавство. Пресуда Врховног касационог суда Рев. 14012/2022 показала је, у истом правцу, где домаћи оквир застаје: заштита детета зависи од става родитеља коме је поверено вршење родитељског права, иако је управо родитељ, у контексту шерентинга, најчешће онај ко тај ризик и ствара.

Трећа хипотеза, да постојећи правни оквир Републике Србије не обезбеђује адекватан ниво заштите права детета на приватност у дигиталном простору, будући да није у довољној мери прилагођен специфичним ризицима и изазовима савременог дигиталног окружења, потврђена је, и то као национална потврда онога што је првом

хипотезом утврђено за посматране системе. Домаћи оквир располаже пристојним нормативним основама, али механизми недостају управо тамо где је приватност детета данас највише угрожена. Питања попут профилисања деце, зависничког дизајна и обавезе платформи према малолетницима у домаћем праву немају посебан режим, већ се, уколико су уопште обухваћена, решавају општим правилима о заштити података, породичноправним и медијским механизмима. Стога се неадекватност заштите не огледа толико одсуству норми, колико у недостатку механизама и њиховој неприлагођености савременим изазовима заштите дечје приватности у дигиталном простору.

Када је реч о четвртој хипотези, да стандарди Европске уније, Савета Европе и праксе Европског суда за људска права могу представљати значајан основ за процену и унапређење правног оквира Републике Србије, иста је потврђена, али условно. Стандарди заиста постоје као довољан основ: оквир заштите података о личности, обавезе пружалаца услуга, позитивне обавезе државе и начела најбољег интереса и развојних способности детета. Њихова преносивост, међутим, није аутоматска. Без изричитих обавеза пружаоцима услуга и без изричито уређених овлашћења надзорног органа у дигиталном окружењу, стандарди остају на папиру, будући да се њима не може деловати према оном субјекту који у дигиталном простору највише одређује услове приватности детета. Унапређење стога не захтева нови партикуларни закон за сваку појаву, него неколико усмерених измена, свака са узором у посматраним системима, и ниједна не зависи од технолошког развоја или будућих европских аката.

У погледу пете хипотезе, да ефикасна заштита захтева јасно дефинисане обавезе и одговорности не само родитеља и државе, већ и пружалаца дигиталних услуга и платформи, иста је потврђена као услов без којег остале мере остају недовршене. Пракса примене Акта о дигиталним услугама показала је да обавезе пружаоцима могу имати стварни ефекат, од забране огласа заснованих на профилисању малолетника до поступака против највећих друштвених мрежа. Ефикасност тих обавеза, притом, зависи од санкције: када су велики пружаоци услуга спремни да казну плаћају као трошак пословања, јер профит надмашује казну, обавеза остаје програмска. Зато је питање ефикасног, сразмерног и одвраћајућег санкционисања, а не само нормативног обавезивања, оно које ће одлучивати о стварној вредности овог правца.

Посебну тежину у укупној оцени има шерентинг, који у овом раду служи као тест целог оквира, јер се у њему све утврђене празнине сабирају у једну: одлука о подацима који се о детету објављују остаје у потпуности на родитељима, без механизма којим би

се проверавала у складу са његовим најбољим интересом, право на брисање је детету у најрањивијем узрасту недоступно, надзор недостаје, а судска заштита зависи од родитељске воље. Упоредни материјал нуди решење за сваки појединачни елемент тог низа, али не и модел целине, тако да би изричито уређење шерентинга у српском праву, ако будући законодавац прихвати наведене елементе, морало бити састављено из појединачних модела, а не преписано из једног система. Таквим уређењем српски законодавац би, по садржаном прегледу држава бивше Југославије изложеном у овом раду, направио први такав покушај у посматраном кругу држава. У томе, и у едукативном слоју који обухвата децу, родитеље, институције и правосудне органе, лежи разлика између заштите која је нормативно прокламована и заштите која је стварна: регулатива без едукације не затвара празнину коју креативност корисника ствара, а едукација без регулативе остаје на савести појединца.

Из наведеног произлази и смер даљег развоја ове области, како у теорији, тако и у пракси: пракса Европског суда за људска права у односу на шерентинг и профилисање деце још увек је у изградњи, а исход предлога EU KIDS Act-a и примене европског новчаника дигиталног идентитета показаће да ли ће најновији слој европске заштите превазићи напетост између безбедности и основних права детета или да је трајно учврсти у самом дизајну система. На крају, вреди констатовати да право детета на приватност у дигиталном простору постаје стварно и делотворно не онда када дете сазре за систем, него када систем сазре за дете.

8. ЛИТЕРАТУРА

8.1. Попис коришћене литературе

1. Вучковић, М. (2025). Појам приватности у пракси Европског суда за људска права; у: *Заштита људских и мањинских права у европском правном простору*. Ниш: Правни факултет Универзитета у Нишу. 169–184. DOI: 10.5281/zenodo.17799946.
2. Вучковић Шаховић, Н. и Петрушић, Н. (2015). *Права детета*. Ниш: Правни факултет, Центар за публикације.
3. Настић, М. (2009). Уставноправни значај Европске конвенције за заштиту људских права и основних слобода у правном систему Републике Србије; у: *Право Републике Србије и право Европске Уније – стање и перспективе*. Ниш: Правни факултет у Нишу. 500–501.
4. Пауновић, М. Кривокапић, Б. и Крстић, И. (2018). *Међународна људска права*. Београд: Универзитет у Београду – Правни факултет, Центар за издаваштво и информисање.
5. Akay, O. (2026). *Children's Privacy, Autonomy, and Digital Identity in Sharenting Research: A Scoping Review with Bibliometric Mapping*. Frontiers in Psychology. Vol. 17. 1845715. DOI: 10.3389/fpsyg.2026.1845715.
6. Barassi, V. (2018). The Child as Datafied Citizen: Critical Questions on Data Justice in Family Life; in: Mascheroni, G. Ponte, C. and Jorge, A. (eds.). *Digital Parenting: The Challenges for Families in the Digital Age*. Göteborg: Nordicom. 169–177.
7. Berg, V. Arabiat, D. Mörelius, E. Kervin, L. Zgambo, M. Robinson, S. Jenkins, M. and Whitehead, L. (2024). Young Children and the Creation of a Digital Identity on Social Networking Sites: Scoping Review. *JMIR Pediatrics and Parenting*. Vol. 7, No. 1. e54414. DOI: 10.2196/54414.
8. Blum-Ross, A. and Livingstone, S. (2017). *"Sharenting," Parent Blogging and the Boundaries of the Digital Self*. Popular Communication. Vol. 15, No. 2. 110–125. DOI: 10.1080/15405702.2016.1223300.
9. Brosch, A. (2016). When the Child is Born into the Internet: Sharenting as a Growing Trend among Parents on Facebook. *The New Educational Review*. Vol. 43, No. 1. 230. DOI: 10.15804/tner.2016.43.1.19.
10. Buckingham, D. (2015). Defining Digital Literacy: What Do Young People Need to Know About Digital Media? *Nordic Journal of Digital Literacy*. Vol. 10. 21–35.
11. Buitelaar, J. (2018). Child's Best Interest and Informational Self-Determination: What the GDPR Can Learn from Children's Rights. *International Data Privacy Law*. Vol. 8, No. 4. 293–308.
12. Culver, S. and Grizzle, A. (2017). *Survey on Privacy in Media and Information Literacy with Youth Perspectives*. Paris: UNESCO.
13. Donovan, S. (2020). 'Sharenting': The Forgotten Children of the GDPR. *Peace Human Rights Governance*. Vol. 4, No. 1. 53. DOI: 10.14658/pupj-phrg-2020-1-2.

14. Duggan, M. Lenhart, A. Lampe, C. and Ellison, N. B. (2015). *Parents and Social Media*. Washington: Pew Research Center. преузето 9. 9. 2026. http://www.pewresearch.org/internet/2015/07/16/parents-and-social-media/.
15. Greco, R. (2024). Children's Right to Privacy in the Digital Age: Is the ECtHR's Current Approach up to the New Challenges? *Diritti umani e diritto internazionale*. No. 3. 573–599. DOI: 10.12829/115907.
16. Haidt, J. (2024). *The Anxious Generation: How the Great Rewiring of Childhood Is Causing an Epidemic of Mental Illness*. New York: Penguin Press.
17. Hinduja, S. and Patchin, J. W. (2009). *Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying*. Thousand Oaks: Corwin Press.
18. Kidron, B. Evans, A. and Afia, J. (2018). *Disrupted Childhood: The Cost of Persuasive Design*. London: 5Rights Foundation. преузето 15. 9. 2026. https://5rightsframework.com/static/5Rights-Disrupted-Childhood.pdf.
19. Kravchuk, N. V. (2022). Privacy of a Child in the Digital Environment: New Risks Unaddressed. *Legal Issues in the Digital Age*. Vol. 3, No. 2. 73–89. DOI: 10.17323/2713-2749.2022.2.73.89.
20. Kuzmanović, D. Pavlović, Z. Popadić, D. and Milošević, T. (2019). *Korišćenje interneta i digitalne tehnologije kod dece i mladih u Srbiji: Rezultati istraživanja Deca Evrope na internetu*. Београд: Institut za psihologiju Filozofskog fakulteta u Beogradu. преузето 30.9.2026. https://www.pametnoibezbedno.gov.rs/extfile/sr/761/8121_koriscenje_interneta_i_digitalne_tehnologije_kod_dece_i_mladih_u_Srbiji%20(1).pdf.
21. Laufer, R. S. and Wolfe, M. (1977). Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory. *Journal of Social Issues*. Vol. 33, No. 3. 22. DOI: 10.1111/j.1540-4560.1977.tb01880.x.
22. Lendvai, G. F. (2024). Sharenting as a Regulatory Paradox: A Comprehensive Overview of the Conceptualization and Regulation of Sharenting. *International Journal of Law, Policy and the Family*. Vol. 38, No. 1. DOI: 10.1093/lawfam/ebae013.
23. Lendvai, G. F. and Ambrazevičiūtė, K. (2025). Parenting in the Digital Age: Addressing the Sharenting Phenomenon in Central and Eastern Europe; in: *Children's Rights in Central and Eastern Europe: A Comparative Analysis with a Spotlight on Lithuania*. Cham: Springer. 349–364. DOI: 10.1007/978-3-032-07092-0_17.
24. Livingstone, S. (2018). Children: A Special Case for Privacy? *InterMedia*. Vol. 46, No. 2. 18–23. преузето 15. 9. 2026. https://researchonline.lse.ac.uk/id/eprint/89706/.
25. Livingstone, S. Nair, A. Stoilova, M. van der Hof, S. and Caglar, C. (2024). Children's Rights and Online Age Assurance Systems: The Way Forward. *International Journal of Children's Rights*. Vol. 32, No. 3. 721–747. DOI: 10.1163/15718182-32030001.
26. Livingstone, S. Stoilova, M. and Nandagiri, R. (2020). Data and Privacy Literacy: The Role of the School in Educating Children in a Datafied Society; in: Frau-Meigs, D. (ed.). *Handbook on Media Education Research*. London: Wiley Blackwell. 413–425.
27. Livingstone, S. и др. (2020). *EU Kids Online 2020: Survey Results from 19 Countries*. London: EU Kids Online. преузето 30. 9. 2026. https://doi.org/10.21953/lse.47fdeqj01ofo.

28. Livingstone, S. and Sylwander, K. R. (2025). There Is No Right Age! The Search for Age-Appropriate Ways to Support Children's Digital Lives and Rights. *Journal of Children and Media*. Vol. 19, No. 1. 6–12. DOI: 10.1080/17482798.2024.2435015.
29. Lupton, D. and Williamson, B. (2017). The Datafied Child: The Dataveillance of Children and Implications for Their Rights. *New Media & Society*. Vol. 19, No. 5. 780–794. DOI: 10.1177/1461444816686328.
30. Marwick, A. E. and boyd, d. (2014). Networked Privacy: How Teenagers Negotiate Context in Social Media. *New Media & Society*. Vol. 16, No. 7. 1051–1067. DOI: 10.1177/1461444814543995.
31. Mulligan, D. K. Koopman, C. and Doty, N. (2016). Privacy is an Essentially Contested Concept: A Multi-Dimensional Analytic for Mapping Privacy. *Philosophical Transactions of the Royal Society A*. Vol. 374, No. 2083. DOI: 10.1098/rsta.2016.0118.
32. Niestadt, M. (2025). *Protecting Children Online: Selected EU, National and Regional Laws and Initiatives*. Brussels: European Parliamentary Research Service. преузето 9.9.2026.https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769570/EPRS_BRI(2025)769570_EN.pdf.
33. Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford: Stanford University Press.
34. Nyst, C. (2017). *Privacy, Protection of Personal Information and Reputation*. New York: UNICEF. преузето 1. 10. 2026. https://www.unicef.org/childrightsandbusiness/media/281/file/UNICEF-CRB-Digital-World-Series-Privacy.pdf.
35. OECD. (2021). *Children in the Digital Environment: Revised Typology of Risks*. Paris: OECD Publishing. DOI: 10.1787/9b8f222e-en.
36. Sarikakis, K. and Winter, L. M. (2017). Social Media Users' Legal Consciousness About Privacy. *Social Media + Society*. Vol. 3, No. 1. DOI: 10.1177/2056305117695325.
37. Sas, M. and Mühlberg, J. T. (2024). Trustworthy Age Assurance? A risk-based evaluation of available and upcoming age assurance technologies from a fundamental rights perspective. Brussels: The Greens/EFA in the European Parliament. преузето: 25. 9. 2026. https://extranet.greens-efa.eu/public/media/file/1/8760.
38. Selwyn, N. (2019). What's the Problem with Learning Analytics? *Journal of Learning Analytics*. Vol. 6, No. 3. 11–19. DOI: 10.18608/jla.2019.63.3.
39. Shaffique, M. R. and van der Hof, S. (2024). *Mapping Age Assurance Typologies and Requirements*. Luxembourg: Publications Office of the European Union.
40. Staksrud, E. Helsper, E. Livingstone, S. Lobe, B. Mascheroni, G. Stoilova, M. and Ólafsson, K. (2026). *The EU Kids Online 2026 Comparative Study: Children's Views, Experiences, Opportunities and Risks in a Digital World*. University of Oslo and London School of Economics and Political Science. преузето 18. 9. 2026. DOI: 10.21953/researchonline.lse.ac.uk.00140901.
41. Stalla-Bourdillon, S. (2025). A GDPR Lens on the Draft Article 28 DSA Guidelines and Their Approach to Age Assurance. *European Data Protection Law Review*. Vol. 11, No. 2. 207–214.

42. Stoilova, M. Livingstone, S. and Nandagiri, R. (2020). Digital by Default: Children's Capacity to Understand and Manage Online Data and Privacy. *Media and Communication*. Vol. 8, No. 4. 197–205. DOI: 10.17645/mac.v8i4.3407.
43. Stoilova, M. Nandagiri, R. and Livingstone, S. (2021). Children's Understanding of Personal Data and Privacy Online: A Systematic Evidence Mapping. *Information, Communication & Society*. Vol. 24, No. 4. 557–575. DOI: 10.1080/1369118X.2019.1657164.
44. Tasić, A. (2026). Rizici „digitalnog" djetinjstva: Sharenting u praksi Republike Srbije i Republike Hrvatske. *Dijete i obitelj u suvremenom društvu*. Vol. 3, No. 1. 86. DOI: 10.25234/dosd/41302.
45. Volz, S. (2026). Age Restrictions as a Tool for Enhancing Children's Online Safety: An Analysis with Special Reference to Australian Law. *Computer Law & Security Review*. Vol. 61. DOI: 10.1016/j.clsr.2026.106278.
46. Walrave, M. Verswijvel, K. Ouvrein, G. Staes, L. and Hallam, L. (2022). The Limits of Sharenting: Exploring Parents' and Adolescents' Sharenting Boundaries Through the Lens of Communication Privacy Management Theory. *Frontiers in Education*. Vol. 7. 803393. DOI: 10.3389/feduc.2022.803393.
47. Warren, S. D. and Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review*. Vol. 4, No. 5. 193–220. DOI: 10.2307/1321160.
48. Westin, A. F. (1967). *Privacy and Freedom*. New York: Atheneum.

8.2. Остала истраживачка грађа

Босна и Херцеговина

1. Закон о заштити личних података. Службени гласник Босне и Херцеговине. бр. 12/25. преузето 16. 8. 2026. https://www.sluzbenilist.ba/page/akt/aCRNh0ohz4nh78h77P7BE=.

Црна Гора

2. Zakon o zaštiti podataka o ličnosti. Službeni list CG. Бр. 79/2008, 70/2009, 44/2012, 22/2017 и 77/2024 – prečišćeni tekst. преузето 16. 8. 2026. https://www.gov.me/dokumenta/d65b84b4-14df-43e0-aeb2-aadf44149486.
3. Агенција за заштиту личних података и слободан приступ информацијама Црне Горе. Саопштење за јавност бр. 02-125-9970-1/24 од 27. 9. 2024. преузето 16. 8. 2026. https://www.azlp.me/me/izvjestaji/20144.
4. Заштитник људских права и слобода Црне Горе. Извјештај о раду за 2021. годину. Подгорица, 2022. преузето 16. 9. 2026. https://www.ombudsman.co.me/docs/1652269181_final_izvjestaj_05052022.pdf.

Француска

5. Code de l'éducation. преузето 20. 10. 2026. https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000045289043.
6. Conseil constitutionnel. Décision n° 2026-911 DC од 14. 8. 2026. преузето 10. 9. 2026. https://www.conseil-constitutionnel.fr/decision/2026/2026911DC.htm.
7. Loi n° 2020-1266 du 19 octobre 2020 visant à encadrer l'exploitation commerciale de l'image d'enfants de moins de seize ans sur les plateformes en ligne. преузето 15. 9. 2026. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000042439054.

8. Loi n° 2023-566 du 7 juillet 2023 visant à instaurer une majorité numérique et à lutter contre la haine en ligne. преузето 1. 10. 2026. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047799533.
9. Loi n° 2024-120 du 19 février 2024 visant à garantir le respect du droit à l'image des enfants. преузето 15. 9. 2026. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000049163317.
Loi n° 2026-813 du 24 août 2026 visant à protéger les mineurs des risques auxquels les expose l'utilisation des réseaux sociaux. JO бр. 197 од 25. 8. 2026. Преузето 19.10.2026. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000054743001.

Хрватска

10. Zakon o provedbi Opće uredbe o zaštiti podataka. Narodne novine. Бр. 42/2018. Преузето 15. 9. 2026. https://narodnenovine.nn.hr/clanci/sluzbeni/2018_05_42_805.html.
11. Агенција за заштиту особних података Републике Хрватске. Objava videozapisa djece i dijeljenje sadržaja na internetu i društvenim mrežama. преузето 12. 9. 2026. https://azop.hr/objava-videozapisa-djece-i-dijeljenje-sadrzaja-na-internetu-i-drustvenim-mrezama/.
12. Агенција за заштиту особних података Републике Хрватске. Primjena Opće uredbe o zaštiti podataka u odgojno-obrazovnim ustanovama. преузето 12. 9. 2026. https://azop.hr/primjena-opce-uredbe-o-zastiti-podataka-u-skolskim-ustanovama/.

Италија

13. Legge 17 maggio 2024, n. 70, Disposizioni e delega al Governo in materia di prevenzione e contrasto del bullismo e del cyberbullismo. Gazzetta Ufficiale n. 125 од 30. 5. 2024. преузето 1. 10. 2026. https://www.normattiva.it/atto/caricaDettaglioAtto?atto.codiceRedazionale=24G00086&atto.dataPubblicazioneGazzetta=2024-05-30.

Северна Македонија

14. Агенција за заштиту личних података Северне Македоније. Одржани часови за средношколци на тема „Заштита на личните податоци при користење на интернет“. Објава од 31. 1. 2024. преузето 16. 9. 2026. https://azlp.mk/одржани-часови-за-средношколци-на-тем/.
15. Закон за заштита на личните податоци. Службен весник на Република Северна Македонија. бр. 42/2020, 294/2021 и 101/2025. преузето 18. 9. 2026. https://azlp.mk/wp-content/uploads/2022/11/zakon_za_zastita_na_licnite_podatoci.pdf.

Словенија

16. Informacijski pooblaščenec. Kdo odloča o objavi fotografij otrok. Бр. 07121-1/2025/1393, 5. 9. 2025. преузето 15. 8. 2026. https://www.ip-rs.si/mnenja-zvop-2/kdo-odlo%C4%8Da-o-objavi-fotografij-otrok-1764575439.
17. Informacijski pooblaščenec. Objavljanje fotografij mladoletnega otroka s strani enega izmed staršev kljub nasprotovanju drugega. Бр. 07121-1/2024/483, 23. 4. 2024. преузето 15. 8. 2026. https://www.ip-rs.si/mnenja-zvop-2/objavljanje-fotografij-mladoletnega-otroka-s-strani-enega-izmed-star%C5%A1ev-kljub-nasprotovanju-drugega-1714390337.

18. Safe.si – Center za varnejši internet Slovenije. преузето 15. 8. 2026. https://safe.si/.
19. Zakon o varstvu osebnih podatkov (ZVOP-2). Uradni list RS. Št. 163/22, 40/25 in 10/26. преузето 15. 8. 2026. https://pisrs.si/pregledPredpisa?id=ZAKO7959.

Србија

20. BIRN Србија. Invazija na privatnost: Analiza medijskog izveštavanja. Београд, 2024. преузето 15. 9. 2026. https://birnsrbija.rs/wp-content/uploads/2024/01/Invazija-na-privatnost-%E2%80%93-Analiza-medijskog-izvestavanja.pdf.
21. BIRN Србија. Случај Ribnikar: Da li će tabloidi snositi posledice za medijsko lešinarenje. 26. 12. 2024. преузето 15. 9. 2026. https://birn.rs/slucaj-ribnikar-medijsko-lesinarenje/.
22. BIRN Србија. Пуцњава у Рибникару: Како су Вучић и Милић прекршили законе. 27. 6. 2023. преузето 18. 9. 2026. https://birn.rs/pucnjava-u-ribnikaru-krsenje-zakona/.
23. Закон о електронским медијама. Службени гласник РС. Бр. 83/2014 и 6/2016 – др. закон.
24. Закон о електронским медијама. Службени гласник РС. Бр. 92/2023.
25. Закон о заштити података о личности. Службени гласник РС. Бр. 87/2018.
26. Закон о изменама и допунама Закона о основама система образовања и васпитања. Службени гласник РС. Бр. 92/2023.
27. Закон о основама система образовања и васпитања. Службени гласник РС. Бр. 88/2017, 27/2018 – др. закони, 10/2019, 6/2020 – др. закон и 129/2021.
28. Закон о потврђивању Конвенције Савета Европе о заштити деце од сексуалног искоришћавања и сексуалног злостављања. Службени гласник РС – Међународни уговори. Бр. 1/2010.
29. Закон о ратификацији Европске конвенције за заштиту људских права и основних слобода. Службени лист СЦГ – Међународни уговори. Бр. 9/2003, 5/2005 и 7/2005 – испр. Службени гласник РС – Међународни уговори. Бр. 12/2010 и 10/2015.
30. Закон о јавном информисању и медијама. Службени гласник РС. Бр. 92/2023 и 51/2025.
31. Кривични законик. Службени гласник РС. Бр. 85/2005, 88/2005 – испр., 107/2005 – испр. и др. закони, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016, 35/2019, 94/2024 и 63/2026.
32. Министарство просвете, науке и технолошког развоја. Одлаже се пуштање у рад корисничког дела портала Здравитас. преузето 22. 9. 2026. https://prosveta.gov.rs/vesti/odlaze-se-pustanje-u-rad-korisnickog-dela-portala-zdravitas/.
33. Министарство просвете, науке и технолошког развоја. Портал Здравитас је дигитализација вођења евиденције у оквиру предмета Физичко и здравствено васпитање. преузето 22. 9. 2026. https://prosveta.gov.rs/vesti/portal-zdravitas-je-digitalizacija-vodjenja-evidencije-u-okviru-predmeta-fizicko-i-zdravstveno-vaspitanje/.
34. Национална платформа за превенцију насиља Чувам те. преузето 1. 10. 2026. https://cuvamte.gov.rs.

35. Нацрт закона о заштити података о личности. Чл. 20. преузето 20. 9. 2026. https://www.paragraf.rs/dnevne-vesti/310726/310726-vest13.html.
36. Нова С. Распуст је провео по болницама, 38 ноћи нисмо спавали: Потресна исповест родитеља дечака који је преживео сексуално насиље у школи у Мрчајевцима. 3. 9. 2026. преузето 15. 9. 2026. https://nova.rs/vesti/hronika/sta-se-dosad-desavalo-u-slucaju-u-mrcajevcima-od-neprimerenog-ponasanja-do-polnog-uznemiravanja/.
37. Повереник за информације од јавног значаја и заштиту података о личности. Саопштење: „Здравитас“. Београд, 28. 10. 2024. преузето 10. 9. 2026. https://poverenik.rs/saopstenje-poverenika-zdravitas/.
38. Породични закон. Службени гласник РС. Бр. 18/2005, 72/2011 – др. закон, 6/2015 и 109/2025 – др. закон.
39. Правилник о заштити права малолетника у области пружања медијских услуга. Службени гласник РС. Бр. 25/2015.
40. Правилник о заштити права малолетника у области пружања медијских услуга. Службени гласник РС. Бр. 43/2024.
41. Регулаторно тело за електронске медије. Извештај о раду за 2017. годину. Београд, 2018. преузето 15. 9. 2026. https://www.rem.rs/uploads/files/izvestaj%20o%20radu/Izvestaj%20o%20radu%20REM%202017..pdf.
42. Регулаторно тело за електронске медије. Регистар пружалаца медијских услуга. преузето 15. 9. 2026. https://rem.rs/sr/registar-pruzalaca-medijskih-usluga/575.
43. Синдикат образовања Србије. Захтев Повереникy за спровођење допунског надзора примене ЗЗПЛ у оквиру пројекта „Здравитас“. Београд, новембар 2024. преузето 15. 9. 2026. https://sind-obr.org.rs/wp-content/uploads/2024/11/Povereniku_ZDRAVITAS.pdf.
44. Устав Републике Србије. Службени гласник РС. Бр. 98/2006 и 115/2021.

УНИЦЕФ

45. UNICEF. Children's Online Privacy and Freedom of Expression: Industry Toolkit. Њујорк, 2018. преузето 15. 9. 2026. https://www.unicef.org/childrightsandbusiness/reports/childrens-online-privacy-and-freedom-expression.

Европска Унија

46. EU KIDS Act to restrict social media platforms' access to children in the EU. Саопштење за јавност IP/26/1890. Стразбур, 17. 9. 2026. преузето 1. 10. 2026. https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_26_1890/IP_26_1890_EN.pdf.
47. North Macedonia 2025 Report. Commission Staff Working Document SWD(2025) 759 final. Брисел, 4. 11. 2025. преузето 4. 9. 2026. https://enlargement.ec.europa.eu/document/download/267b368e-6b55-4a42-bb72-6395593de4da_en?filename=north-macedonia-report-2025.pdf.
48. Serbia 2025 Report. Commission Staff Working Document SWD(2025) 755 final. Брисел, 4. 11. 2025. преузето 1. 10. 2026.

https://enlargement.ec.europa.eu/document/download/6e68ce26-b95b-48e1-921a-c60c12da8f00_en?filename=serbia-report-2025.pdf.

49. Предлог уредбе Европског парламента и Савета о заштити малолетника на интернету и измену Уредбе (ЕУ) 2022/2065 (EU Keeping Internet Digital Spaces Accountable and Trustworthy, EU KIDS Act). COM(2026) 681, 17. 9. 2026. преузето 20. 9. 2026. https://digital-strategy.ec.europa.eu/en/library/proposal-eu-kids-act-eu-keeping-internet-digital-spaces-accountable-and-trustworthy.
50. Предлог уредбе Европског парламента и Савета о успостављању правила за спречавање и сузбијање сексуалног злостављања деце. COM(2022) 209 final, 11. 5. 2022. преузето 15. 9. 2026. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2022:209:FIN.
51. Препорука Комисије (ЕУ) 2026/1035 од 29. априла 2026. године о успостављању заједничког оквира за технологије верификације узраста на нивоу ЕУ. Сл. лист ЕУ, L, 2026/1035.
52. Смернице о мерама за обезбеђивање високог нивоа приватности, безбедности и сигурности малолетника на интернету, у складу са чл. 28 ст. 4 Акта о дигиталним услугама (Guidelines on measures to ensure a high level of privacy, safety and security for minors online, pursuant to Article 28(4) of Regulation (EU) 2022/2065). C(2025) 5519, Брисел, 14. 7. 2025. преузето 11. 9. 2026. https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-protection-minors.
53. Уредба (ЕУ) 2016/679 Европског парламента и Савета од 27. априла 2016. године о заштити физичких лица у вези са обрадом података о личности и о слободном кретању таквих података (Општа уредба о заштити података). Сл. лист ЕУ, L 119, 4. 5. 2016. преузето 28. 8. 2026. https://eur-lex.europa.eu/eli/reg/2016/679/oj.
54. Уредба (ЕУ) 2022/2065 Европског парламента и Савета од 19. октобра 2022. године о јединственом дигиталном тржишту, измена и допуна Директиве 2000/31/ЕЗ (Акт о дигиталним услугама). Сл. лист ЕУ, L 277, 27. 10. 2022. преузето 20. 9. 2026. https://eur-lex.europa.eu/eli/reg/2022/2065/oj.
55. Уредба (ЕУ) 2024/1183 Европског парламента и Савета од 11. априла 2024. године о измени Уредбе (ЕУ) 910/2014 у погледу успостављања европског оквира за дигитални идентитет. Сл. лист ЕУ, L, 30. 4. 2024. преузето 19. 9. 2026. https://eur-lex.europa.eu/eli/reg/2024/1183/oj.

Европски суд за људска права

56. Bogomolova против Русије, представка бр. 13812/09, пресуда од 20. 6. 2017.
57. Dupate против Летоније, представка бр. 18068/11, пресуда од 19. 11. 2020.
58. I.V.T. против Румуније, представка бр. 35582/15, пресуда од 1. 3. 2022.
59. K.U. против Финске, представка бр. 2872/02, пресуда од 2. 12. 2008.
60. Reklos и Davourlis против Грчке, представка бр. 1234/05, пресуда од 15. 1. 2009.
61. Söderman против Шведске, представка бр. 5786/08, пресуда Великог већа од 12. 11. 2013.
62. Volodina (бр. 2) против Русије, представка бр. 40419/19, пресуда од 14. 9. 2021.
63. Авилкина и др. против Русије, представка бр. 1585/09, пресуда од 6. 6. 2013.

Организација уједињених нација

64. Комитет за права детета УН. Општи коментар бр. 25 (2021) о правима детета у вези са дигиталним окружењем. CRC/C/GC/25, 2. 3. 2021.
65. Конвенција о правима детета. Службени лист СФРЈ – Међународни уговори. Бр. 15/90 и Службени лист СРЈ – Међународни уговори. Бр. 4/96 и 2/97.
66. Међународни пакт о грађанским и политичким правима. Њујорк, 1966.
67. Општа декларација о људским правима. Париз, 1948.

Република Србија

68. Пресуда Врховног касационог суда Републике Србије, Рев. 14012/2022 од 6. 10. 2022. године.

Савет Европе

69. Lanzarote Committee. Извештај о мониторингу феномена сексуалних садржаја које деца сама генеришу (self-generated sexual material). 2022.
70. Европска мрежа правобранилаца за децу (ENOC). Став о правима детета у дигиталном окружењу, усвојен на 23. Општој скупштини ENOC-а, Белфаст, 27. 9. 2019. преузето 20.9.2026. https://enoc.eu/wp-content/uploads/2019/10/ENOC-2019-Statement-on-Childrens-Rights-in-the-Digital-Environment.pdf.
71. Конвенција за заштиту људских права и основних слобода. Рим, 1950.
72. Конвенција о заштити деце од сексуалног искоришћавања и сексуалног злостављања (Ланзаротска конвенција). CETS No. 201, Лансароте, 25. 10. 2007.
73. Конвенција о заштити лица у односу на аутоматску обраду личних података, са Протоколом о изменама и допунама (Конвенција 108+). Службени гласник Републике Србије – Међународни уговори. Бр. 4/20.
74. Смернице за поштовање, заштиту и остваривање права детета у дигиталном окружењу. Препорука CM/Rec(2018)7, Стразбур, 2018.
75. Стратегија за права детета (2022–2027). Стразбур, 2022.

9. САЖЕТАК И КЉУЧНЕ РЕЧИ

Развој дигиталних технологија суштински је изменио услове у којима се право детета на приватност остварује и штити. Деца од најранијег узраста користе дигиталне услуге и друштвене мреже, а њихови лични подаци се прикупљају, обрађују и даље деле не само од стране пружалаца услуга и платформи, него и најближег окружења, пре свега родитеља (шерентинг). Рад испитује ефикасност правне заштите права детета на приватност у дигиталном простору.

Истраживање обухвата међународни оквир (Конвенција о правима детета, Општи коментар бр. 25), европске стандарде (ГДПР, ДСА, Смернице Савета Европе, пракса Европског суда за људска права), правни оквир Републике Србије и држава насталих на простору бивше Југославије. Примењени су нормативно-догматски и компаративно-правни метод, метод анализе садржаја и судске праксе, као и телеолошки метод.

Анализа показује да механизми заштите постоје на свим посматраним нивоима, али да празнине у заштити нису појединачни недостаци прописа, него последица начина на који су системи, под истим европским стандардом, организовани: шерентинг није изричито уређен ни на једном нивоу; надзор над обрадом података од стране приватних лица испод кривичноправног прага је епизодичан и реактиван; утврђивање узраста носи напетост између заштите и основних права детета; а судска и институционална пракса реагују кроз општа начела и најчешће по иницијативи оштећеног.

Као правци унапређења предлажу се изричито уређење шерентинга, састављено из појединачних упоредних модела (француско решење, црногорски критеријум најбољег интереса, словеначка и хрватска надзорна пракса), конкретизација провере пристанка законског заступника у Закону о заштити података о личности, изричито уређење овлашћења Повереника у дигиталном окружењу и едукативни слој који обухвата децу, родитеље, институције и правосудне органе. Све предложене мере имају узор у посматраним системима и не зависе од технолошког развоја или будућих европских аката. Закључак рада јесте да право детета на приватност у дигиталном простору постаје стварно не онда када дете сазре за систем, него када систем сазре за дете.

Кључне речи: право детета, приватност, дигитални простор, шерентинг, заштита података о личности, најбољи интерес детета, правци унапређења.

10. ABSTRACT AND KEY WORDS

Title of the paper: **The Right of the Child to Privacy in the Digital Environment**

Digital technologies have profoundly altered the conditions under which children exercise and enjoy their right to privacy. From the earliest age, children use digital services and social networks, while their personal data are collected, processed and further shared not only by service providers and platforms, but also by their closest environment, above all by parents (sharenting). The thesis examines the effectiveness of the legal protection of children's right to privacy in the digital environment.

The research covers the international framework (the Convention on the Rights of the Child and General Comment No. 25 on children's rights in relation to the digital environment), the European standards (the General Data Protection Regulation, the Digital Services Act, the Council of Europe Guidelines and the case law of the European Court of Human Rights), as well as the legal framework of the Republic of Serbia and the States that emerged from the former Yugoslavia. The methods applied include dogmatic-normative and comparative legal analysis, content analysis and case-law analysis, as well as teleological interpretation.

The analysis shows that protection mechanisms exist at all levels examined, yet the gaps in protection are not isolated shortcomings of individual provisions, but consequences of the way in which the systems, under the same European standard, are organised: sharenting is not expressly regulated at any level; supervision over the processing of children's data by private actors below the threshold of criminal liability is episodic and reactive; age assurance is in tension with the fundamental rights of the child; and judicial and institutional practice operates through general principles and most often upon the initiative of the injured party.

The following directions for improvement are proposed: the express regulation of sharenting, assembled from individual comparative models (the French solution, the Montenegrin best-interests criterion, and Slovenian and Croatian supervisory practice); the concretisation of the verification of parental consent in the Law on Personal Data Protection; the express regulation of the powers of the Commissioner for Information of Public Importance and Personal Data Protection in the digital environment; and an educational layer encompassing children, parents, institutions and judicial authorities. All proposed measures have models in the systems examined and do not depend on technological development or future European instruments. The thesis concludes that children's right to privacy in the digital environment becomes real not when the child matures into the system, but when the system matures for the child.

Key words: the right of the child, privacy, digital environment, sharenting, personal data protection, best interests of the child, directions for improvement.

11. БИОГРАФИЈА АУТОРКЕ

Душица Лазић рођена је 20. 3. 2000. године у Прокупљу. Основну школу „Никодије Стојановић Татко“ и Гимназију завршила је у Прокупљу као носилац Вукових диплома. Основне академске студије права уписала је 2019. године на Правном факултету Универзитета у Нишу, а завршила 2024. године са просечном оценом 9,30. Након завршених основних студија, уписала је мастер академске студије права на истом факултету, смер Општи, Грађанскоправна научна област.

Током студија бавила се питањима људских права и заштите од дискриминације кроз бројна Moot Court такмичења. На такмичењу „Бранко Маринковић“ освојила је награду „Звезда у успону“. На регионалном такмичењу „Симулација поступка пред Европским судом за људска права“, у организацији *Civil Rights Defenders*, заједно са својим тимом освојила је 1. место, а потом и 2. место у великом финалу, одржаном у новембру 2023. године пред судијама Европског суда за људска права у Стразбуру. У оквиру такмичења Нелсон Мандела, одржаног у седишту Уједињених нација у Женеви, пласирала се у топ 16 тимова. На такмичењу „Осуди дискриминацију“, које организује Канцеларија Повереника за заштиту равноправности, као чланица тима „Драга Љочић“ освојила је 1. место за писани поднесак и усмено излагање, уз индивидуалну награду за најбољег говорника. Током основних и мастер студија била је и полазница бројних програма и летњих школа у земљи и иностранству, посвећених питањима људских права и процесу дигитализације.

Истраживачким радом почела је да се бави у Истраживачкој станици Петница, као полазница Летње научне школе 2014. године, а потом семинара геологије од 2016. године, где данас учествује у статусу стручног сарадника. Њени ауторски и коауторски рад, „Могућност реексплоатације воде Куршумлијске бање“ и „Хемијске карактеристике воде Петничког језера“, представљени су на конференцији „Корак у науку“ 2017. и 2018. године и објављени у Петничким свескама.

Током студија била је добитница стипендије Министарства просвете, науке и технолошког развоја (стипендија Доситеја) и, у два наврата, награде Града Прокупља за надарене студенте. У оквиру програма Таленти у јавном сектору обавила је шестомесечну праксу у Вишем суду у Нишу. Од децембра 2025. године уписана је у Адвокатску комору у Нишу као адвокатска приправница.

ИЗЈАВА О ИСТОВЕТНОСТИ
ШТАМПАНОГ И ЕЛЕКТРОНСКОГ ОБЛИКА МАСТЕР РАДА

Име и презиме аутора мастер рада: **Душица Лазић**

Наслов мастер рада: „**Право на приватност детета у дигиталном простору**“.

Ментор: **Проф. др Анђелија Тасић**

Изјављујем да је електронски облик мастер рада у pdf формату истоветан штампаном облику, који сам предао/ла Правном факултету Универзитета у Нишу.

У Нишу, _____

Потпис аутора

_____
Душица Лазић

ИЗЈАВА О АУТОРСТВУ И ОДОБРАВАЊУ ОБЈАВЉИВАЊА МАСТЕР РАДА

Изјављујем да је мастер рад, под насловом: „**Право на приватност детета у дигиталном простору**“ пријављен и одбрањен на Правном факултету Универзитета у Нишу:

• резултат сопственог истраживачког рада;

• да овај мастер рад у целини, нити у деловима, нисам пријављивао/ла на другим факултетима, нити универзитетима;

• да нисам повредио/ла ауторска права, нити злоупотребио/ла интелектуалну својину других лица.

Дозвољавам да се овај мастер рад чува у библиотеци и објави на сајту Правног факултета Универзитета у Нишу, са подацима о датуму одбране и комисији пред којом је рад брањен.

Аутор мастер рада: **Душица Лазић**

У Нишу, _____

Потпис аутора

_____

Душица Лазић