

УНИВЕРЗИТЕТ У НИШУ

ПРАВНИ ФАКУЛТЕТ

Људска права у дигиталном добу

(мастер рад)

Ментор

Проф. др Маја Настић

Студент

Јулија Пејчић
Број индекса: М006/21-ИТ

Ниш, 2024. године

САДРЖАЈ

I УВОД	1
II ИНФОРМАЦИОНЕ ТЕХНОЛОГИЈЕ И ПОСТОЈЕЋА ЛЈУДСКА ПРАВА.....	3
2.1. Слобода изражавања	4
2.2. Право на претпоставку невиности.....	7
2.3. Право на образовање.....	10
2.4. Право на заштиту података о личности.....	13
III ИНФОРМАЦИОНЕ ТЕХНОЛОГИЈЕ И ДИГИТАЛНА ПРАВА.....	18
3.1. Право на приступ интернету.....	18
3.2. Право на информационо самоодређење.....	22
3.3. Право на заборав.....	24
IV СУДСКА ПРАКСА САВЕЗНОГ УСТАВНОГ СУДА НЕМАЧКЕ У ПРЕДМЕТИМА ЗАШТИТЕ ПРАВА НА ИНФОРМАЦИОНО САМООДРЕЂЕЊЕ.....	28
4.1. 2BvR 939/13.....	28
4.2. BVerfGE 120, 238.....	31
4.3. 1BvR 2649/21.....	34
4.4. 1BvR 518/02.....	36
4.5. BVerfGE 65, 1.....	39
V ЗАКЉУЧАК.....	41
<i>Литература</i>	43
<i>Сажетак и кључне речи</i>	46
<i>Summary and key words</i>	48
<i>Биографија аутора</i>	50

I УВОД

Информационо комуникационе технологије подразумевају употребу рачунарских и телекомуникационих технологија, система и алата за олакшавање начина на који се информације креирају, прикупљају, обрађују, преносе и чувају. Информационо комуникационе технологије укључују како застареле технологије као што су фиксни телефони, радио и телевизијско емитовање, које се и данас активно користе, тако и најсавременије технологије као што су вештачка интелигенција и роботика. Њихова појава драстично је променила начин на који људи воде своје свакодневне животе: раде, комуницирају, уче и живе.

Сведоци смо огромног технолошког напретка. Нове технологије су нашле своје место у данашњем друштву и људи их свакодневно користе за обављање већине својих активности. Имајући напред наведено на уму, морамо бити свесни обавезе поштовања постојећих људских права и стварања потпуно нових права која су се могла формирати само у новонасталој дигиталној ери.

У многим случајевима, на технологију можемо гледати као на један од битнијих фактора за далекосежније поштовање и уживање људских права - слобода изражавања је, примера ради, добила нове димензије увођењем нових облика изражавања формираних на мрежи, те су припадници народа чије се мишљење до сада није чуло коначно добили шансу да постану део глобалне демократије и активно учествују у борби против разних видова дискриминације и правног угњетавања.

С друге стране, технологија је такође створила проблеме и изазове како организацијама тако и појединцима и друштву у целини. Дигитализација података, све већа употреба брзог интернета и растућа глобална мрежа заједно су довели до нових облика криминала, који подразумевају средства и начине који се у претходном веку нису могли ни замислити.

Претходно поменута слобода изражавања која је првенствено доживела експанзију у онлајн свету, данас је често изложена филтрирању, а њено уживање ограничава се и потпуним блокирањем садржаја, па чак и искључењем приступа интернету. Свакако, процес транзиције и преласка људских права на мрежу не своди се само на право на слободу изражавања, већ укључује и многа друга људска права која своју примену и праксу могу остварити у онлајн свету. Претпоставка невиности је, рецимо, једно од најспорнијих људских права у онлајн сфери, и изложено је ризику због праксе прикупљања података у сврхе превентивног надзора без претходне сумње.

У наставку овог рада бавићемо се питањем изложености људских права на интернету, са фокусом на подизању свести о различитим начинима на које онлајн присутност и активности појединца утичу на његова права и слободе као и степену у којем су људска права угрожена у дигиталном добу. До одговора на поменута питања доћи ћемо обрадом *de jure* и *de facto* стања разматрајући три целине.

У другом делу скренућемо пажњу на утицај информационих технологија на постојећа, историјски установљена и широко примењивана људска права и то: слободу говора, право на претпоставку невиности, право на образовање и право на заштиту података о личности. Изучавајући овај утицај доћи ћемо до одговора да ли су и у којој мери постојећа људска права поштована на мрежи, али и колико су угрожена развојем информационих технологија. Открићемо такође и које су могућности да прописи иду у корак са развојем технологија и амортизују њихов утицај на људска права и слободе.

У трећем делу открићемо новонастала права и слободе која су спонтано настала заједно са развојем информационих технологија и која се уско везују за њихову примену, и то: право на приступ интернету, право на информационо самоодређење и право на заборав. Сва ова права једним именом можемо назвати дигиталним правима у складу са њиховим подручјем примене. У овом делу рада сазнаћемо колико су ова права територијално распрострањена, колики су изгледи њихове правне заштите као и могућност њиховог дефинитивног дефинисања у динамичној информационо-технолошкој ери.

У четвртном делу овог рада, осврнућемо се на неке од одлука Савезног уставног суда Немачке у предметима заштите права на информационо самоодређење. Анализом судске праксе уочава се велики помак у заштити права појединца на информационо самоодређење и тежња да се грађанима пружи адекватна заштита која је загарантована уставом и законима. Случајеви пред овим судом довели су до утврђивања граница права на информационо самоодређење и постављања услова чијим испуњењем ово право може бити ограничено у корист јавног интереса. На основу изнетих случајева може се уочити објективност, политичка независност и конзистентност суда при доношењу одлука.

У закључном делу сумираћемо резултате истраживања, дефинисати тренутни положај људских права у добу дигиталне експанзије, те покушати да одредимо основне забринутости у вези са њиховим коришћењем, остваривањем и заштитом, посебно узевши у обзир динамичност дигиталног напретка.

II ИНФОРМАЦИОНЕ ТЕХНОЛОГИЈЕ И ПОСТОЈЕЋА ЉУДСКА ПРАВА

Информационе технологије, услед сталног развоја и напретка, до данашњих дана још увек нису добиле једну јединствену дефиницију која би могла да дочара све оно што оне представљају. Ипак, можемо закључити да информационе технологије, у материјалном смислу, представљају примену постојећих и нових технолошких средстава ради остваривања складиштења, размене и обраде дигитализованих информација.¹

Комуникационо-информационе технологије, с техничке стране гледишта, подразумевају велике базе података и мреже рачунара који служе у сврху комуникације субјеката. Ове технологије састоје се, дакле, како из мрежног хардвера, тако и из софтвера. За функционисање информационо-комуникационих система неопходно је да је софтвер повезан са хардвером односно да хардвер садржи софтвер, у супротном, систем неће функционисати.

У скоро свим сферама друштва ове технологије донеле су корените трансформације, а посебно у виду ефикасности, нивоа интеракције и брзине. Појединцима широм света је појава информационих технологија омогућила лакшу комуникацију, као и креирање и управљање информацијама новим, креативним алатима. Имајући у виду степен интегрисаности нових технологија у велики део друштвених активности и свакодневног живота, савремени свет не може се замислити без њих.

Упркос бројним предностима које ове технологије омогућавају у уживању људских права, њихов ефекат веома је видљив и у области ограничавања и кршења ових права, посебно у виду надзора и цензуре. На овај начин постојећа људска права директно су стављена у ризик, нарушена је социјална заштита, неједнакости продубљене, а постојећа дискриминација попримила нове оквире, чему државне институције и органи тешко стају на пут. Чак и демократске владе које су предњачиле у заштити људских права сада масовно крше, или не успевају да стану на пут кршењима људских права, а све у име националне безбедности и борбе против тероризма.

У наставку рада бавићемо се утицајем информационих технологија на основна људска права, и то: слободу изражавања, право на претпоставку невиности, право на образовање и право на заштиту података о личности.

¹ С. Н. Андоновић, *Заштита података у електронској јавној управи у Републици Србији - правни аспекти*, Београд, 2019, стр. 36

2.1. Слобода изражавања

Слобода изражавања или слобода говора једна је од највећих вредности модерног (слободног) друштва. Као таква предвиђена је чланом 10 Европске конвенције о људским правима, те се слобода говора у њој дефинише као “право које припада свима и које укључује слободу поседовања сопственог мишљења, примања и саопштавања информација и идеја без мешања јавне власти и без обзира на границе”²

Универзална декларација о људским правима слободу говора у члану 19. дефинише као “право на слободу мишљења и изражавања, што обухвата и право да не буде узнемираван због свог мишљења, као и право да тражи, прима и шири информације и идеје било којим средствима и без обзира на границе.”³

Слободу изражавања препознаје и Устав Републике Србије у члану 46 којим се јемчи слобода мишљења и изражавања, као и “слобода да се говором, писањем, сликом или на други начин траже, примају и шире обавештења и идеје.”⁴

Уколико се на тренутак вратимо на дефиницију слободе говора наведену у члану 19. Универзалне декларације о људским правима и посебну пажњу посветимо делу дефиниције који наводи да се идеје и информације могу тражити, примити и ширити “било којим средствима”, долазимо до закључка да је ова дефиниција имала у виду сва постојећа, али и средства комуникације у настајању, те тако слободно можемо рећи да је интернет једно од поменутих средстава.

Наиме, неспорно је да са појавом интернета ово право добија нове, шире димензије. До појаве интернета, право на слободно изражавање упражњавало се искључиво путем медија у којима постоји неколико посредника, док са интернетом појединац добија могућност директног обраћања ширем аудиторијуму.⁵ Обичан човек добио је могућност креирања порука које затим директно дистрибуира другима, те тиме постаје конкуренција професионалним ствараоцима јавног мњења и посредно учествује у обликовању визије стварности.⁶ Такође, “без обзира на границе” добија на значају тек са појавом интернета, која је довела до тога да међудржавне границе полако бледе, те се

² Чл. 10 Европске конвенције о људским правима, 1950.

³ Чл. 19 Универзалне декларације о људским правима, 1948.

⁴ Чл. 46 Устава Републике Србије, *Службени гласник РС*, бр. 98/06

⁵ Ј. Сурчулија, *Слобода изражавања на интернету*, Центар за развој интернета, Београд, 2010, стр. 20

⁶ Д. Тодоровић, Д. Прља, Д. Петровић, *Интернет и друштво*, Ниш и Београд, 2014, стр. 320

омогућава да информације и идеје буду у истом тренутку доступне широм земаљске кугле.

У земљама у којима су мреже комуникације традиционално биле контролисане, појава интернета донела је наду грађанима који су дуго били спутавани да слободно изразе своје идеје и мишљење. Без обзира на то колико тема била непопуларна или интригантна, свако може да изрази своје мишљење о њој без бриге да ће његово мишљење бити игнорисано или потиснуто. Грађани су, дакле, пронашли нови медијум за слободно изражавање, који у земљама у којима је цензура свакодневна појава, често крши чврста ограничења наметнута њиховим правима. Због тога је интернет виђен као прозор у демократију и својеврсни вид савремене слободе.⁷

Све напред наведено можемо сматрати позитивним исходима утицаја интернета на слободу изражавања, међутим, као и у реалном животу, ово право трпи висок ниво дискриминације и цензуре на интернету, али се у неким случајевима мора и законски ограничити како би се предупредиле његове злоупотребе, посебно ако упражњавање слободе говора доводи у опасност права и репутацију других лица, или јавно здравље и морал.

Као једна од негативних последица утицаја интернета на право на слободу изражавања појављује се и чињеница да је владама земаља широм света интернет пружио нове могућности за надзор и цензурисање слободе изражавања која се испољава у онлајн свету. Посматрајући поступке влада широм света, слободу изражавања могли бисмо дефинисати и као “слободу да говорите када би већина желела да то не чините, и радо би вас ућуткала да то може”.⁸ Чак и “дугопостојеће” демократије као што су Уједињено Краљевство, САД или Француска, практикују цензуру и разне врсте надзора у циљу безбедности и борбе против тероризма. Међутим, многи примери оваквог нарушавања слободе изражавања немају утемељени и подобно оправдани разлог.⁹ Бројни софистицирани алати користе властима да цензуришу онлајн садржај само зато што се садржај нечијег израженог мишљења коси са актуелном политиком те државе.¹⁰

Као један од примера може се навести Белорусија у којој су телекомуникацијске мреже контролисане од стране владе те државе уз помоћ компаније Beltelecom која

⁷ Internet and Society Collaboratory e.V. *Human Rights and Internet Governance*, Berlin, 2012, 1st edition, pp. 50

⁸ *Ibid.* pp. 42

⁹ K. K. Singh, *Human Rights in Information Age: Emerging Issues and Challenges*, Delhi, 2015, pp. 12

¹⁰ Legal Vidhiya, *Effect of Internet on Freedom of Speech & Expression*; преузето 12.09.2023.

<https://legalvidhiya.com/effect-of-internet-on-freedom-of-speech-expression/>

држи монопол међу провајдерима.¹¹ Контрола се огледа у блокирању опозиционих веб-сајтова, који својим садржајем најчешће подривају установљене принципе и политички правац владајуће већине. Ово се најчешће дешава у јеку предизборних кампања како би се грађани изоловали од информација које су пласиране на веб-сајтовима независних опозиционих медија, политичких партија и опозиционих кандидата, а који би потенцијално могли да грађанима промене мишљење о актуелним темама и устаљеној пракси и политици коју је наметнула владајућа већина.

Кина, с друге стране, поседује један од најсложенијих и најраспрострањенијих система за контролу и филтрирање информација на вебу, тзв. „Велики заштитни зид“. Циљ је блокирање приступа веб-сајтовима који као кључне речи садрже појмове “људска права” и “демократија”. Такође, постоји мрежа људи који су плаћени од стране државе како би се на веб-сајтовима представљали као редовни корисници, а све у циљу лоцирања критика на рачун власти. На захтев владе, велике интернет платформе у Кини успоставиле су разрађене механизме самоцензуре, као и имплементацију система са правим именом који подразумева да су интернет провајдери услуга и садржаја обавезни да прикупљају права имена корисника, идентификационе бројеве и друге информације приликом пружања услуга.¹²

Такође, настанком друштвених мрежа појављује се нова опасност по злоупотребу слободе говора јер исте омогућавају корисницима говор мржње, ширење дезинформација и других штетних садржаја, што слободу говора може окренути против њених уживаоца. Жене, мањине и друге маргинализоване групе су посебно подложне узнемиравању на мрежи, које може укључивати претње насиљем и другим облицима узнемиравања.

Једна од група лица која јако често потпада под руке судске власти јесу блогери. То су лица која своју препознатљиву појаву на интернету користе како би изнели мишљења о разним темама као што су: култура, политика, јавне личности, актуелна дешавања. Услед несмотреног, или можда умишљајног, изношења мишљења, често се дешава да блогери буду приведени правди због клевета изречених на њиховим платформама. Статистика изведена у Сједињеним Америчким Државама показује да су судови, ипак, најчешће на страни блогера, али се често овакви случајеви завршавају тако што приватна лица одустају од тужби.¹³

¹¹ J. Сурчулија, *op.cit.*, стр. 95.

¹² J. Coccoli, *The Challenges of New Technologies in the Implementation of Human Rights: an Analysis of Some Critical Issues in the Digital Era*; *Peace Human Rights Governance*, Padova, 2017, pp. 229-230

¹³ J. Сурчулија, *op.cit.*, стр. 28-34

Међитим, како је интернет срушио међудржавне границе, а корисници интернета ипак постоје у реалном свету и њихове активности се могу лоцирати у једној или више јурисдикција, поставља се питање: када лице лоцирано у оквирима једне јурисдикције својим слободним говором наруши права лица или органа који припада другој јурисдикцији, које ће се право користити приликом оцењивања штетности изреченог мишљења? Уколико као пример узмемо поступак који се водио пред немачким судом, а против аустралијског држављанина за материјал који негира постојање холокауста, поставља се питање: да ли аутор одређеног рада или идеје изречене на интернету треба да зна и кривично право државе коју изнете чињенице директно погађају како би био спреман на евентуални судски процес који би уследио као последица изношења потенцијално увредљивих информација? Како би се овакав сценарио избегао, најкориснији алат јесте онемогућавање приступа материјалу државама на које се изнете информације директно односе (гео-блокирање).¹⁴

Слобода говора на интернету је моћно оружје јер омогућава појединцима да изразе своја мишљења и идеје без страха. Интернет је омогућио појединцима да се организују и окупе око друштвених и политичких идеја, и да оне на власти позову на одговорност, али и маргинализованим групама да се чује и њихов глас и да се разне организације окупе у жељи да поспеше њихова права и могућности.

Иако су отворили нове путеве за изражавање и учешће, интернет и информационе технологије створили су нове изазове и ризике којима се треба позабавити како би се заштитила и промовисала слобода говора у дигиталном добу. Узимајући у обзир и позитивне и негативне стране експлоатације слободе говора на интернету важно је да друштво ради на проналажењу равнотеже која омогућава слободну размену идеја, а истовремено штити појединце од штетних утицаја.

2.2. Право на претпоставку невиности

Право на претпоставку невиности је основно људско право уставног ранга, које је заједно са правом на правично суђење дефинисано у члану 6 Европске конвенције о људским правима, и сматра се процесном гаранцијом и препреком за злоупотребу кривичне одговорности. Овим чланом јасно се наводи да се “свако ко је оптужен за

¹⁴ J. Сурчулија, *op.cit.*, стр. 22-24

кривично дело мора сматрати невиним све док се не докаже његова кривица на основу закона.”¹⁵

Устав Републике Србије право на претпоставку невиности дефинише чланом 34 и наводи да се “свако сматра невиним за кривично дело док се његова кривица не утврди правноснажном одлуком суда.”¹⁶

Ово право сматра се једним од најоспораванијих и најугроженијих људских права у време убрзаног технолошког развоја.

Терористички напади који су се догодили у Сједињеним Америчким Државама 11. септембра 2001. године, довели су до претварања спорадичних случајева дигиталног надзора у сталну праксу којој националне владе прибегавају уз образложење да се тиме тежи ка стварању сигурније средине за све становнике. Дигитални надзор као превентивна мера потпомаже државама у лоцирању и спречавању потенцијалних терористичких акција на њиховим територијама. Оно што у тим тренуцима није узето у обзир јесте опасност коју оваква пракса представља за очување права на претпоставку невиности. Стална пракса прикупљања података у сврхе надзора без претходне сумње сматра се једном од највећих претњи која се везује за ово право.¹⁷

Савремене технологије надзора довеле су до настанка “дигиталних доказа” који се дефинишу као “свака информација обрађена електронским медијем која подржава или оповргава хипотезу о стању дигиталних артефаката или дигиталних догађаја, потенцијално релевантне и доказне вредности за кривичну истрагу.”¹⁸ Они негативно утичу на право на претпоставку невиности на два различита начина наведена у наставку.

Као први негативни утицај наводи се чињеница да терет доказивања прелази са оштећеног на окривљеног - дакле, окривљени ће бити задужен да докаже да се докази које нуде технологије надзора не могу сматрати довољним и поузданим у доказивању његове кривице. Оваква пракса резултира подизањем прага невиности, те су додатни напори и докази неопходни како би се невиност пред судом у кривичном поступку и доказала.

¹⁵ Чл. 6 Европске конвенције о људским правима, 1950

¹⁶ Чл.34 Устава Републике Србије, *Службени гласник РС*, бр. 98/06

¹⁷ A. Galetta, The changing nature of the presumption of innocence in today's surveillance societies: rewrite human rights or regulate the use of surveillance technologies?; in: *European Journal of Law and Technology*, Vol.4, No.2, 2013; преузето 12.09.2023. <https://ejlt.org/index.php/ejlt/article/view/221/377>

¹⁸ R. Stoykova, Digital Evidence: Unaddressed Threats to Fairness and the Presumption of Innocence; in: *Computer Law & Security Review*, Vol.42, 2021, Article 105575, pp. 2

Други негативни ефекат дигиталних доказа је опасност стигматизације. Наиме, савремене технологије надзора могу повећати уверење да лице чији су подаци техникама надзора прикупљени нужно мора бити осумњичени, те се тиме дубоко ремети гаранција права на претпоставку невиности. Стигматизација оставља друштвени траг, иако је потенцијално у току истраге и судског поступка лице проглашено невиним.¹⁹ До којих размера и последица ће стигматизација осуђеног на основу доступних информација и вести довести зависи и од елемената кривичног дела које је почињено. Губитак посла, изолација од заједнице и породице и нарушен углед у друштву само су неке од негативних последица за које су бивши окривљени тражили и добили обештећење. У појединим случајевима ове последице се протежу и на шири круг лица, погађајући не само окривљеног већ и чланове његове породице, децу или особе са којима су или су на други начин повезани.²⁰

Према подацима Уједињеног Краљевства, дигитални елемент је присутан у око 90% кривичних истрага. Методе дигиталног прикупљања доказа се временом мењају и добијају нове облике и домете. Неодговарајућа употреба нових технологија које још увек нису тестиране у сфери истражног поступка додатно подрива право на правично суђење и угрожава претпоставку невиности у раној фази истраге.²¹

Даље, компјутерски надзор скројен је тако да омогућава захватање података који нису ни намењени за пресретање и пренос. Ова врста задирања у информације, поред угрожавања права на претпоставку невиности, такође омета права на приватност, заштиту података и телекомуникацијску тајност, нарушава интегритет и поверљивост информационих система.

Поред истражних и полицијских превентивних мера за надзор који нарушавају право на претпоставку невиности, ту су и други начини у сфери информационих технологија којима се ова претпоставка ставља у ризик и то од стране јавности. Један од таквих примера јесу и друштвене мреже.

У зависности од начина коришћења друштвених мрежа, разни негативни ефекти на законом признате гаранције и права могу угледати светлост дана. Резултати су показали да активности на друштвеним мрежама могу утицати на права окривљених, да имају важну улогу у обликовању мишљења јавног мњења и утичу на правилно вођење кривичног поступка.

¹⁹ J. Coccoli, *op.cit.*, pp. 231-233

²⁰ D. Markov, *The presumption of innocence and the media coverage of criminal cases*, (2020); преузето 14.09.2023. <https://arisa-project.eu/the-presumption-of-innocence-and-the-media-coverage-of-criminal-cases/>

²¹ R. Stoykova, *op.cit.*, pp. 1

Кривична дела сматрају се богатим информативним материјалом који ће привући велику пажњу корисника, велики број “кликова” и “свиђања”, али и лавину коментара који обилују “сензационалним” информацијама из прве руке или фотографијама у вези са злочином. Међутим, објављивање, коментарисање и изношење нових информација на овакав начин сматра се директним нападом на право на претпоставку невиности. Корисници друштвених мрежа ретко износе поуздане информације и доказе, али се, у сваком случају, њихови коментари тумаче и доводе до забуне међу сведоцима, оптуженима, експертима, члановима цивилног друштва и агенцијама за кривично право.²²

Иако би њихов професионални интегритет генерално требало да их спречи у доношењу пристрасних одлука, судије у кривичном поступку ипак нису имуне на јавно мњење и притисак јавности. У светској историји бележе се примери где је јавност потенцијално надјачала и надгласала судску непристрасност, те се још увек сумња у правичност исхода тих поступака.

Упркос чињеници да се употреба савремених технологија надзора често спроводи у светлу потребе да се сузбију злочини и тероризам, у циљу заштите права на безбедност, истина је да ће критична и широка употреба ових технологија сигурно имати негативан утицај на људска права. У будућем периоду неминован је даљи развој технологија, а самим тим и напредовање постојећих и настанак нових дигиталних доказа који могу далекосежно утицати на поштовање права на претпоставку невиности. Владе су стога позване да усвоје правила и мере које ће обезбедити одговарајући приступ и успоставити равнотежу приликом коришења метода надзора путем савремене технологије, како би се истовремено обезбедила безбедност грађана, али и заштитила традиционално успостављена права која су изложена ризицима.

2.3. Право на образовање

Право на образовање је основно људско право дефинисано у члану 26 Универзалне декларације о људским правима као право сваког лица. Члан 26 даље наводи да “образовање треба да буде бесплатно бар у основним и нижим школама.

²² T. M. Shiyab, The impact of social media on the rights of the accused in Jordan: Does public opinion matter?, *Cogent Arts & Humanities*, Vol.8, 2021, Article 1994112, преузето 13.09.2023.
<https://www.tandfonline.com/doi/full/10.1080/23311983.2021.1994112>

Основно образовање је обавезно. Техничко и стручно образовање треба да буде свима подједнако доступно на основу њихове способности.”²³

Протокол бр. 1 уз Европску конвенцију о људским правима и основним слободама у члану 2 утврђује да “нико не може бити лишен права на образовање. У вршењу свих својих функција у области образовања и наставе, држава поштује право родитеља да обезбеде образовање и наставу који су у складу с њиховим верским и филозофским уверењима.”²⁴

Устав Републике Србије у члану 71 такође свим својим грађанима гарантује право на образовање, и то бесплатно и обавезно основно образовање, а приступ високошколском образовању омогућен је свим грађанима под једнаким условима.

Технологија је својом појавом и развојем донела промене које су се тичале упражњавања и поштовања овог права. Степен употребе технологије у сфери образовања (EdTech) последњих година расте у складу са технолошким развојем који се дешава на глобалном нивоу. Пандемија COVID-19 овај тренд додатно је убрзала услед чињенице да је највећи део ученика и студената широм света био погођен затварањем образовних институција, те је онлајн образовање преузело место традиционалног образовања у школским установама.

Међу предностима EdTech-а наводе се: побољшање приступа и квалитета образовања, примена методологија инклузивног учења, развијање пројеката виртуелног учења кроз које ученици из различитих земаља комуницирају и отварање могућности доживотног учења за све кроз формално и неформално образовање.²⁵ Међутим, иако нам се предности чине импресивним, оне нису загарантоване. Друга страна медаље са собом носи потенцијално правно и друштвено погубне последице: повећана искљученост и дискриминација, а не побољшан приступ; стандардизација уместо потенцијалне персонализације; већи стереотип, а не повећана разноликост, и ограничена аутономија и слобода уместо креативности и учешћа.

Такође, не сме се занемарити чињеница да технолошки развој није текао једнако у свим крајевима света - многи ученици у руралним и неразвијеним подручјима су се нашли искључени из школовања у тренуцима транзиције са традиционалног на онлајн образовање и не могу да приступе онлајн ресурсима због недостатка инфраструктуре, недоступности електричне енергије и електронских уређаја. Наставници и професори нашли су се, такође, пред изазовом да спроведу информатизацију свог добро

²³ Чл.26 Универзалне декларације о људским правима, 1948

²⁴ Чл.2 Додатног Протокола уз Конвенцију о људским правима и основним слободама, 1952

²⁵ М. Replitz, The socio-economic argument for the human right to internet access, *Politics Philosophy & Economics*, 2023, No.1, pp. 13

установљеног традиционалног начина подучавања. У зависности од научне области којом се баве, информационе технологије нуде им разне платформе и начине за осавремењивање предавања који би, такође, омогућили ученицима већи ниво интерактивности и жеље за новим, иновативнијим и комплетнијим сазнањима. То, међутим, изискује додатне напоре, посвећеност и обучавање наставног кадра, посебно у мање развијеним земљама где информационе технологије још увек нису ушле у све домове.²⁶

Као једна од најизраженијих и најзапаженијих последица коришћења EdTech-а у претходном периоду јесте повреда права на приватност деце и њихових породица. У журби да повежу децу са виртуелним учионицама, само неколико влада је проверило да ли је технологија која омогућава едукацију безбедна за децу. Као резултат тога, деца чије су породице могле да приуште приступ интернету и повезаним уређајима, или су се тешко жртвовале да би то учиниле, била су изложена праксама повреде приватности од стране EdTech платформи у виду надгледања деце, у већини случајева тајно и без њихове сагласности, прикупљајући податке о томе где су, шта раде у учионици, ко су њихова породица и пријатељи. Неке од платформи поседовале су и технологију за узимање отисака прстију што је остало трајно забележено у меморији платформе. Прикупљени подаци слати су трећим лицима, најчешће компанијама чија је основна делатност онлајн рекламирање.

Онлајн настава ученицима омогућава удобно окружење за образовање и огромне могућности за раст, али, с друге стране, доводе до стварања осећаја социјалне изолације. Ученици најбоље напредују у друштвено симулираном окружењу. Међутим, с обзиром на постављање онлајн часова, деца не успевају да остваре довољан социјални контакт који би их стимулисао да поједине научене и усвојене навике и знања преиспитају и дају им право значење.

Даље, онлајн часови такође ограничавају време и пажњу коју наставници могу да посвете својим ученицима. Као последица тога, ученици који захтевају додатну пажњу и вођство немају довољну интеракцију са лицима задуженим за њихово подучавање, те зато најчешће не успевају добро и потенцијално бележе неуспехе у образовању. Такође, онлајн образовање може бити доступно, али не и приступачно. Онлајн учење захтева скупу опрему као што су рачунари, лаптопови, таблети или паметни телефони. Дакле, ученици из недовољно економски развијених земаља су аутоматски изопштени и дискриминисани.

²⁶ Д. Тодоровић, Д. Прља, Д. Петровић, *op.cit.*, стр. 236-238

Са позитивне стране, платформе за учење на мрежи нуде разне курсеве и програме који оснажују ученике да истражују могућности изван домена њиховог наставног плана и програма. Штавише, пошто није могуће да наставници стално прате активности свих ученика, онлајн часови у њима усађују осећај одговорности и самодисциплине јер их се наводи да схвате да ће њихови поступци и немар имати дугорочан утицај на њихову будућност.

Мапирање и разумевање позитивних и негативних страна онлајн образовања омогућиће образовним институтима и технолошкој индустрији која омогућава онлајн образовање да установе стратегије за ефикасније пружање образовања. Истовремено, законодавна власт мора заузети проактиван став у осигуравању да основно право на образовање буде заштићено на све начине и форме без икаквог компромиса по добробит ученика.

2.4. Право на заштиту података о личности

Једно од уставом загарантованих права, касније детаљније уређено посебним законом јесте право на заштиту података о личности. Ово право најпре је дефинисано као уставом загарантовано право у члану 42 Устава Републике Србије којим је употреба података о личности изван сврхе за коју су подаци прикупљени забрањена и кажњива. Као изузетак од овог правила наведене су потребе вођења кривичног поступка или заштите безбедности Републике Србије, и то искључиво на начин предвиђен законом.

У Закону о заштити података о личности, податак о личности дефинише се како следи: “Сваки податак који се односи на физичко лице чији је идентитет одређен или одредив, непосредно или посредно, посебно на основу ознаке идентитета, као што је име и идентификациони број, података о локацији, идентификатора у електронским комуникационим мрежама или једног, односно више обележја његовог физичког, физиолошког, генетског, менталног, економског, културног и друштвеног идентитета”.²⁷

Дакле, податак у питању мора се односити на физичко лице, које је унапред одређено или је накнадно одредиво. Законска дефиниција не одређује конкретан начин сазнавања као ни средство којим је лице дошло у посед одређеног податка. Под личним податком сматра се било која информација која користи тачној идентификацији појединца као што су: име, физички или физиолошки подаци, ЈМБГ, адреса,

²⁷ Чл.4 Закона о заштити података о личности, *Службени гласник РС*, бр. 87/2018

фотографија, IP адреса и слично. Тумачењем дефиниције податка о личности, долазимо до закључка да се ради о информацијама доступним у било ком облику или медијуму.

Тема заштите података о личности представља релативно нову сферу у правном оквиру. Наиме, пре увођења информационо-комуникационих технологија у свакодневни живот људи, првобитни облици правне заштите односили су се на физички израђене документе који су садржали личне податке грађана. Тако изражени лични подаци који су се могли размењивати искључиво физичким путем нису се сматрали ризичном групом података којој је неопходна додатна правна заштита. Документи са личним подацима су чувани на физички изолованим местима која су се сматрала сигурним, што је довело до тога да није постојала потреба за детаљнијим правним регулисањем њихове заштите. Такође, мала важност личних података у друштву није налагала потребу за њиховим законским уређењем.

Заштита података о личности креће да привлачи посебну пажњу од тренутка настанка и развоја информационих технологија који је водио ка небројеним начинима не само прикупљања, већ и обраде и размене личних података остављеним на мрежама. Протеком времена људи су се све више ослањали на информационо комуникационе технологије и уређаје, а економски надмоћни субјекти су у том процесу пронашли начин да остваре још већу контролу над грађанима - корисницима њихових производа и услуга, што им је даље омогућило остваривање додатне моћи и доминације у сфери у којој обављају своју делатност.

Међутим, с друге стране нашли су се грађани који су препознали значај њихових личних података и информација које су доступне на мрежи, као и начине на које се исти ти подаци злоупотребљавају и бесправно размењују, те су отпочели своју борбу и побуну износећи све више информација о томе како се лични подаци размењују и користе за својеврсно праћење њихових преференција и навика. Један од најзначајнијих случајева у блиској историји јесте случај узбуњивача Едварда Сноудена коме је радно место информатичара у компанији повезаној са Националном Безбедносном Агенцијом САД омогућавало приступ „поверљивим“ информацијама у оквиру пројекта „Пет очију“. Априла 2012. године, Сноуден тајно преузима информације о прикупљеним подацима и дели их са јавношћу. Главни циљ овог “херојског” поступка било је расветљавање масовног кршења људских права које се спроводи надзором друштвених активности.

Када говоримо о регулаторним оквирима и прописима који регулишу питање заштите података о личности, почеци правне заштите података о личности сежу у 70.

године прошлог века, када је Шведска донела закон који ће касније служити као основ за европско законодавство у области заштите података. Један од основних принципа који овај закон доноси јесте да је обрада података који се налазе у јавним регистрима органа управе стављена под надзор шире јавности, заинтересованих лица као и тела која су посебно образована ради обављања послова заштите података. Имајући у виду напред речено, принцип транспарентности избио је у први план и представља један од најбитнијих основа заштите личних података.

Заштита података о личности на нивоу Европе најпре је регулисана Конвенцијом о заштити лица у односу на аутоматску обраду личних потока уз коју је касније усвојен и Допунски протокол, а затим и Протокол о изменама и допунама Конвенције о заштити лица у односу на аутоматску обраду личних потока. Такође, вреди поменути и Директиву 95/46 која је донета као смерница европским државама за израду националних закона. Као круна читавог европског регулаторног рада у области заштите података без икакве сумње може се навести Општа уредба о заштити података о личности (GDPR) која је на снази од 25. маја 2018. године, и у обавезној је примени у свим државама чланицама Европске уније.

Република Србија први закон у области заштите података о личности доноси 2008. године, а десет година касније, 2018. године исти бива замењен новим Законом о заштити података о личности који је својим одредбама испратио талас измена у области заштите података о личности. Закон је применљив како на аутоматизовану, тако и на неаутоматизовану обраду података о личности који чине или су намењени збирци података.

Закон прави јасну разлику између руковоаца (лице које одређује сврху и начин обраде) и обрађивача података (лице које обрађује податке о личности у име руковоаца); дефинише начела на којима се обрада података заснива (законистост, поштење, транспарентност); дефинише права лица на која се подаци односе; дефинише различито поступање приликом обраде података у посебне сврхе, обраде посебних врста података о личности, обраде у вези са кривичним пресудама и слично.

Као битан фактор у ланцу заштите података о личности закон одређује Повереника за заштиту информација од јавног значаја и заштиту података о личности. Повереник представља независан државни орган, који не подлеже непосредном или посредном спољном утицају и не може да тражи или да прима налоге од било кога. Као неке од најбитнијих дужности које повереник обавља у сфери заштите података о личности издвајају се следеће:

1. Вршење општег инспекцијског надзора над применом Закона о заштити података о личности
2. Утврђивање законитог поступања руковоаца
3. Давање претходног мишљења о утицају специфичне обраде на заштиту података о личности пре отпочињања обраде и креирања нове збирке података
4. Издавање сертификата о заштити података о личности
5. Предузимање одговарајућих мера у односима са органима надлежним за заштиту података о личности у другим државама и међународним организацијама
6. Давање мишљења Народној скупштини, Влади и другим државним органима о мерама у вези са обрадом а у вези са заштитом права и слобода физичких лица
7. Поступање по притужбама лица на које се подаци односе
8. Старање о подизању јавне свести о изазовима и ризицима које обрада личних података са собом носи, као и подизању свести руковоаца и обрађивача у вези са њиховим законом прописаним дужностима

Свако лице које сматра да су његова законом прописана права повређена начином прикупљања и обраде података има право да поднесе притужбу Поверенику, који по њој поступа без посебне накнаде. Повереник је у циљу поједностављења подшења притужбе прописао њен образац и могућност њеног подшења електронским путем. Лицу које поднесе притужбу и даље следује право да покрене друге поступке судске и управне заштите, што је евидентно у супротности са начелом *ne bis in idem* и може довести до правне несигурности. Против одлуке Повереника може се покренути управни спор у року од 30 дана.

Узимајући у обзир све интензивнији развој информационих технологија као и све већу количину личних информација које се налазе на мрежама, нужно је пратити развој права у области заштите подата о личности али и могућност Повереника као самосталног органа да искористи своја широко постављена овлашћења и испуни велики опсег обавеза које су му законом прописане.

Стални надзор и истраживања у области заштите података о личности, а посебно оних које се прикупљају, размењују и обрађују онлајн, од битне је важности за

предвиђање нових ризика по информације како би се исти дефинисали и како би се благовремено прописали унапређени системи њиховог надзора и заштите.

III ИНФОРМАЦИОНЕ ТЕХНОЛОГИЈЕ И ДИГИТАЛНА ПРАВА

Дигиталне технологије трансформишу начин на који се основна права као што су слобода изражавања и приступ информацијама остварују, штите и злоупотребљавају, али такође воде ка признавању нових, дигиталних права. Закон се стога прилагођава новој ери са развојем дигиталних права и дигиталног грађанства, дозвољавајући и регулишући приступ онлајн информацијама на безбедан и транспарентан начин.

Дигитална права сматрају се надградњом права утврђених у Универзалној декларацији о људским правима од стране Уједињених нација која се примењују на онлајн свет. Главни циљ је да гарантују приступ интернету, избегавајући дигитални јаз, и правилно коришћење мреже као заједничког добра целог човечанства. За разлику од традиционално утврђених људских права, дигитална права су флексибилна и подложна променама које су условљене развојем и трансформисањем дигиталних технологија.²⁸ У наставку рада бавићемо се настанком и развојем три дигитална права: права на приступ интернету, права на информационо самоодређење и права на заборав.

3.1. Право на приступ интернету

Кроз историју се доказало да новонастале комуникационе технологије имају трансформишући и револуционарни ефекат на друштво. Узмимо за пример Гутенбергову штампаћу машину чијим је настанком и применом забележен утицај на протестантске реформе. Радио је имао запамћени ефекат у јеку народне побуне на Филипинима, која је резултовала збацивањем режима Фердинанда Маркоса 1986. и обнављањем демократије у овој земљи.²⁹ Можемо се, дакле, сложити да је улога информационо комуникацијских технологија велика и добија све већи значај с временом.

Ипак, интернет се по својим функцијама разликује од других начина информисања и комуникација. За разлику од радија, телевизије, и других облика комуникације који су контролисани и креирани од стране емитера и уредника, интернет пружа могућност неограничене комуникације one to one (преко е-маила), one to many (преко личних страница, блогова, твитера) и, можда најбитније, many to many (онлајн

²⁸ M. Nastić, The Impact of Informational and Communication Technology on the Realization and Protection of Human Rights, *Balkan Social Science Review*, 2021, Vol. 17, pp. 83

²⁹ Wikipedia, *Journalism during the Marcos dictatorship*, преузето: 02.12.2023.
https://en.wikipedia.org/wiki/Journalism_during_the_Marcos_dictatorship

четови, комуникација путем налога на друштвеним мрежама као што су Фејсбук или Линкедин).³⁰

Дакле, имајући у виду претходно речено, интернет пружа могућност да се информације преносе даље и брже, међу већим бројем корисника, те тако умањује трошкове стварања, проналажења, обраде, преношења и приступа информацијама и повећава потребу прилагођавања дигиталним технологијама широм света. Интернет се данас сматра једним од основних алата за остваривање основних социо-економских људских права као што су: образовање (у време савремених информационих технологија моге сфере образовања обликовале су се у складу са технолошким напретком, те је многе свакодневне активности и изазове у образовању готово немогуће обавити без посредства интернета), здравље (интернет је, између осталог, пружио могућност развоја апликација и платформи које омогућавају корисницима брзу комуникацију са стручним лекарским особљем, посебно у случајевима хитних интервенција особа којима лекарска помоћ није физички доступна, и то преко онлајн консултација и саветовалишта), рад (интернет је неопходно средство за рад почевши од конкурисања за жељено радно место па до обављања радних обавеза, посебно у време актуелности тзв. „рада од куће“).

Међутим, приступ модерним дигиталним технологијама не доноси увек са собом позитивне резултате и последице. Забележен је пораст злоупотребе технологија у последњих неколико деценија у виду искоришћавања исте у сврху ширења и чињења доступним дечије порнографије, дигиталних превара, крађе идентитета, говора мржње, трговине људима, тероризма, али и неосноване или нелегалне цензуре или ускраћивања приступа интернету од стране владе. Оно што су корисници интернета навели као највећу забринутост у вези са коришћењем интернета, па тако и у вези са проглашењем права на приступ интернету људским правом јесу: опасности од преваре, лак приступ насилном и експлицитном садржају и бриге око приватности.³¹

Државе су често регулишући одређену правну сферу довели у питање постојање и поштовање права на слободан приступ интернету. Један од примера неуставне и незаконите одредбе нашао се у француском закону о кршењу ауторских права на мрежи, чијом се одредбом установљава Високи орган за дифузију ауторских дела и заштиту ауторских права на интернету, који је имао овлашћења за санкционисање која су се протезала на ограничавање или ускраћивање приступа интернету одређеним

³⁰ Q. Qerimi, Bridge over Troubled Water: An Emerging Right to Access to the Internet; in: *International Review of Law*, 2017, pp. 4

³¹ BBC NEWS, *Internet Access is 'a Fundamental Right'*; преузето 12.09.2023
<http://news.bbc.co.uk/2/hi/technology/8548190.stm>

претплатницима. Његова овлашћења нису била ограничена ни на једну конкретну категорију лица, већ су укључивала читаву популацију. Суд је пресудио да таква широка овлашћења, поверена органу који је поверен за заштиту ауторских права, за разлику од суда, може довести до ограничења права на слободу изражавања и комуникације, посебно до ограничавања могућности да се ова права остварују из свог дома. Након овакве пресуде суда, уведен је нови поступак, где тек након треће опомене осумњичени корисник бива позван пред суд, који му као меру може изрећи укидање приступа интернету до једне године.³²

С друге стране, битно је напоменути још један проблем који се јавља са приступом интернету - немогућност његовог једнаког остварења у свим крајевима света. Појава коју можемо назвати “дигиталном подвојеношћу” и даље је актуелна. Она подразумева јаз између људи и области са активним приступом интернету и оних који имају врло ограничени или немају никакав приступ интернету. Према истраживањима спроведеним 2019. године, просечан проценат становништва које има приступ интернету износи 57,3%. Као континент са најнижим степеном интернет пенетрације издвојила се Африка са 39,8%, док се Северна Америка са 89,4% издвојила као континент са највећим процентом становништва који има приступ интернету.³³

Садашњи трендови у доношењу одлука на глобалном нивоу о праву на приступ интернету далеко су од уједначених. Међутим, не смеју се занемарити напори који се улажу на регионалним нивоима, највише унутар ЕУ (Грчка, Шпанија, Италија, Француска, Пољска).³⁴ Ове примере треба тумачити као охрабрујуће, те као показатеље да је изванредан напредак могућ, посебно када су развијене земље у питању.

Неке од земаља ЕУ су донеле законе којима су регулисале право на приступ интернету (Естонија и Финска), међутим, начин на који је право на приступ интернету регулисано разликује се од земље до земље. Многе владе оформиле су своју мисију која се огледа у томе да саме поставе оптичку мрежу или да у великој мери субвенционишу инвестиције приватне компаније – или групе компанија – које одлуче да се баве овим послом. У сваком случају, начин спровођења овог права ће у великој мери зависити од традиционалног и тренутног окружења регулације телекомуникација, димензија нације и дистрибуцији становништва, профила постојећих телекомуникационих предузећа и

³² N. Lucchi, Access to Network Services and Protection of Constitutional Rights: Recognizing the Essential Role of Internet Access for the Freedom of Expression, *Cardozo Journal International & Comparative Law*, No. 3, Vol.19, pp. 650-652

³³ Voitsikhovskiy A, Bakumov O, Ustyomenko O, Syroid T, The Right of Access to the Internet as Fundamental Human Right given the Development of Global Information Society, *The Law, State and Telecommunications Review*, 2021, No.1, Vol. 13, pp. 2

³⁴ M. Nastić, *op.cit.*, pp. 86-87

нивоа економског развоја који доживљава друштво. Право на приступ интернету свакако не подразумева да оно мора бити бесплатно, већ само да мора бити доступно, приступачно и адекватно обезбеђено. Ако било шта од наведеног недостаје, позитивна обавеза да се обезбеди прави приступ интернету не може бити испуњена.³⁵

Када говоримо о глобалном установљавању права на приступ интернету, најконсолидованија правна мера на међународном нивоу до сада остаје Директива 2002/22 Европског парламента и Савета, позната као Директива о универзалним услугама. „Универзални сервис“ је замишљен овом Директивом као обезбеђивање електронских телекомуникационих мрежа и дефинисање минималног скупа квалитетних, јавно доступних услуга свим крајњим корисницима по приступачној цени.³⁶

Уједињене нације су, такође, на својој генералној седници усвојиле документ “Трансформисање нашег света: Агенда за одрживи развој 2030”, где се под циљем 17 дефинише и приступ информационо- комуникационим технологијама.

Изван напред поменутих напора ка остварењу и стварању института права на приступ интернету, не постоји интернационални правнообавезујући акт који налаже државама да својим становницима обезбеди универзално право на приступ интернету. Ово свакако не спречава даљу анализу и тежњу ка успостављању интернационалних инструмената којима ће се креирати не само обавеза да се лицима обезбеди приступ интернету, већ и забрана да се ово право злоупотребљава или на било који начин неосновано ограничава.

Ширим тумачењем члана 19 Универзалне декларације о људским правима којим се право на слободу мишљења и изражавања даје сваком, и наводи да исто подразумева и право да лице тражи, прима и шири идеје и информације “*било којим средствима и без обзира на границе*”³⁷ долази се до закључка да је исти састављен са предвиђањем да укључи и да прилагоди будући технолошки развој кроз који појединци могу да остваре своје право на слободу изражавања. Стога, међународни регулаторни оквир људских права остаје релевантан и применљив чак и на интернет.

Поставља се питање: да ли би међународне организације и институције уопште требало да усмеравају развој интернационалних прописа и регулисање основних људских права тако да право на слободна приступ интернету постане једно од њих?

³⁵ A. Picot, C. Wernick, The Role of Government in Broadband Access; in: *Telecommunication Policy*, New York, 2007, pp. 671

³⁶ Art. 1&2, Council Directive 2002/21/EC of the European Parliament and of the Council (on a common regulatory framework for electronic communications networks and services), 2002

³⁷ Чл. 19 Универзалне декларације о људским правима, 1948

Технологија (у коју сврставамо и интернет) најпре треба да служи обезбеђивању несметаног уживања основних права. Упитна је тежња сврставања приступа интернету у ред људских права, посебно имајући у виду високо постављену лествицу да би се нешто сматрало људским правом. Један од битнијих критеријума које би одређена активност/уздржавање требало да испуни како би се сматрала људским правом јесте да је неопходна како би човек водио здрав и смислен живот. Сврставање права на приступ интернету у ред грађанских права би могло да има више основа и оправдања узевши у обзир да су грађанска права дата законом, за разлику од људских права која су концептуално заснована на урођеном људском достојанству и задржавају свој универзални и неотуђиви карактер.³⁸

3.2. Право на информационо самоодређење

Право на информационо самоодређење изведено је из права на слободан развој личности и општег права на достојанство садржано у члану 2 Устава, а први пут је артикулисано одлуком Савезног уставног суда Немачке којом је 1983. године прогласио неуставном одредбу Закона о попису становништва која је оспоравана од стране разних еминентних удружења за заштиту основних људских права³⁹. Одлуком је установљено да “основно право гарантује способност појединца да у принципу одреди откривање и коришћење његових личних података”⁴⁰. Суд је даље право дефинисао као “овлашћење појединца да сам одлучује, на основу идеје самоопредељења, када и у којим границама информације о његовом приватном животу треба саопштавати другима”.⁴¹

Обим заштите права на информационо самоодређење није ограничен на информације које су већ осетљиве по својој природи и стога су заштићене основним правима. У зависности од сврхе и постојећих опција обраде и повезивања, руковање личним подацима, који сами по себи имају само мало информативног садржаја, може имати утицаја у вези са основним правима на приватност и слободу понашања дотичне особе. У том смислу, у условима електронске обраде података, више нема небитних личних података, без обзира на контекст коришћења.

³⁸ D. Eloff, *The Nature of Rights and Access to the Internet*, Department of Law, Akademia, 2023, pp. 45-49

³⁹ Decision of the Federal Constitutional Court of Germany as from 15 December 1983, 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83. Преузето 25. 07. 2023.

https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1983/12/rs19831215_1bvr020983.html

⁴⁰ *Ibid.*

⁴¹ Dr. A. Rouvroy, Prof. Y. Pouillet - *The right to informational self-determination and the value of self-development. Reassessing the importance of privacy for democracy*, Springer, Dordrecht, 2009, pp. 3

Ако неко није сигуран да ли се девијантно понашање бележи и трајно чува као информација, или се примењује или прослеђује, трудиће се да таквим понашањем не привуче пажњу. Уколико сматра да ће учешће у грађанској иницијативи бити званично регистровано и да из тога произилазе лични ризици и потенцијалне мере, могуће је да се одређи остваривања својих права. Ово не само да би утицало на његове шансе за развој, већ би утицало и на опште добро, јер је самоодређење елементарни функционални услов слободног демократског друштва заснованог на способности грађана да делују и сарађују.

Иако право на информационо самоодређење даје гаранцију да појединци могу сами да одлучују када и у којим границама ће открити податке из свог личног живота, ова гаранција може бити ограничена у интересу јавности, под условом да је ограничење пропорционално и засновано на закону; ограничење не може бити шире него што је апсолутно неопходно ради заштите јавних интереса.⁴²

Много година након првобитне правне артикулације, ово право добија све већи значај појавом информационих технологија, њиховим унапређењем и аутоматизацијом. Интернет је успео да у великој мери поткопа унапред одређене вредности и значај овог права и данас су лица практично изгубила контролу над прикупљањем, откривањем и коришћењем њихових личних података.

Употреба информационих технологија се од почетка сматрала као погоршање асиметрије моћи између субјеката података (појединаца чији се подаци обрађују) и контролора података (задужених за прикупљање, складиштење, обраду, употребу и ширење података). Технолошки развој постепено је довео до ситуације у којој готово да не постоји ограничење количине информација које се могу снимити, не постоји ограничење обима анализе које може да се уради, а информације се могу чувати практично заувек.⁴³

У практичном делу овог рада обрађено је неколико одлука Савезног уставног суда Немачке у вези са правом на информационо самоодређење, а које је изведено из права на слободан развој личности и општег права на достојанство садржано у члану 2 Устава.

Право на информационо самоодређење гарантује способност појединца да у принципу одреди откривање и коришћење његових личних података, односно његово

⁴² М. Настић, *Уставна заштита људских права*, Ниш, 2021, стр. 239

⁴³ Н. Nissenbaum, *Protecting Privacy in an Information Age: the Problem of Privacy in Public*; in: *Law and Philosophy*, New York, 1998, pp. 576

овлашћење да сам одлучује када и у којим границама информације о његовом приватном животу треба саопштавати другима.

Анализом судске праксе уочава се велики помак у заштити права појединца на информационо самоодређење и тежња да се грађанима пружи адекватна заштита која је загарантована уставом и законима. Суд је, такође, утврдио границе овог права и поставио услове чијим испуњењем оно може бити ограничено. Дакле, упркос чињеници да право на информационо самоодређење даје широка овлашћења појединцу, суд је својим одлукама утврдио да ово право није гарантовано без икаквих ограничења, те да потенцијална ограничења морају бити оправдана претежним интересима заједнице. Као услов за ограничење овог права наводи се да ограничења морају бити прописана законом, да морају одговарати начелу сразмерности и захтеву за јасноћом норми.

С друге стране, са порастом примене вештачке интелигенције, аналитике великог обима података и других трансформативних технологија, потенцијал за невиђене инвазије на приватност експоненцијално је порастао. Стога постаје још важније ојачати ово право и осигурати да предности технолошког напретка не иду на штету личних и грађанских слобода.

У годинама које следе биће од велике важности пратити развој права на информационо самоодређење и изазове са којима ће се законодавци и судови сусретати у тежњи да га што боље дефинишу, тумаче, а касније и заштите.

3.3. Право на заборав

У људској природи је да активно истражује друштво и свет око себе. Са развојем технологије радозналост добија нове оквире, те је човек радознао да сазна какве се информације појављују кад је њихово име предмет претраживања на интернету. Међутим, имајући у виду лакоћу ширења информација о нашем приватном и јавном животу онлајн, резултати претраге често и нису тако повољни, а такође постоји вероватноћа да њихова истинитост није потпуна. Европски регулатори верују да се сви грађани суочавају са потешкоћама да побегну од своје прошлости сада када интернет све бележи и ништа не заборавља.

На питање да ли и шта можемо учинити да резултати неповољни по нас “нестану” с интернета одговор је право настало у претходној деценији - право на

заборав.⁴⁴ Настанак права на заборав датира из 2014. године као последица и одговор на убрзани технолошки напредак и све већи број информација које се чувају у готово безграничној меморији интернета.⁴⁵

Пред Европским судом правде, те 2014. године, водио се случај Google Spain⁴⁶ у вези са резултатима претраге Марија Костеје Гонзалеса на Google претраживачу. Суд је утврдио да Директива 95/46 чланом 12 даје субјекту података право на брисање личних података који се односе на њу/њега. Субјекту је, дакле, омогућено да се директно обрати претраживачу са захтевом за спречавање индексирања информација и података која су у директној вези с њим.

Доношењем Опште уредбе о заштити података о личности (GDPR) Европска унија прописује и гарантује право на заборав својим грађанима. Ова уредба прописује на који начин се лични подаци грађана ЕУ штите од стране посредника и провајдера.⁴⁷

Дакле, када подносилац захтева за уклањање информација поднесе релевантне и довољне доказе који доказују очигледну нетачност података и поткрепи свој захтев за уклањање информација, оператер претраживача је дужан да удовољи том захтеву. Приликом одлучивања о уклањању података, претраживачи морају да размотре да ли су дотичне информације „нетачне, неадекватне, ирелевантне или сувишне“ и да ли постоји јавни интерес да информације остану доступне у резултатима претраге.⁴⁸

Да би пратио упутства Европског суда за људска права, Google је установио систем на мрежи који обрађује и процењује захтеве и покушава да уравни права на приватност појединца са правом јавности да приступи информацијама и дистрибуира их. Стручни тим обрађује сваки захтев и оцењује оправданост захтева на основу фактора као што су: улога подносиоца у јавном животу, одакле информација потиче, колико је стар садржај у коме се информација налази, утицај на кориснике Google

⁴⁴ Lexology, Intellectual property blog, *Right to be forgotten: developments with regard to de-referencing in the light of inaccurate information*, преузето 02.09.2023.

<https://www.lexology.com/library/detail.aspx?g=d63e8758-1ffc-4273-a767-5ca772642d3b>

⁴⁵ М. Настић, *op.cit.*, стр. 240

⁴⁶ Пред Европским судом правде 2014. године повео се случај C-131/12 Google Spain SL v. Mario Costeja González. González је поднео жалбу шпанској агенцији за заштиту података (AEPD) против Google Spain и шпанског листа La Vanguardia. Подносилац жалбе је изнео да Google претрага његовог имена резултира линковима који воде ка новинским чланцима из 1998. године који говоре о заплени његове имовине због дугова, што је, по његовом мишљењу, застарела и ирелевантна информација. Европски суд правде је утврдио одговорност за обраду личних података претраживача попут Google-a, те да појединци имају право да захтевају уклањање одређених резултата претраге када су подаци неадекватни, или ирелевантни. Ова пресуда сматра се зачетком "права на заборав", омогућавајући појединцима да траже уклањање личних података из резултата претраге под одређеним условима.

⁴⁷ Lexology, Vaish Associates Advocates, *Right to be forgotten*, преузето 09.09.2023.

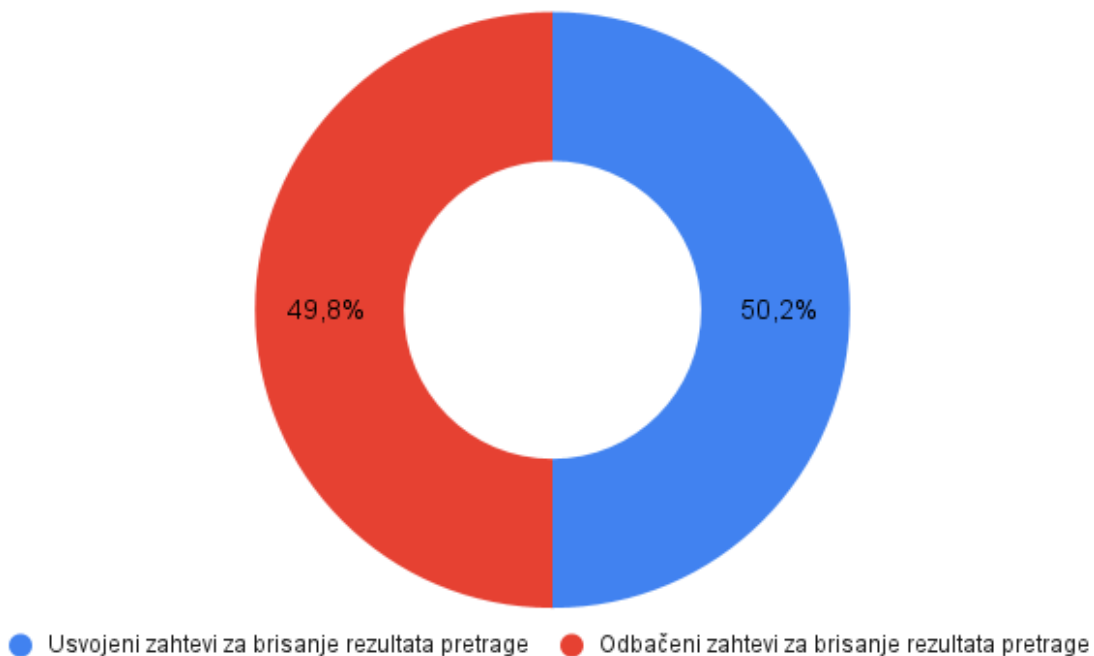
<https://www.lexology.com/library/detail.aspx?g=e0dc65db-85eb-4a93-afa0-30597fb2a037>

⁴⁸ Lexology, Stevens & Bolton LLP, *The right to be forgotten - recent updates for navigating the freedom of information*; преузето 10.09.2023

<https://www.lexology.com/library/detail.aspx?g=f17dd4ab-75da-47b9-8fa4-429e986d5656>

производа, тачност, осетљивост података.⁴⁹ Ефекат усвајања захтева јесте да се одређени резултати више неће појављивати приликом претраживања имена подносиоца на претраживачу, али ће садржај који садржи критичне информације и даље бити доступан као резултат других претрага.⁵⁰

Према званичним подацима доступним на Google платформи, укупан број придошлих захтева за брисање података износи 1,576,276, а укупан број веб-страница чије је брисање тим захтевима тражено износи 6,128,524. Највећи број уклоњених резултата потиче са друштвених мрежа и платформи као што су Facebook, Twitter (X), Youtube.⁵¹ Процентуални однос усвојених и одбачених захтева за брисање података на платформи Google може се наћи на графикону испод.



Слика 1. Графикон са процентуалним приказом усвојених и одбачених захтева за брисање података на Google платформи. Извор: <https://transparencyreport.google.com/eu-privacy/overview?hl=en>

Уколико одређени случај у вези са брисањем података и правом на заборав доспе пред суд, суд при одлучивању о применљивости права на заборав у специфичном случају процењује факторе као што су: природа спорних информација, какав утицај на

⁴⁹ Google Support - Legal Help, *Right to be Forgotten Overview*; преузето 09.09.2023. <https://support.google.com/legal/answer/10769224?hl=en>

⁵⁰ The NATO Cooperative Cyber Defence Centre of Excellence, *“Right to be Forgotten” or “Right to Know”?*; преузето 10.09.2023. <https://ccdcoe.org/incyber-articles/right-to-be-forgotten-or-right-to-know/>

⁵¹ Requests to delist content under European privacy law, преузето 20.04.2024. <https://transparencyreport.google.com/eu-privacy/overview?hl=en>

лице могу имати дате информације уколико остану доступне јавности, да ли постоји јавни интерес за задржавање таквих информација и слично.⁵²

Право на брисање података у великој мери се користи од стране лица против којих се водио судски поступак од великог јавног значаја, лица која су из било којих разлога у прошлости стављани на тзв. “црне листе” (од којих многи на професионалне црне листе чиме се угрожава њихова репутација и даљи професионални развој). С друге стране, жртва такође има право на уклањање садржаја који крши њено право на приватност и има „право да буде заборављена“. Ово се посебно односи на актере/жртве сексуално експлицитних слика и другог порнографског садржаја.

Упркос великој важности и корисности права на заборав, постоје ипак одређени изазови са којима се поштовање и исцрпљивање овог права сусреће. Наиме, поставља се питање кошења овог права са правом на слободу говора и изражавања. У случају обавезе креатора да услед заштите права на заборав одређени садржај обрише са канала и веб-страница то ће утицати на њихово право на слободу говора и изражавања. Такође, право на заборав може потенцијално утицати и на право појединца на информисање, а новинари ће, иако носиоци једног од стубова демократије, имати ограничења и сметње у својој активности преношења информација у медијима. Све ово су аргументи које истичу они који се залажу против права на заборав у смислу заштите података.⁵³

Међутим, они који се залажу за право на заборав, наводе околности као што су порнографија освете и штета коју она наноси људима као јасан разлог за њено постојање. Исти аргумент у прилог укључује случајеве да резултати претраге покупе нечије раније кривичне осуде или информације о личности.

⁵² Lexology, TMT Law Practice, *Right to be forgotten*, преузето 10.09.2023.
<https://www.lexology.com/library/detail.aspx?g=abd8fb99-391d-4f35-a44d-68360ea1e670>

⁵³ Z. Ahmad, Manupatra Articles, *Right to be forgotten* (2022); преузето 15.09.2023.
<https://articles.manupatra.com/article-details/Right-to-be-forgotten>

IV СУДСКА ПРАКСА САВЕЗНОГ УСТАВНОГ СУДА НЕМАЧКЕ

Савезни уставни суд Немачке се у око 70 година постојања развио у угледног и активног актера у државној структури Савезне Републике Немачке захваљујући богатој пракси, посебно у вези са одлучивањем о заштити основних права грађана.

Бројне одлуке овог суда из темеља су уздрмале систем заштите основних права и креирале трендове развоја и тумачења истих. Наиме, број поднетих представки и жалби пред овим судом указује на озбиљно кршење загарантованих основних људских права у Немачкој, на основу чега се може претпоставити да су истоветна кршења присутна и у свим другим европским државама, али и свим другим крајевима света.

Из горе поменутих разлога који потврђују значај овог суда у заштити људских права, у овом делу рада посебну пажњу посвећујемо тумачењу неколико одлука Савезног уставног суда Немачке у области заштите права на информационо самоодређење⁵⁴, које је први пут дефинисано одлуком овог суда BVerfGE 65, 1 из 1983.године.

4.1. 2 BvR 939/13

Уставном жалбом подносилац оспорава налог Окружног суда да се од њега узме узорак ћелијског ткива, како би исто било предмет генетског и молекуларног испитивања, а све у циљу утврђивања идентитета у будућем кривичном поступку, наводећи да такав поступак представља повреду права на информационо самоодређење у складу са чланом 2.1. Основног закона Немачке.⁵⁵

Пресудом Окружног суда у Хамбургу из фебруара 2012. године, подносилац представке осуђен је за руковање украденом робом⁵⁶ и осуђен на казну затвора у трајању од једне године и пет месеци. Извршење казне накнадно је суспендовано, те је

⁵⁴ Више о праву на информационо самоодређење може се наћи у одељку 3.2. овог рада

⁵⁵ Order of the Third Chamber of the Second Senate as of 29 September 2013, 2 BvR 939/13. Преузето 25.07.2023.

https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2013/09/rk20130929_2bvr093913en.html

⁵⁶ Art. 259(1) Strafgesetzbuch für das Deutsche Reich (StGB), 1871 - Кривични законик Савезне Републике Немачке; преузето: 11.09.2023.

<https://lexetius.com/leges/StGB/Inhalt.jsessionid=node05grafoxopm1p1triatdmrnyng8389.node0?0>

подносиоцу представке одобрена условна казна у складу са чланом 56.1. и 56.2. Кривичног законика.

У вези са горе наведеном пресудом, а на основу Закона о кривичном поступку,⁵⁷ Хамбуршки локални суд је наложио прикупљање ћелијског ткива од подносиоца представке и његово подвргавање молекуларном и генетском испитивању. Ова мера образложена је аргументом да упркос чињеници да подносилац представке није раније осуђиван, количина и вредност украдене робе јасно указују на то да је код подносиоца присутан тежак поремећај личности, те се чини могућим да ће против њега у будућности бити вођене истраге због сумње да је да је починилац кривичних дела од велике важности. Све то одовело је до налога суда да као меру одреди прикупљање доказа који садрже ћелијско ткиво. Окружни суд у Хамбургу је одбацио жалбу подносиоца представке против овог налога као неосновану.

Треће веће Другог сената Савезног уставног суда усвојило је уставну жалбу на одлучивање и оценило да је дозвољена и основана. Ова одлука је заснована на разматрањима наведеним у наставку.

Најпре, узимање, чување и (будућа) употреба ДНК профила омета основно право на информационо самоодређење загарантовано чланом 2.1. у вези са чланом 1.1. Основног закона. Ово право даје гаранцију да појединци могу сами да одлучују када и у којим границама ће открити податке из свог личног живота. Ова гаранција може бити ограничена само у интересу јавности, под условом да је ограничење пропорционално и засновано на закону; ограничење не може бити шире него што је апсолутно неопходно ради заштите јавних интереса. Приликом тумачења и примене одговарајућег члана Закона о кривичном поступку, суд мора на адекватан начин размотрити значење и обим овог основног права.

Као други аргумент истиче се да је за изрицање мере у складу са Законом о кривичном поступку нужно да због природе кривичног дела, начина његовог извршења, личности осуђеног учиниоца, или због других околности, постоје разлози који указују да ће се против њега убудуће водити кривични поступак због кривичног дела од битног значаја. Ова одлука захтева да јој је претходило довољно разјашњење чињеница, те да исте буду свеобухватно изложене у образложењу одлуке.

Оспорене одлуке нису испуниле напред наведене уставне услове. Судови нису укључили све околности које су биле релевантне за неопходну равнотежу или их нису у

⁵⁷ Art. 81(g) Strafprozeßordnung (StPO), 1950 - Закон о кривичном поступку Савезне Републике Немачке, преузето: 12.09.2023.
<https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/82015/97990/F1944933040/stpo.pdf>

потпуности навели и образложили. Савезни уставни суд је тако преиначио одлуке локалног суда у Хамбургу и регионалног суда у Хамбургу и вратио предмет на поновно одлучивање.

4.2. BVerfGE 120, 238

Уставна жалба у овом предмету усмерена је на полицијске прописе донете у Немачким покрајинама Хесе и Шлезвиг-Холштајн, а којима се допушта аутоматизовано препознавање регистарских таблица моторних возила.⁵⁸⁵⁹

Аутоматизовано препознавање регистарских таблица подразумева оптичко снимање возила видео камером, те читање ознака регистарских таблица уз помоћ посебно креираног софтвера. Уколико се након аутоматског упоређивања регистарских таблица са полицијским досијеима истраге установи да се регистарска таблица налази у бази података, издаје се порука о поготку. Уколико снимљене регистарске таблице нема у бази података, слика и снимљена регистарска таблица ће се одмах избрисати.

Својим уставним жалбама подносиоци наводе повреду њиховог основног права на информационо самоодређење из члана 2.1. у вези са чланом 1.1. Устава. Уставна жалба усмерена је против закона, а уставна жалба је допуштена јер се наведеним прописима повређена основна права непосредно, лично и тренутно.

Подносиоци жалбе сматрају себе лицима чија су основна права овим прописима директно угрожена. Они су регистровани власници путничких аутомобила, којима се редовно крећу путевима савезне државе и врло је вероватно да ће бити подвргнути контроли регистарских таблица која се спроводи у складу са оспореним прописима.

Снимање регистарских таблица има за циљ да прикупљени подаци буду доступни државним системима за обраду података како би се могли упоредити са са подацима из полицијских истражних досијеа, чиме се омета основно право на информационо самоодређење. Брисање у случајевима непогођених и лажних погодака се дешава тек након поређења, тако да долази до задирања у основна права.

Државни парламент и државна влада Шлезвиг-Холштајна, државна влада Хесена и независни државни центар за заштиту података Шлезвиг-Холштајн изјаснили су се на наводе уставне жалбе. Неки од аргумената којима су оправдавали аутоматско читавање регистарских таблица наведени су у наставку:

⁵⁸ Фондација Konrad Adenauer e.V. - Изабране одлуке Немачког Савезног уставног суда, Санкт Аугустин, Немачка (2009), Превод: проф. др. Един Шарчевић, стр.123

⁵⁹ Judgment of the First Senate of March 11, 2008, BVerfGE 120, 238 , 1 BvR 2074/05. Преузето 28.07.2023. https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/03/rs20080311_1bvr207405.html

1. Поређење се врши одмах након снимања. У случају промашаја, произведена слика и низ знакова броја регистарске таблице биће аутоматски избрисани из нестабилне меморије читача за мање од једне секунде.
2. Поређење се показало као делотворно и даје високи број погодака који укључују кривично гоњење, те се употреба овлашћења снимања таблица може сматрати оправданом и корисном.
3. Прописи су јасни и конкретни - јасно наводе надлежни орган, разлог прикупљања података и њихову намену.

Након расправе сенат је усвојио уставне жалбе. Подносиоци жалбе су непосредно, лично и тренутно погођени у својим основним правима.

Уставне жалбе су основане. Оспореним одредбама је повређено опште право личности подносилаца притужби из члана 2.1. у вези са чланом 1.1. Основног закона у његовом испољавању као основног права на информационо самоодређење. Право на информационо самоодређење односи се на угрожавање и повреду личности који карактеришу обраду података у савременим условима и који произилазе из мера које се односе на информације. Ово право утврђује и проширује заштиту основног права на подручју слободе понашања и приватности; оно започиње већ на степену угрожавања личности. Ово право обухвата ситуације које могу настати и пре конкретног напада на правна добра.

Помоћу електронске обраде података, поједини лични детаљи особе могу се чувати на неодређено време и комбиновати са другим збиркама података, што резултира широким спектром могућих употреба и веза, а касније и њиховој даљој генерацији и извођењу закључака.

Задирање у право на информационо самоодређење се проширује ако се чувају додатни подаци, као што су подаци о локацији или смеру кретања моторног возила, који би директно водили добијању додатних информација о кретању особе.

Аутоматске провере регистарских таблица за тражење људи или ствари су интервенције велике тежине, те је неопходно да се исте заснивају на разлозима који служе за заштиту значајног јавног интереса. Неограничено овлашћење да се врше провере регистарских таблица да би се спречиле одређене опасности или, још више, да би се заштитила приватна права и други неодређени задаци полиције, није уставно оправдано.

Обим заштите права на информационо самоодређење не ограничава се само на информације које су по својим карактеристикама осетљиве, већ се односи на податке који се тичу личности, који имају незнатан информативни садржај, али који према свом циљу и постојећим могућностима обраде и спајања могу имати релевантан учинак на приватност и слободу понашања лица.

4.3. 1 BvR 2649/21

По свом циљу и ефектима, обавеза пружања доказа о вакцинацији против COVID-19 из става 20а Закона о заштити од зараза представља директно мешање у члан 2.2. Основног закона којим се појединац штити од државних мера које нарушавају физички интегритет и с тим повезано право на информационо самоодређење.⁶⁰

Оспорене одредбе донете су у вези са глобалном пандемијом изазваном вирусом SARS-CoV-2 и болешћу COVID-19.

Оспорене одредбе намећу обавезу пружања доказа о вакцинацији или опоравку од COVID-19 особљу у сектору здравства и неге. Особље у одређеним здравственим установама и организацијама је у обавези да буде потпуно вакцинисано против COVID-19 или да се опоравило од болести, те о томе мора доставити менаџменту своје установе или организације доказ, а све у складу са оспореним законом. Уколико се до одређеног рока не достави доказ о вакцинацији или опоравку или ако постоје сумње у његову аутентичност или тачност, руководство дотичне институције или организације мора без непотребног одлагања обавестити локални јавни здравствени орган.

Особе које тек почну да раде у одређеним здравственим институцијама или организацијама морају поднети тражени доказ пре ступања на рад. У супротном, они од самог почетка не могу бити запослени у таквим институцијама или организацијама, нити радити у њима.

Жалиоци оспоравају спорне одредбе у својству лица која подлежу обавези давања доказа о вакцинацији или опоравку, те тврде да обавеза давања личних података локалном јавном здравству представља повреду права на информационо самоодређење.

Када законске одредбе доводе до мешања у основна права, таква мешања могу бити оправдана само ако законодавац следи уставно легитимне циљеве. Да ли законодавац тежи легитимним циљевима је предмет ревизије Савезног уставног суда. С тим у вези, Савезни уставни суд није ограничен на преиспитивање циљева које је изричито одредио законодавац. За законе које законодавац доноси у циљу решавања ситуација за које претпоставља да угрожавају општу јавност или правне интересе појединаца, ревизија коју спроводи Савезни уставни суд обухватиће испитивање да ли су такве претпоставке које је изнео законодавац засноване на довољно чврстим темељима.

⁶⁰ Order of the First Senate of 27 April 2022 - 1 BvR 2649/21. Преузето 27.06.2023.
https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2022/04/rs20220427_1bvr264921en.html

Према образложењу нацрта акта, обавеза пружања доказа о вакцинацији против COVID-19 или опоравку од COVID-19, наметнута чланом 20а Закона о заштити од зараза, која важи до 31. децембра 2022, служи за заштиту јавног здравља и заштиту посебно угрожених група од заразе COVID-19. Тачно је да се предлог акта односи на општу законодавну сврху „заштите јавног здравља“. Ипак, из даљих разлога је јасно да законодавац само намерава да заштити особе које се сматрају посебно рањивим (штићеници домова за пензионере, особе са инвалидитетом који проводе време у установама, и сл.).

Суд је обавезу пружања доказа о вакцинацији или опоравку оценио уставном и одговарајућом за постизање законодавне сврхе. Наиме, према уставном праву, одредба се сматра прикладном ако постоји могућност да ће постићи законодавну сврху. Уколико одређена мера доведе до мешања у основна права али се истовремено врши ради заштите значајних уставних интереса, и ако су могућности законодавца да донесе довољно поуздане закључке ограничене с обзиром на чињеничне несигурности, преиспитивање Савезног уставног суда је заузврат ограничено на оцену да ли је претпоставка законодавца о подобности мере била одговарајућа односно чињенично тачна и одржива, што је Суд у овом конкретном случају позитивно оценио.

Дакле, одлука законодавца да уведе обавезу достављања доказа о вакцинацији или опоравку која се овде оспорава била је уставно одржива у конкретној ситуацији пандемије и на основу тада доступних информација о ефектима вакцина против COVID-19.

4.4. 1 BvR 518/02

Уставном жалбом у овом предмету оспоравају се судске одлуке о електронском профилисању и претресима (растер потрага) као превентивној полицијској мери.⁶¹

Растер потрага је посебна истражна техника која користи електронску обраду података за вршење полицијског гоњења. Полицијски органи захтевају да друга јавна или приватна тела поделе личне податке лица у њиховом поседу, који се у аутоматизованој процедури (профилисање) укрштају са другим подацима. Ова унакрсна провера података служи за идентификацију особа које испуњавају одређене критеријуме, који се морају унапред дефинисати и сматрати значајним за даље спровођење истраге, а осмишљена је у циљу потраге за исламистичким терористима након терористичких напада 11. септембра 2001. године.

Подносилац притужбе тврди да му је оспореним судским одлукама повређено основно право на информационо самоодређење из члана 2.1. у вези са чланом 1.1. Основног закона. Полицијске мере надгледања или надзора могу утицати на обим заштите овог основног права, посебно када се лични подаци прикупљају и чувају за потребе електронске обраде података и даљег упоређивања са подацима прикупљеним из других извора. Овлашћења за задирање у основна права утврђена чланом 31.1. Закона о полицији Северне Рајне - Вестфалије из 1990. године суд оцењује као уставне из следећих разлога:

1. Основно право на информационо самоодређење није загарантовано без ограничења - појединац мора прихватити да ово право подлеже ограничењима која служе преовлађујућим јавним интересима. Таква ограничења захтевају законску основу која мора бити уставна, која посебно задовољава захтеве пропорционалности и правне јасноће;
2. Спорни члан Закона о полицији из 1990. године, који ограничава претходно поменуто основно право, задовољава принцип пропорционалности. Овај принцип налаже да држава, мешајући се у основна права, следи легитимну сврх одговарајућим и неопходним средствима;
3. Поменута одредба служи легитимној сврси отклањања опасности за постојање или сигурност Федерације или земље, или за живот, тело или слободу особе.

⁶¹ Decision of the First Senate of April 4, 2006, 1 BvR 518/02; Преузето 28.07.2023.
https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2006/04/rs20060404_1bvr051802.html

4. Растер потрага је такође погодно средство за постизање ове сврхе. Закон је погодан за постизање своје сврхе ако је погодан за тражени исход;
5. Задирање у основно право је такође неопходно за постизање законодавне сврхе. Не постоје ништа мање рестриктивна средства која би била подједнако ефикасна у постизању циља којем се тежи;
6. Начело пропорционалности у свом строгом смислу захтева да тежина задирања, у општој процени, не буде несразмерна тежини разлога на које се позива да би се оправдало. Одређена, посебно наметљива, мешања у основна права могу бити дозвољена само када сумња или опасност која изазива мешање достигне одређени праг, који мора бити утврђен законским одредбама. У конкретном случају електронског профилисања, члан 31.1. Закона о полицији из 1990. испуњава овај стандард тиме што меру условљава постојањем конкретне опасности за угрожене правне интересе.

Право на информационо самоодређење није гарантовано без икаквих ограничења. Појединац мора прихватати ограничења својих права ако су она оправдана претежним интересима заједнице. Таква ограничења морају бити прописана законом и морају одговарати начелу сразмерности и захтеву за јасноћом норми.

Задирање у право на информационо самоодређење дозвољено спорним чланом Закона о полицији из 1990. служи за заштиту високих уставних интереса. Постојање и сигурност Федерације и њених становника, као и живот, тело и слобода личности, које одредба има за циљ да заштити од опасности, правни су интереси значајне уставне тежине.

У правној процени врсте мешања у основна права обухваћених законским овлашћењем, значајно је, између осталог, колико је носилаца основних права погођено, колике су последице ова мешања изазвала, посебно да ли су их погођене особе подстакле.

Растер потрага се првенствено фокусира на идентификационе податке, односно име, адресу, датум и место рођења. Ипак, законско овлашћење није ограничено на ове податке. Уместо тога, такође дозвољава да „било која друга врста података, по потреби у појединачном случају буде укључена у меру”⁶². Сходно томе, захтеви за подацима могу

⁶² Art. 31(2) Polizeigesetz des Landes Nordrhein-Westfalen (PolG NRW), 1990 - Закон о полицији Северне Рајне – Вестфалије; преузето: 11.09.2023.
https://recht.nrw.de/lmi/owa/br_text_anzeigen?v_id=3120071121100036031

се проширити тако да укључују додатне информације о вери, националности, грађанском статусу и области студија – што се догодило у предмету који је у питању.

Закон о полицији такође не предвиђа никаква ограничења у погледу обима података који се могу захтевати за потребе електронског профилисања. Не постоји такво ограничење, чак ни индиректно, ни у погледу врсте тражених података нити у вези са циљаним лицима, с обзиром на то да се од било ког јавног органа и било ког „органа ван јавног сектора“ може захтевати да дели податке у складу са формулацијом члана 31.1. Закона о полицији из 1990. године.

Истражне мере у вези са информацијама могу стигматизовати погођене особе у случају да ове мере постану јавно познате. Ово може индиректно повећати ризик ових особа да буду дискриминисане у свакодневном или професионалном животу.

Коначно, такође је значајно да члан 31.1. Закона о полицији из 1990. Предвиђа мешање у основна права која не захтевају никакве основе за сумњу и неселективно утичу на велики број особа. Таква мешања могу такође да изазову застрашујуће ефекте, који могу нарушити остваривање основних права - људи можда више неће деловати без бриге или страха ако неселективни ефекат истражних мера доприноси осећају да су под сталном присмотром.

Ометање основних права које произилази из растер потраге има велику тежину, посебно ако се има у виду да предуслови за такво мешање нису уско дефинисани законом. Као резултат тога, законодавцу је дозвољено да одобри електронско профилисање ради заштите високих правних интереса наведених у спорном члану Закона о полицији из 1990. године само под условом да постоји посебна опасност за ове интересе.

На основу овог стандарда, електронско профилисање није дозвољено као мера предострожности пре него што се појави конкретна опасност, јер би то довело до мешања у основна права која се потенцијално тичу веома осетљивих личних података.

Оспорене одлуке не испуњавају уставне услове. Они се заснивају на експанзивном тумачењу термина „садашња опасност“ у члану 31.1. Закона о полицији из 1990. године које је у супротности са принципима изнетим горе и при томе доводи до преобликовања опуномоћења у претходно овлашћење. Овакво тумачење овој одредби придаје смисао који ни законодавац не би могао да усвоји без повреде основног права на информационо самоодређење из члана 2.1. у вези са чланом 1.1. Основног закона.

4.5. BVerfGE 65, 1

Право на информационо самоодређење из члана 2.1. Основног закона Немачке омогућава појединцу да самостално донесе одлуку о коришћењу и стављању на располагање својих личних података. Ограничења овог права допуштена су само у општем интересу, те као таква морају имати уставни основ у закону.⁶³

Међу личним подацима може се направити разлика између оних који су прикупљени у статистичке сврхе и оних који се прикупљају у неанонимној форми. У случају прикупљања података у статистичке сврхе, везивање података за конкретну сврху не може се захтевати, али се прикупљање и обрада морају ограничити.

Закон о попису становништва из 1983. године, о чијој се уставности одлучује, својим програмом прикупљања података нема за последицу регистровање података и лица које би било у супротности са достојанством човека.

Пресудом Првог сената од 15. децембра 1983. године образложено је да право на информационо самоодређење може бити ограничено. Ограничења се могу наметнути ако имају законски основ који јасно указује на обим и претпоставке ограничења. Законски основ, дакле, мора бити јасан и сразмеран.

Пресудом се одлучује о домету права на самоодређење, а имајући у виду државне мере којима се од појединаца захтева одавање података личне природе. Одлучивање о овом питању може се спровести тек када постану јасне две карактеристике: у коју сврху се подаци захтевају и какве су могућности њихове обраде. При томе, мора се правити разлика између података који нису прикупљени и обрађени у анонимној форми 1) и оних који се прикупљају за потребе статистике 2).

1) Принудно одавање података личне природе подразумева да су подаци од стране законодавца прецизно одређени као погодни и потребни. Неанонимни подаци не смеју се држати у резерви да би они у будућности послужили унапред недефинисаним сврхама. Коришћење оваквих података је унапред ограничено на законом одређену сврху.

2) Прикупљање и обрада података у статистичке сврхе садржи одређене специфичности. Статистички подаци имају битну улогу у одређивању државне политике - тек се спознајом релевантних података (у вези са економским, социјалним и привредним односима) државна политика може ефикасно водити.

⁶³ Фондација Konrad Adenauer e.V, *op.cit.*, стр. 144

Специфична намена и везивање података прикупљених у статистичке сврхе није могућа - тако прикупљени подаци користе се за различите, унапред неодређене задатке. Како би држава била спремна на индустријски развој друштва, попис становништва мора егзистирати као база разноврсних података који се држе у резерви.

Како појединац не би постао објекат информација које се односе на његову личност, јасне и недвосмислене претпоставке за обраду података морају бити унапред одређене и поштоване. У сврху заштите личних права појединаца на које се прикупљене информације односе, статистичко прикупљање и обрада података обавља се под посебним условима.

У случају постојања опасности да због одавања специфичних личних података појединац буде стигматизован законодавац мора доћи до одговора да ли се исти подаци могу прикупити и остварити своју сврху путем анонимног истраживања.

У циљу заштите права на информационо самоодређење неопходно је спровести посебне мере за организацију прикупљања и обраде података, док је с друге стране неопходно донети прописе који уређују поступак брисања оних података који омогућавају индивидуализацију појединца (име, адреса и сл.). Као меру предострожности неопходно је прикупљене податке учинити недоступним трећим лицима као и држати прикупљене податке у тајности све док се њиховом обрадом може успоставити персонална веза са одређеним лицем.

Чињењем података анонимним, држањем података у тајности, као и њиховим персоналним и временским ограничењем не нарушава се право на информационо самоодређење и може се очекивати од грађана поштовање обавезе давања личних података државним органима.

Супротна пракса (стављање на располагање података који нису учињени анонимним) довела би до високог степена неповерења од стране грађана, те нестанка спремности на кооперацију у процесу прикупљања статистичких података. Оваква пракса сматрала би се недопуштеним задирањем у право на информационо самоодређење.

V ЗАКЉУЧАК

Интернет и нове технологије својим настанком и унапређивањем измениле су друштвену свакодневницу у готово свим сферама живота: пословној, трговинској, комуникацијској и слично. Док је при почецима интернета примарни циљ био прилагодити га друштвеним потребама, сада смо у позицији у којој је неопходно друштво и право прилагодити интернету.

Почевши од своје појаве у 20. веку до данашњих дана, информационе технологије интерагују са људским правима на много различитих начина дајући им нове димензије, чинећи их све применљивијим, али и крхкијим и тежим за правну заштиту услед непредвидивости даљег развика онлајн комуникација и немогућности законодавстава да исти испрате у корак.

Људска права примарно су установљена тако да по својој природи буду генерална и статична. Насупрот њима, информационе технологије су у сталном развоју и напретку. Имајући у виду да је неизбежно и пожељно преплитање људских права и информационих технологија, опште прихваћена људска права више нису у могућности да буду статична, нити би као таква служила својој примарној сврси осигурања слободног и сигурног бивствовања појединаца у демократском друштву. Супротно томе, људска права се последњих година непрестано развијају и трансформишу у складу са дешавањима у друштву и науци, те тако у потпуности испуњавају своју напред поменуту сврху.

У овом раду обрађена је тема постојећих и новонасталих људских права у дигиталном добу. Истражујући ову област ближе је објашњена како практична примена и појава ових права у онлајн свету, тако и питање колико правна регулатива успева да иде у корак са напретком информационих технологија и њеним све израженијим утицајем на уставна и људска права. Овим питањима бавили смо се кроз неколико целина: прва су постојећа људска права, друга су људска права настала у корелацији са информационим технологијама, и трећа целина која се бави судским одлукама Савезног уставног суда Немачке у области права на информационо самоодређење.

С обзиром на чињеницу колику популарност и продор у свакодневни живот појединаца онлајн мреже бележе у последњим деценијама, закључујемо да иста права која људи уживају у свакодневном животу такође морају бити заштићена на мрежи где појединци проводе велики део свог времена, у професионалном и приватном животу.

Чињеница је да су информационе технологије довеле до позитивних ефеката и великог напретка и установљавања нових појавних облика постојећих људских права, али и настанка нових права. У ближем одређивању нових појавних облика већ постојећих, као и дефинисању и одређивању опсега нових, дигиталних права, велику улогу играју уставни судови широм света, посебно имајући у виду чињеницу да законодавства држава тешко иду у корак са динамичним променама у онлајн свету.

Међутим, узевши у обзир сва запажања изнета у раду, не можемо занемарити традиционалну забринутост за људска права која су се појавила настанком, а посебно брзим развојем дигиталних технологија, а то је глобална неједнакост и висок степен злоупотребе и кршења људских права. Ова забринутост проузрокована је ограниченим приступом технологијама у одређеним крајевима света с једне стране, као и превисоком степену задирања технологија у свакодневни живот с друге стране. Док неки од нас не могу да се сете какав је свакодневни живот без интернета и дигиталних уређаја, већина људи на свету нема никакво или има врло осиромашено дигитално искуство.

Као највећи изазов у области заштите људских права и слобода у дигиталном добу појављује се управо проналажење баланса између позитивних и негативних утицаја информационих технологија на свакодневно уживање људских права. Свесни да ће и једних и других увек бити у постојећим или новим појавним облицима, остаје да се законодавствима широм света, као и уставним судовима, препусти терет стављања свих аспеката утицаја савремених технологија на људска права у правне оквире, а да се тиме не зауставља неизбежни процес њиховог прожимања и међусобног утицаја.

Литература

Монографије и чланци

1. Андоновић Стефан, *Заштита података у електронској јавној управи у Републици Србији - правни аспекти*, Београд, 2019, Правни факултет Универзитета у Београду
2. Ahmad Zubair, Manupatra Articles, *Right to be forgotten* (2022); преузето 15.09.2023. <https://articles.manupatra.com/article-details/Right-to-be-forgotten>
2. BBC NEWS, *Internet Access is 'a Fundamental Right'*; преузето 12.09.2023 <http://news.bbc.co.uk/2/hi/technology/8548190.stm>
3. Voitsikhovskiy A, Bakumov O, Ustymenko O, Syroid T, *The Right of Access to the Internet as Fundamental Human Right given the Development of Global Information Society, The Law, State and Telecommunications Review*, 2021, No.1, Vol. 13, 1-19;
4. Google Support - Legal Help, *Right to be Forgotten Overview*; преузето 09.09.2023. <https://support.google.com/legal/answer/10769224?hl=en>
5. Google Transparency Report, *Requests to delist content under European privacy law*, Преузето 20.04.2024. <https://transparencyreport.google.com/eu-privacy/overview?hl=en>
6. Galetta Antonella, *The changing nature of the presumption of innocence in today's surveillance societies: rewrite human rights or regulate the use of surveillance technologies?*; in: *European Journal of Law and Technology*, Vol.4, No.2, 2013; преузето 12.09.2023. <https://ejlt.org/index.php/ejlt/article/view/221/377>
7. Digital Class, *Importance of information technology in today's world*; преузето 13.09.2023. <https://www.digitalclassworld.com/blog/importance-of-information-technology/>
8. Дилигенски Андреј, Прља Драган, *Фејсбук и право*, Београд, 2014, Институт за упоредно право;
9. Dr. Antoinette Rouvroy, Prof. Yves Poullet, *The right to informational self-determination and the value of self-development. Reassessing the importance of privacy for democracy*, Springer, Dordrecht, 2009
10. Daniël Eloff, *The Nature of Rights and Access to the Internet*, Department of Law, Akademia, 2023
11. Internet and Society Collaboratory e.V, *Human Rights and Internet Governance*, Berlin, 2012
12. Jóri András, *Protection of fundamental rights and the internet: a comparative appraisal of German and Central European constitutional case law*; in: Oreste Pollicino & Graziella Romeo (eds.), *The Internet and Constitutional Law*, London, 2016, Routledge, 166-176.
13. Khandagale V.S, *Information Communication Technologies and Human Rights in 21st Century*, Human Rights Education and Indian Scenario, Pethwadgaon, 2016; преузето: 08.09.2023 <https://www.researchgate.net/publication/303895075>
14. Krystyna Kowalik- Bańczyk, *Constitutional adjudication on internet issues in Poland*; in: Oreste Pollicino & Graziella Romeo (eds.), *The Internet and Constitutional Law*, London, 2016, Routledge, 176-192;
15. Kshitij Kumar Singh, *Human Rights in Information Age: Emerging Issues and Challenges*, Delhi, 2015
16. Legal Vidhiya, *Effect of Internet on Freedom of Speech & Expression*; преузето 12.09.2023. <https://legalvidhiya.com/effect-of-internet-on-freedom-of-speech-expression/>
17. Lexology, *Intellectual property blog, Right to be forgotten: developments with regard to de-referencing in the light of inaccurate information*; преузето 02.09.2023. <https://www.lexology.com/library/detail.aspx?g=d63e8758-1ffc-4273-a767-5ca772642d3b>

18. Lexology, Vaish Associates Advocates, *Right to be forgotten*, преузето 09.09.2023. <https://www.lexology.com/library/detail.aspx?g=e0dc65db-85eb-4a93-afa0-30597fb2a037>
19. Lexology, Stevens & Bolton LLP, *The right to be forgotten - recent updates for navigating the freedom of information*; преузето 10.09.2023. <https://www.lexology.com/library/detail.aspx?g=f17dd4ab-75da-47b9-8fa4-429e986d5656>
20. Lexology, *TMT Law Practice*, *Right to be forgotten*, преузето 10.09.2023. <https://www.lexology.com/library/detail.aspx?g=abd8fb99-391d-4f35-a44d-68360ea1e670>
21. Lucchi Nicola, Access to Network Services and Protection of Constitutional Rights: Recognizing the Essential Role of Internet Access for the Freedom of Expression, *Cardozo Journal International & Comparative Law*, No. 3, Vol.19, 654-678;
22. Markov Dimitar, *The presumption of innocence and the media coverage of criminal cases*, (2020); преузето 14.09.2023. <https://arisa-project.eu/the-presumption-of-innocence-and-the-media-coverage-of-criminal-cases/>
23. Mahmoud Shiyab Tayil, The impact of social media on the rights of the accused in Jordan: Does public opinion matter?, *Cogent Arts & Humanities*, Vol.8, 2021, Article 1994112, преузето 13.09.2023. <https://www.tandfonline.com/doi/full/10.1080/23311983.2021.1994112>
24. Мидоровић Слобода, Право на брисање података о личности доступних на интернету, *Зборник радова Правног факултета у Нишу*, Vol. 84, 281-306;
25. Настић Маја, *Уставна заштита људских права*, Ниш, 2021, Правни факултет у Нишу
26. Nastić Maја, The Implact of Informational and Communication Technology on the Realization and Protection of Human Rights, *Balkan Social Science Review*, 2021, Vol. 17, 75-97;
- 27 Nissenbaum Helen, Protecting Privacy in an Information Age: the Problem of Privacy in Public; in: *Law and Philosophy*, New York, 1998, Springer, 559-596;
28. Picot Arnold & Wernick Christian, The Role of Government in Broadband Access; in: *Telecommunication Policy*, New York, 2007, Pergamon Press, 660-694;
29. Popov V.V, Grineva A.S, Erokhina A.V, Human rights to a favorable social environment on the Internet, *Vestnik universiteta*, 2022, No. 7, 177–183;
30. Прља Драган, Рељановић Марио, Ивановић Звонимир, *Интернет право*, Београд, 2012, Институт за упоредно право;
31. Reglitz Merten, The socio-economic argument for the human right to internet access, *Politics Philosophy & Economics*, 2023, No.1, 1-29;
32. Stoykova Radina, Digital Evidence: Unaddressed Threats to Fairness and the Presumption of Innocence; in: *Computer Law & Security Review*, Vol.42, 2021, Article 105575; преузето 11.09.2023. https://pure.rug.nl/ws/portalfiles/portal/208549295/1_s2.0_S0267364921000480_main.pdf
33. Сурчулија Јелена, *Слобода изражавања на интернету*, Београд, 2010, Центар за развој интернета;
34. Тодоровић Драган, Прља Драган, Петровић Далибор, *Интернет и друштво*, Ниш и Београд, 2014, Српско социолошко друштво, Универзитет у Нишу-Филозофски факултет, Институт за упоредно право, Београд;
35. The NATO Cooperative Cyber Defence Centre of Excellence, “*Right to be Forgotten*” or “*Right to Know*”?; преузето 10.09.2023. <https://ccdcoe.org/incyber-articles/right-to-be-forgotten-or-right-to-know/>
36. Фондација Konrad Adenauer e.V. - Изабране одлуке Немачког Савезног уставног суда, Санкт Аугустин, Немачка, 2009, Превод: проф. др. Един Шарчевић,

37. Coccoli Jacopo, The Challenges of New Technologies in the Implementation of Human Rights: an Analysis of Some Critical Issues in the Digital Era; in: *Peace Human Rights Governance*, Padova, 2017, Padova University Press, 223-250;
38. Qerim Qerimi, Bridge over Troubled Water: An Emerging Right to Access to the Internet; in: *International Review of Law*, 2017, HeinOnline, 1-22;
39. Wikipedia, *Journalism during the Marcos dictatorship*; преузето: 02.12.2023. https://en.wikipedia.org/wiki/Journalism_during_the_Marcos_dictatorship

Правни прописи

1. Polizeigesetz des Landes Nordrhein-Westfalen (PolG NRW), 1990 - Закон о полицији Северне Рајне – Вестфалије; преузето: 11.09.2023. https://recht.nrw.de/lmi/owa/br_text_anzeigen?v_id=3120071121100036031
2. Strafgesetzbuch für das Deutsche Reich (StGB), 1871 - Кривични законик Савезне Републике Немачке; преузето: 11.09.2023. <https://lexetius.com/leges/StGB/Inhalt.jsessionid=node05grafoxopm1p1triatdmrnyng8389.no.de0?0>
3. Strafprozeßordnung (StPO), 1950 - Закон о кривичном поступку Савезне Републике Немачке; преузето: 12.09.2023. <https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/82015/97990/F1944933040/stpo.pdf>
4. Grundgesetz, *Bundesgesetzblatt Teil III*, Gliederungsnummer 100-1 - Устав Републике Немачке; преузето: 13.09.2023. <https://www.gesetze-im-internet.de/gg/GG.pdf>
5. International Bill of Human Rights, i.e. the Universal Declaration of Human Rights (UDHR, 1948), the International Covenant on Civil and Political Rights (ICCPR, 1966), and the often-overlooked International Covenant on Economic, Social and Cultural Rights (ICESCR, 1966); преузето: 08.09.2023. <https://www.ohchr.org/sites/default/files/Documents/Publications/Compilation1.1.en.pdf>
6. Council Directive 2002/21/EC of the European Parliament and of the Council (on a common regulatory framework for electronic communications networks and services), 2002; преузето: 10.09.2023 <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:108:0033:0050:EN:PDF>
7. European Convention on Human Rights, 1950; преузето: 12.09.2023 https://www.echr.coe.int/documents/d/echr/convention_ENG
8. Устав Републике Србије, *Службени гласник РС*, бр. 98/06

Одлуке Савезног уставног суда Немачке

1. Decision of the Federal Constitutional Court of Germany as of 15 December 1983, 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83
2. Decision of the Second Senate as of September 9, 1951, BVerfGE 1,1, 2 BvQ 1/51
3. Decision of the First Senate as of April 4, 2006, 1 BvR 518/02
4. Judgment of the First Senate as of March 11, 2008, BVerfGE 120, 238, 1 BvR 2074/05
5. Order of the First Senate as of 27 April 2022, 1 BvR 2649/21
6. Order of the Third Chamber of the Second Senate as of 29 September 2013, 2 BvR 939/13

Сажетак

Значај овог рада огледа се у анализи изложености и значаја примене основних људских права и слобода у свету информационих технологија, настанка нових, дигиталних људских права, као и анализи потенцијалних злоупотреба и ограничења једних и других. Циљ мастер рада је да прикаже тренутни статус основних људских права у информационим технологијама, тежње ка њиховим даљим дефинисањем, као и начине њихове заштите од стране организација и иницијатива које раде на заштити и промовисању људских права у дигиталном царству, као и Уставних судова који се иначе баве њиховом заштитом у реалном свету.

Обрада ове теме обезбеђује критички осврт на питање изложености људских права на интернету, са фокусом на подизању свести о различитим начинима на које онлајн присутност и активности појединца утичу на његова права и слободе, као и степена у којем су људска права угрожена у дигиталном добу, истражујући утицај на слободу изражавања, приватност, заштиту података и друго.

За анализу статуса постојећих и новонасталих људских права у сфери информационих технологија као и напорима њиховог правног дефинисања, коришћена је домаћа и страна литература, одредбе Устава Републике Немачке и Србије, законски прописи који спецификују изложеност уставом загарантованих права и слобода у онлајн свету. Као основни метод истраживања коришћен је нормативни метод у анализи законских прописа, као и студија случаја приликом тумачења података добијених увидом у праксу Савезног уставног суда Немачке.

Кроз три одвојене целине утврђује се тренутни статус људских права у дигиталном добу. Најпре су издвојена поједина постојећа људска права како би се утврдио неминовни утицај технолошког напретка на њихово уживање, али и угрожавање у свакодневним активностима и то: слобода говора, право на претпоставку невиности, право на образовање и право на заштиту података о личности. У другом делу фокус је на такозваним дигиталним правима и њиховом настанку и развоју који се дешава паралелно са настанком и развојем информационих технологија и то: право на приступ интернету, право на информационо самоодређење и право на заборав. У финалном делу рада обавља се анализа пресуда Савезног уставног суда Немачке у вези са правом на информационо самоодређење, којима су постављени темељи, опсег примене и ограничења овог права.

Након свеобухватне анализе, рад доводи до закључка да се, упркос бројним предностима које су информационе технологије донеле у свакодневном животу појединаца, ипак не могу занемарити штетни утицаји и злоупотреба технологија у циљу ограничавања и кршења основних људских права и слобода. Као један од озбиљнијих демократских задатака које морамо обавити као појединци јесте рад на откривању кршења људских права на мрежи и проналажењу начина да наша основна права сачувамо од њихове потпуне деградације и занемаривања.

***Кључне речи:** Људска права, Дигитална права, Информационе технологије, Устав, Уставни суд*

Summary

Human Rights in the Digital Age

This thesis's significance lies in analyzing the exposure and importance of applying fundamental human rights and freedoms in the world of information technology, the emergence of new digital human rights, and the analysis of potential abuses and limitations of both. The master's thesis aims to depict the current status of basic human rights in information technologies, aspirations towards their further definition, as well as the methods of their protection by organizations and initiatives working on the protection and promotion of human rights in the digital realm, including Constitutional Courts which otherwise deal with their protection in the real world.

Processing this topic provides a critical review of the exposure of human rights on the Internet, focusing on raising awareness of various ways in which individuals' online presence and activities affect their rights and freedoms, as well as the extent to which human rights are threatened in the digital age, exploring the impact on freedom of expression, privacy, data protection, and more.

The methods used for the analysis of the status of existing and emerging human rights in the sphere of information technology and efforts towards their legal definition are the following: domestic and foreign literature, provisions of the Constitutions of Germany and Serbia, and legal regulations specifying the exposure of constitutionally guaranteed rights and freedoms in the online world. The normative method was used as the primary research method in analyzing legal regulations, as well as a case study in interpreting data obtained through the practice of the Federal Constitutional Court of Germany.

Through three separate sections, the current status of human rights in the digital age is established. Firstly, individual existing human rights are singled out to determine the inevitable impact of technological progress on their enjoyment and endangerment in everyday activities, including freedom of speech, the right to presumption of innocence, the right to education, and the right to data protection. In the second part, the focus is on so-called digital rights and their emergence and development which occur parallel to the emergence and development of information technologies, including the right to internet access, the right to informational self-determination, and the right to be forgotten.

In the final part of the thesis, an analysis of precedents of the Federal Constitutional Court of Germany regarding the right to informational self-determination is conducted, establishing the foundations, scope of application, and limitations of this right. After

comprehensive analysis, the thesis concludes that despite the numerous advantages that information technologies have brought to individuals' everyday lives, harmful impacts and abuses of technologies aimed at restricting and violating basic human rights and freedoms cannot be ignored. As one of the serious democratic tasks that we must undertake as individuals is to work on detecting violations of human rights online and finding ways to preserve our fundamental rights from their complete degradation and neglect.

Key words: *Human Rights, Digital rights, Informational Technologies, Constitution, Constitutional Court*

Биографија аутора

Јулија Пејчић рођена је у Нишу 19. 05. 1994. године. Основну школу „Цар Константин“ завршила је 2009.године, а потом и гимназију „Бора Станковић“ 2013.године, обе са одличним успехом и као добитник Вукове дипломе. Правни факултет је уписала 2013. године и на истом дипломирала 23. марта 2018. године са просечном оценом 8.39.

Након студија, у периоду од 2018. до 2020. године, обављала је приправнички стаж у адвокатској канцеларији адвоката Милене Братић Јанковић, уско специјализованој за заштиту права интелектуалне својине. По завршетку приправничког стажа, добија заспослење у интернационалној компанији на пословима супервизора за правну усаглашеност производа. Мастер студије, смер право и информационе технологије, уписала је 2021. године. Течно говори енглески, а на основном нивоу знања је немачког језика.