УНИВЕРЗИТЕТ У БЕОГРАДУ
ПРАВНИ ФАКУЛТЕТ

СТЕФАН Н. АНДОНОВИЋ

ЗАШТИТА ПОДАТАКА У ЕЛЕКТРОНСКОЈ ЈАВНОЈ УПРАВИ У РЕПУБЛИЦИ СРБИЈИ – ПРАВНИ АСПЕКТИ

Докторска дисертација

Београд, 2019

UNIVERSITY OF BELGRADE
FACULTY OF LAW

STEFAN N. ANDONOVIC

DATA PROTECTION IN E-GOVERNMENT IN THE REPUBLIC OF SERBIA – LEGAL ASPECTS

Doctoral Dissertation

Belgrade, 2019

ПОДАЦИ О МЕНТОРУ И ЧЛАНОВИМА КОМИСИЈЕ

Ментор:

др Добросав Миловановић
редовни професор Правног факултета Универзитета у Београду

Чланови комисије:

др Предраг Димитријевић
редовни професор Правног факултета Универзитета у Нишу

др Вук Цуцић
доцент Правног факултета Универзитета у Београду

Датум одбране:

У Београду, дана _____ 2019. године

ИЗЈАВЕ ЗАХВАЛНОСТИ

Докторска дисертација не представља само научни рад. Она представља дуг пут који истраживач мора да прође од постављених хипотеза до постизања резултата. Тај пут је пун различитих успона, падова и изненађења, па је значајно имати сапутнике који олакшавају такав научни подухват. Због тога, користим ову прилику да искажем велику захвалност драгим сапутницима и пријатељима који су ми олакшали и улепшали ово путовање и дали допринос квалитету овог истраживања.

На првом месту, захвалност дугујем ментору проф. др Добросаву Миловановићу који је комбинацијом знања, интелигенције и лакоће изражавања помогао да ово истраживање буде квалитетно и поткрепљено правим аргументима. Начин нашег заједничког рада, који ме је умногоме професионално развио, био је у потпуној сагласности са начелима ефикасности и продуктивности. Захвалан сам и проф. др Драгану Прљи, који ме је својом визијом подстакао да видим више научне врхове , а саветима помогао да ово истраживање добије облик који ће служити теорији и пракси. Захвалност упућујем и проф. др Владимиру Чоловићу, директору Института за упоредно право и представнику елегантне јуриспруденције, који ми је указао поверење да заиграм у научним водама. За богату литературу у овој неистраженој области захвалан сам комшиници Слађи Стојаковић из Народне библиотеке.

Неизмерну захвалност на овом научном и животном путовању дугујем свом принципалу и оцу Небојши, који ме је стручним саветима и правничким дилемама подстицао да увек левитирам између теорије и праксе, мајци Ољи, која ме је својом духовношћу и подршком подстакла да се развијам и да лакше завршим овај велики рад и сестри Тијани, на тихој подршци и разумевању. Наравно, морам да поменем и свог ујака, Небојшу који је свој луцидни допринос пружио у форми доскочица.

Захвалио бих се пријатељима, младим докторима наука и великим стручњацима, проф. др Андреји Катанчевићу, доц. др Андреју Коренићу и др Милошу Станићу, који су ми давали значајне стилске, техничке и материјалне савете. Такође, захвалан сам на пријатељској подршци Данилу, Душану, Митру, Николи, Стефану, Лидији, Јовани, Урошу, екипи „Гас до даске“, колегама са Института за упоредно право и многим другима.

Посебну захвалност дугујем Сањи Андрејевић, сјајном сапутнику великог духа и топлине, која је учинила овај научни пут много лакшим, а својом бескрајном енергијом помогла да овај докторат буде успешно и ефикасно завршен.

ЗАШТИТА ПОДАТАКА У ЕЛЕКТРОНСКОЈ ЈАВНОЈ УПРАВИ У РЕПУБЛИЦИ СРБИЈИ- ПРАВНИ АСПЕКТИ

Резиме:

Појава интернета и информационо-комуникационих технологија утицала је на скоро све аспекте друштвеног живота, тако да се модерно друштво може назвати информационим друштвом. Јавна управа, као значајна друштвена појава, није могла да остане изван таквих трендова. Штавише, поменуте појаве су из корена утицале на њен начин функционисања и организације. У контакту са модерним технологијама јавна управа добија ново рухо и мења своју правну природу, трансформишући се у електронску јавну управу. У електронској јавној управи, која се заснива на употреби информационо-комуникационих технологија и интернета, основни елемент рада представљају информације и лични подаци грађана. Међутим, нове технологије носе и бројне ризике по безбедност информација и личних података које органи управе користе у свом раду, што може довести до повреде права грађана и јавног интереса. Као значајна потреба грађана у савременом друштву истиче се захтев за адекватном заштитом личних података у односу на органе управе.

Због тога, предмет дисертације представљају правни аспекти заштите личних података у електронској јавној управи у Републици Србији. Аутор је истражио систем заштите личних података и правне механизме помоћу којих се остварује њихова заштита у електронској јавној управи, будући да повреда личних података може узроковати значајне повреде људских права и интереса.

Циљ истраживања је да теоријско-практичним приступом анализира позитивно правну регулативу у вези са заштитом личних података у електронској јавној управи.

Кључне речи:

Јавна управа, електронска јавна управа, подаци о личности, заштита података, начини заштите података о личности, права у вези са личним подацима.

Научна област: Право.

Ужа научна област: Управноправна.

УДК број: 342.738

PERSONAL DATA PROTECTION IN E-GOVERNMENT IN THE REPUBLIC OF SERBIA – LEGAL ASPECTS

Summary:

The emergence of the Internet and information and communication technologies has influenced almost all aspects of social life, so we could describe modern society as the information society. As an important social phenomenon, public administration could not avoid such trends. Influence of the Internet and new technologies on public administration is such that today it has changed its legal form into e-government. Because of the use of information and communication technologies, information and personal data are essential elements of e-government work. But, new technologies also carry risks for the security of information and personal data of citizens which are used by administrative bodies in their work. Those risks could lead to violations of citizens' rights and public interest. Adequate protection of personal data is a significant need of citizens in modern society.

Therefore, the subject of this dissertation is the legal aspect of personal data protection in the e-government in the Republic of Serbia. Research aims to analyze the system of personal data protection in e-government, as well as legal mechanisms which provide protection, because violation of personal data could lead to significant damage of human rights. Author has analyzed theoretical and practical aspects of existing legal regulations regarding the protection of personal data in the e-government.

Key words:

Public administration, e-government, personal data, data protection, mechanisms for personal data protections, human rights related to personal data.

Scientific field: Law.

Scientific subfield: Administrative Law.

UDC number: 342.738.

САДРЖАЈ

I УВОДНА РАЗМАТРАЊА

1. ПРЕДМЕТ И ЦИЉ ИСТРАЖИВАЊА

Интернет и информационо-комуникационе технологије извршиле су велики утицај на традиционалне друштвене концепте и обрасце понашања. Савремени свет не може се замислити без нових технологија, будући да су информациони трендови извршили утицај на готово све области друштвеног живота. У таквом стању ствари, информација и лични подаци постају значајна модерна валута и средство размене у свим друштвеним односима. Због тога, читаво модерно друштво се назива информационим друштвом. Суштина информационог друштва осликава се управо кроз размену и коришћење великог броја информација путем интернета и информационо-комуникационих технологија.

Јавна управа, као изразито друштвена појава, неминовно је дошла у контакт са новим технологијама. Тај контакт је из корена утицао на правну природу јавне управе, њен однос према грађанима и улогу у савременом друштву. Захваљујући информационо-комуникационим технологијама, јавна управа мења своју правну природу и добија назив електронска јавна управа. У новом формату она брже и ефикасније обавља свакодневне послове, остварује квалитетнију комуникацију са другим лицима, а њен рад у односу према грађанима постаје транспарентан. Посматрајући са друге стране, грађани добијају отворену, савремену и дигиталну управу, могућност увида у рад органа управе и лакши приступ услугама које управни органи нуде. У таквим дигиталним односима, управа и грађани користе велике количине информације и података, као основне елементе комуникације. На тај начин непрестано се развија улога и значај података у савременим друштвеним односима.

Међутим, нове појаве са собом носе и ризике по функционисање јавне управе и друштва. Употреба информационо-комуникационих технологија отвара значајна питања у вези са законитим и правилним обављањем управних послова. Порастом значаја информација и података јављају се и изазови по безбедност, приватност и друга права грађана. Због тога, нови концепти и изазови захтевају

адекватну и савремену регулативу која се заснива на теоријски анализираним становиштима које прати практична анализа таквих појава.

У складу са значајем савремених појава и повећањем њихове улоге у савременом друштвеном животу, основни предмет нашег истраживања јесу правни аспекти заштите личних података у електронској јавној управи у Републици Србији.

Ради потпуног разумевања и анализе основног предмета истраживања, неопходно је претходно разумети појам електронске јавне управе, будући да је тај нови облик јавне управе довео до великих предности, али и мана, у виду настајања нових ризика по безбедност личних података који се налазе у поседу органа управе. У том смислу, постоји потреба да се анализирају основни теоријски концепти, правни оквир и основни елементи електронске јавне управе у Републици Србији. Ради свеобухватности истраживања, на одређеним местима, аутор је учинио осврт на упоредно-правне системе и њихову регулативу у вези са питањима електронске управе.

Осим појма електронске јавне управе, посебна пажња је посвећена питању личних података у правном систему Републике Србије. У истраживању анализираћемо правну природу, поделе и врсте личних података. Такође, анализа ће обухватити питања улоге и значаја личних података у јавној управи и савременом друштву. Поменута питања даље ће нас водити ка разматрању института правне заштите личних података у оквирима електронске јавне управе.

Материјално најзначајнији део дисертације односи се на основна питања правне заштите личних података у електронској јавној управи. Анализа структуре система и механизама правне заштите заправо представља и главни циљ истраживања. Ради остварења циља, истраживање ће обухватити теоријске аспекте и појмовна одређења кључних питања правног система заштите података у електронској јавној управи. Истраживање ће утврдити основне принципе и начела на којима се заснивају заштита података и права грађана у вези са личним подацима.

Аутор ће обрадити основне механизме правне заштите личних података у Републици Србији, али и Европској Унији, ради свеобухватног прегледа теме истраживања. Под механизмима правне заштите подразумевамо управну и судску

заштиту, као и посебне облике заштите које пружају независна надзорна тела у вези са личним подацима. Такође, анализираћемо и правне елементе информационе безбедности, који се осликавају кроз организационе, техничке и кадровске мере у јавној управи у вези са безбедношћу личних података.

2. НАУЧНА И ДРУШТВЕНА ОПРАВДАНОСТ ТЕМЕ ИСТРАЖИВАЊА

Избор наведене теме истраживања налази оправдање у неколико повезаних разлога. Прво, у домаћој стручној и научној литератури конкретном питању није посвећено пуно пажње. Због тога, истраживање тежи да допринесе развоју и осавремењивању теорије управног права у вези са питањима заштите података о личности. На тај начин указаћемо на нове појавне концепте у савременој управи, као и кључне везе електронске јавне управе и заштите личних података.

Домаћа научно-правна литература није се скоро уопште бавила питањем заштите података у електронској јавној управи. Посредно, у вези са темом истраживања, питање заштите података обрађено је у неколико домаћих монографија, које се претежно баве правом заштите личних података у Европској Унији. Такав је случај са монографијом „*Право заштите података- ГДПР*“ из 2018. године коју су писали Андреј Дилигенски, Драган Прља и Дражен Церовић. Андреј Дилигенски и Драган Прља сачинили су монографију под насловом „*Фејсбук, заштита података и судска пракса*“ 2018. године. Област заштите података слабо је присутна и у домаћим научним радовима, међу којима се истиче Стеван Лилић са неколико пионирских дела у овој области. Стога, постоји очигледна научна потреба за савременим приступом у вези са заштитом података о личности, посебно у ери електронске јавне управе.

Други разлог који оправдава тему истраживања лежи у чињеници да је у Републици Србији 2018. године усвојен *Закон о заштити података о личности*, који је успоставио нов систем у области заштите личних података. Усвајањем закона отворена су бројна питања, посебно у вези са личним подацима које обрађују органи управе. Исте године, на нивоу Европске уније, почела је да се примењује Уредба о заштити физичких лица у односу на обраду податка о личности и о слободном кретању таквих података (Општа уредба о заштити података ЕУ- ГДПР), један од најзначајнијих прописа европског права, који је

изазвао бројне дилеме и полемике у стручној и научној јавности. Будући да један од стратешких циљева Републике Србије представља прикључивање Европској унији, важно је истражити и указати на сличности и разлике између ова два правна система. Анализа домаће и упоредне регулативе представљаће подстицај за нова истраживања и веће интересовање научних радника у овој изузетно актуелној и друштвено значајној области.

Трећи и можда најважнији разлог за израду ове дисертације јесте потреба за савременим истраживањем које ће научним приступом допринети продубљивању фонда знања и развоју свести о значају заштите личних података у електронској јавној управи. Циљ нам је да укажемо на нормативне пропусте и неусаглашености и да развијемо критичко мишљење у вези са појединим традиционалним институтима управног права. Истраживање поменутих питања може да представља и основ будуће научне дисциплине - права заштите података. Због тога, ово истраживање треба да служи правној теорији и пракси, као и да унапреди знања у вези са правним оквиром и праксом која се односи на заштиту личних података које користе органи управе.

На крају, важно је поменути да ће истраживање имати и практични значај, који се огледа у давању препорука на одговарајућим местима за *de lege federenda* (могућа решења) уређење појединих питања заштите података у електронској јавној управи.

3. ХИПОТЕЗЕ

Истраживање се заснива на неколико међусобно условљених хипотеза. Све хипотезе заједно, заправо, представљају једну целину. Истраживање почиње хипотезом да развој електронске јавне управе омогућава брже и боље испуњавање задатака и дужности органа управе према грађанима. Та хипотеза нас даље води до следеће, да се захваљујући електронској јавној управи остварује ефикасност и делотворност у чувању података о грађанима. Трећа хипотеза заснива се на ставу да постојање квалитетне правне регулативе у вези са електронском јавном управом представља један од темеља квалитетне заштите личних података грађана. Следећа, четврта хипотеза односи се на то да упоредно-правна анализа референтних правних система заштите података (правни систем Европске уније и

појединих држава чланица), омогућава извођење општих законитости о заштити података у електронској јавној управи. Следствено томе постављена је и пета хипотеза, која се заснива на томе да је уређеност и примена правних норми које се односе на питање заштите личних података у електронској јавној управи од изузетног значаја за поштовање људских права. У тражењу одговора на постављене хипотезе, неопходно је размотрити различите механизме правне заштите, начела система заштите и права грађана у вези личним подацима у поседу електронске јавне управе.

4. ОДАБИР НАУЧНОИСТРАЖИВАЧКИХ МЕТОДА

Тема истраживања захтева вишедимензионални методолошки приступ који подразумева коришћење неколико научних метода. Како је предмет истраживања усмерен на анализу правног оквира, што превасходно подразумева тумачење и истраживање позитивно-правних прописа, анализа се највећим делом заснива на научним методама који се користе у правним наукама.

Догматски (правни) метод биће употребљен како би се разумела садржина прописа и открило стварно значење правних норми које уређују институте од значаја за електронску јавну управу и заштиту података. У том контексту, у анализи правних прописа аутор ће користити језички и граматички метод тумачења правних норми. Од великог значаја је и системски метод тумачења, који ће се користити за разумевање, позиционирање и теоријску класификацију појединих правних института у вези са предметом истраживања. У истраживању је присутан и упоредно-правни метод. Овај метод је од значаја за идентификацију сличности и разлике домаћих и страних правних система, што може бити од користи за унапређење постојећих нормативних решења.

Истраживање ће на одговарајућим местима приказати референтне прописе и праксу међународног права, права Европске уније и појединих држава чланица, чиме се могу уочити добра или мање добра решења упоредног права. На тај начин бићемо у прилици да изведемо општа правила у материји заштите података у електронској јавној управи. У мањој мери коришћен је и историјско-правни метод, чији је циљ да укаже на разлоге који су условили настанак одређених

појава, пре свега електронске управе и заштите података, али и одговарајућих елемената у поменутим областима.

Осим правних метода, у истраживању ће бити примењени и методи других друштвених наука, попут социолошког и статистичког, који помажу и извођењу закључака у вези са односом теорије и праксе по питању заштите личних података у електронској јавној управи.

Свака темељна научна анализа мора се заснивати на одређеним логичким методама. Такав је случај и са овим истраживањем,које подразумева коришћење индукције и дедукције, а на појединим местима и аналогије. Ови логички методи користиће се приликом извођена закључака у испитивању нормативних решења, али и одлука из праксе.

II ЕЛЕКТРОНСКА ЈАВНА УПРАВА

1. ПОЈАМ, ПОЛОЖАЈ И УЛОГА ЈАВНЕ УПРАВЕ

1.1. Систем поделе власти као полазна тачка одређења јавне управе

За електронску јавну управу можемо рећи да представља сложен систем који се састоји од већег броја чинилаца. Основни полазни елемент у одређењу појма електронске јавне управе јесте јавна управа. Због тога, као претходно питање у одређењу појма електронске јавне управе, јавља се одређење појма и саставних елемената јавне управе. Такав задатак нас усмерава ка ширем друштвено-правном контексту у оквиру кога јавна управа функционише. У том смислу, јавну управу можемо посматрати и одредити кроз систем поделе власти.[1]

Подела власти представља основни принцип готово свих модерних демократских система и практични механизам који омогућава стабилно функционисање државе. Због своје политичко-правне структуре подела власти је у зависности од историјских прилика, у различитим периодима историје, имала другачију теоријску основу и практичну примену. Данас, подела државне власти на законодавну, извршну и судску грану уобичајила се као најшире прихваћена концепција, теоријски и практично. Историјски и вредносно посматрано, она је настала као последица тежње да ниједна грана власти нема надмоћ над другим гранама.[2]

Као и у другим модерним демократским државама, тако је и у Уставу Републике Србије[3] власт подељена на законодавну, извршну и судску грану.[4]

---

[1] За више о подели власти вид. Татјана Кандић, *Судска власт у уставном и законодавном развоју Републике Србије*, докторска дисертација, Правни факултет Универзитета у Београду, Београд 2012, 8-55.

[2] Зачетником теорије о поделе власти сматра се Шарл Монтескје. У свом чувеном делу „О духу закона“, у 11. књизи, Монтескје, говорећи о енглеском уређењу, изложио је теорију поделе власти, наводећи да би „све било изгубљено ако би исти човек или тело угледника, било племића, било људи из народа, вршило поменуте три власти: власт доношења закона, власт извршења јавних одлука и власт суђења за злочине или споровима приватних лица“. Šarl Monteskje, *O duhu zakona*, tom I, knjiga XI, Filip Višnjić, Beograd 1989, 176. Временом, ова теорија ће загосподарити свим модерним демократским уставима и извршити огроман утицај на правно-политичку теорију. За више о Монтескјеовој теорији, вид. Sanja Đurić, „Monteskjeova teorija podele vlasti“, *Poslovne studije*, god. 1, br. 1-2, Banja Luka 2010, 87-100.

[3] Устав Републике Србије, *Службени гласник* РС, бр. 98/2006. У даљем тексту уместо Република Србија биће коришћена скраћеница - Србија.

Однос три гране власти заснива се на равнотежи и међусобној контроли, при чему је судска власт независна.[5]

1.2. Државна управа као део извршне власти

По својој правној природи, извршна власт обухвата два нераскидиво повезана саставна елемента. Први елемент је политичко-извршне природе. Овај елемент оличен је у функцијама председника (шефа државе) и премијера (шефа владе). Њихове дужности тичу се вођења и усмеравања развоја државе, чиме на посредан начин усмеравају друштво у одређеном политичком смеру, због чега се овај елемент и назива политичко-извршним. То значи да „политичко-извршна функција практично представља универзалну димензију политичке организације сваког друштва, на свим нивоима, од основице па до врха политичког система“.[6]

Други саставни елемент је управно-правне природе. Управно-правни елемент састоји се од системски повезаних органа, организација и појединаца који обављају „управну функцију“ у друштву. Управна функција се састоји од бројних јавних задатака и дужности који су у служби примене општих и појединачних правних норми које се могу примењивати и употребом (законитог) државног монопола принуде.[7] Сагледавајући политичко-извршни и управни елемент извршне власти као целину, можемо рећи да су они уско повезани и да један без другог не би могли да остварују своје основне функције и задатке.

Ипак, на трагу одређења појма јавне управе пажњу треба усмерити на управни елемент извршне власти. Основни, најважнији и најмасовнији део управно-извршног елемента чини државна управа. Државна управа[8] представља

---

[4] За више о теоријским и практичним аспектима поделе власти у Републици Србији, вид. Bogoljub Milosavljević, „Načelo podele vlasti u Ustavu i ustavnoj praksi Republike Srbije“, *Pravni zapisi*, god. III, br. 1, Beograd 2012, 5-19.

[5] Чл. 4, Устава Републике Србије.

[6] Небојша Маљковић, *Политичко-извршна функција у друштвенополитичком систему Југославије*, докторска дисертација, Правни факултет Универзитета у Београду, Београд 1985, 146-147.

[7] За садржину управне функције у материјалном смислу вид. Невенка Бачанин, *Управно право, књига I – Уводна и организациона питања*, Крагујевац 2011, 12.

[8] У теоријском смислу, појам државна управа се може двоструко објаснити, у зависности од перспективе посматрања. Са једне стране, државну управу можемо посматрати кроз призму функције коју обавља према грађанима и у том смислу она представља државну делатност која се састоји од посебних обележја и елемената. Други начин посматрања државне управе је кроз призму организације. У том смислу, државна управа се означава помоћу њених органа који

појавни облик државе, који је представљен кроз њене органе који служе извршавању државних задатака и задовољењу потреба друштва. Државне задатке обављају државни органи у облику министарства,[9] органа управе у саставу министарстава, управних организација, итд.[10] Поменути субјекти врше управне послове којим се остварују права, обавезе и интереси државе и њених грађана. Истоветно схватање положаја и улоге државне управе проналазимо и у законодавству Србије.[11]

1.3. Недржавна (јавна) управа

У модерном свету улога државе се шири тако да она прихвата нове послове који раније нису постојали или су били резервисани искључиво за приватни сектор. Таква је ситуација са пословима у областима енергетике, пољопривреде, туризма, здравствене и социјалне заштите, спорта, културе, образовања и многим другим. Добијање нових и сложених задатака, у циљу заштите јавних интереса, створило је потребу да држава оснује јавна предузећа и установа или да одређене важне стратешки важне привредне делатности, односно друштвене делатности, повери приватним физичким и правним лицима, путем нпр. управних уговора, уз задржавање овлашћења која гарантују реализацију јавних интереса.

Поред тога, органи државне управе због великог обима посла, мањка ресурса, потребе за ближим контактом са грађанима и недостатком стручних знања из појединих области, уступају поједине државне послове лицима и организацијама изван државног управног апарата. Због тога, многа правна и физичка лица данас обављају као поверене, послове који сада изворно припадају државној управи, док их је у периоду либералног капитализма обављао искључиво приватни сектор у складу са законима тржишта. Међутим, ти субјекти,

---

обављају управну делатност државе. Славољуб Поповић, Бранислав Марковић, Милан Петровић, *Управно право- Општи део*, Београд 2002, 43.

[9] За министарства се наводи да она представљају основни овлик органа управе, док је за остале органе то упитно. Више о томе: Драган Милков, *Управно право I – уводна и организациона питања*, Нови Сад 2016, 78.

[10] Предраг Димитријевић, „Организација државне управе у Републици Србији“, *Зборник радова Правног факултета у Нишу*, тематски број „Заштита људских и мањинских права у европском правном простору“, бр. LXII, (ур. П. Димитријевић), Ниш 2012, 83.

[11] Државна управа је део извршне власти Републике Србије који врши управне послове у оквиру права и дужности Републике Србије. Чл. 1. Закона о државној управи, *Службени гласник* РС, бр. 79/2005, 101/2007,95/2010, 99/2014.

иако обављају послове од јавног интереса, формално не представљају део државне организационе структуре. Тако се јављају субјекти који „нису део државног апарата, а ипак – по нарочитом правном основу – обављају послове државне управе“, тј. управну делатност, управни рад“.[12]

Сви субјекти који не припадају државној управи, али обављају поједине управне послове као поверене, припадају недржавној јавној управи. Недржавна јавна управа обавља послове од јавног интереса и значаја за ширу друштвену заједницу, али формално није уткана у структуру државне управе. У недржавну управу можемо сврстати органе и организације територијалне аутономије, јединица локалне самоуправе, јавне установе, јавне агенције и јавна предузећа, организације и појединце са повереним јавним овлашћењима.

1.4. Однос јавне и државне управе

Дакле, у пракси се јављају две групе субјеката који обављају јавне послове. То су субјекти државне управе и субјекти недржавне (јавне) управе. Потреба за заједничким називом који би обухватио све субјекте државне и недржавне управе искристалисала је појам јавне управе.[13] Можемо закључити да јавна управа у организационом смислу обухвата:

1. државну управу, односно органе државне управе, као што су министарства, органи у њиховом саставу и управне организације (секретаријати и заводи и сл.), чија је основна делатност обављање државних управних послова,

2. недржавну управу, под којом подразумевамо укупност субјеката којима управни послови не представљају основну делатност, али који обављају управне послове на основу поверених послова државне управе, односно повереног јавног овлашћења (органи територијалне аутономије, органи локалне самоуправе, јавна предузећа, јавне агенције, итд.).[14]

---

[12] Зоран Томић, *Опште управно право*, Правни факултет Универзитета у Београду, Београд 2012, 177.

[13] У литератури се наводи да је крајем 19. века први пут употребљен појам јавна управа и то у теоријске сврхе. Додатној популаризацији појма јавне управе највише је допринео Вудро Вилсон у свом делу *The Study of Administration*, које је објављено 1887. године. Миодраг Петровић, *О појму јавне управе у савременој теорији*, Зборник радова Правно-економског факултета у Нишу II, Ниш 1963, 61.

[14] Стеван Лилић, *Управно право и Управно процесно право*, Београд 2013, 166.

У материјалном смислу, јавна управа обавља све традиционалне послове државне управе, али и послове које је преузела на себе развојем улоге државе у савременом друштву и растом потреба грађана и привреде.[15] То значи да је једна од најзначајнијих промена у систему функционисања државе трансформација јавне управе.[16]

На основу изложеног можемо извести неколико закључака. Појам јавне управе шири је од појма државне управе, будући да обухвата и недржавне субјекте који обављају поверене (државне) управне послове.[17] У литератури налазимо став да „појмови јавне управе и државне управе се разликују утолико што државна управа обухвата знатно мањи број органа и институција изричито одређених законом, док јавна управа обухвата сем државне управе и оне органе и организације којима основна делатност није управног карактера, али који, под условима одређеним законом, врше послове који имају управни карактер“[18].

Даље, органи јавне управе не обухватају сличне појаве (органе и организације) у приватном сектору. Неопходно је нагласити разлику између јавне управе у односу на приватне пословне управе, односно организационе структуре приватног права, као што је случај са администрацијом привредних друштва и другим организационим облицима приватног сектора.[19] Пословне управе не обављају послове у јавном интересу и нису део јавне управе, већ искључиво делују у циљу задовољења приватних интереса власника и саме организације.

У правном систему Србије појам јавне управе помиње се у стратешким документима, док је позитивно правним прописима уређена једино организација државне управе (Закон о државној управи и Закон о државним службеницима). Дакле, тренутно не постоји законски пропис који уређује структуру и посебна правила за целокупну јавну управу. Ипак, јавна управа се помиње у појединим

[15] О томе више: Duško Lozina, Mirko Klarić, „Javna uprava suvremene države u promijenjenim okolnostima“, *Zbornik radova Pravnog fakulteta u Splitu*, br. 1, Split 2012, 24.
[16] Упор. Dragoljub Kavran, *Javna uprava – reforma, trening, efikasnost*, Savet za državnu upravu vlade Srbije – Udruženje za javnu upravu – Centar za javnu upravu FON-a u saradnji sa Fondom za unapređenje kapaciteta Programa za razvoj Ujedinjenih nacija, Beograd 2005, 22.
[17] Упор. Miodrag Petrović, *O pojmu javne uprave u savremenoj teoriji*, Zbornik radova Pravno-ekonomskog fakulteta u Nišu, br. 2, Niš 1963, 74.
[18] D. Kavran (2005), 23.
[19] Марко Давинић, *Европски омбудсман и лоша управа*, Београд 2013, 93.

прописима и правним документима.[20] Свакако, схваћена на изложен начин, јавна управа постоји и обавља послове у правној пракси, будући да органи јавне управе обављају управне (поверене) послове и уживају идентичан статус са органима државне управе у погледу правне природе, улоге и положаја и унутрашњег уређења.[21] Наравно, треба водити рачуна о томе да и поред истоветног статуса функционалног карактера, постоје разлике у организацији и статусу запослених у државној и недржавној јавној управи.[22]

Ради потпуног разумевања структуре и послова јавне управе неопходно је одредити и њене саставне елементе. Због тога, истраживање ће посветити пажњу субјектима који чине јавну управу.

1.5. Субјекти јавне управе

Број субјеката који чини јавну управу изузетно је широк. Субјекти јавне управе обично се одређују прописима, односно законима и подзаконским актима. Прецизно одредити органе који чине јавну управу представља захтеван задатак будући да је „због оваквог шаренила, данас веома тешко говорити о појединим облицима органа управе…“.[23] Тај посао додатно је отежан чињеницом да у Србији тренутно не постоји закон који уређује и одређује органе јавне управе и њихову улогу на јединствен начин, већ постоји закон који се односи само на органе државне управе. Због тога, ради лакшег разумевања субјеката јавне управе,

[20] Појам јавне управе помиње се у Стратегији реформе јавне управе у Републици Србији, *Службени гласник* РС, бр. 9/14 и 42/14. Такође, појам јавне управе налазимо и у оквиру назива органа који је задужен за стручно усавршавање запослених у „јавној управи“, који носи назив Национална академија за јавну управу. Закон којим је основана ова Академија, одређује да јавна управа обухвата државне органе и самосталне и независне организације и тела чији састав бира Народна скупштина, органе, организације и службе аутономне покрајине и јединице локалне самоуправе, јавне агенције и организације на које се примењују прописи о јавним агенцијама и предузећа, установе, организације и појединце којима су поверена јавна овлашћења. Чл. 2, ст. 1, Закона о националној академији за јавну управу, *Службени гласник* РС, бр. 94/2017.

[21] Ови аспекти се односе на правила поступања ових органа (правила општег или посебног управног поступања), прописе по којима поступају, унутрашње уређење, однос са надређеним органима који контролишу правилности и законитост рада и аката ових органа и могућност контроле независне судске контроле. Због тога је са практичне стране, правна природа недржавних органа истоветна правној природи државних органа.

[22] Примера ради, статус државних службеника, на које се примењује Закон о државним службеницима, није идентичан статусу запослених у органима и организацијама аутономне покрајине и локалне самоуправе, на које се примењује Закон о запосленима у аутономним покрајинама и јединицама локалне самоуправе, *Службени гласник* РС, бр. 21/2016, 113/2017, 95/2018.

[23] Д. Милков (2016), 78.

истраживање ће посебно обрадити органе државне управе, а посебно органе недржавне (јавне) управе.

1.4.1. Органи државне управе

Органи државне управе представљају традиционални елемент извршне власти који настао заједно са појавом државе. Током времена, искристалисали су се одређени облици органа државне управе који се структурално и материјално мењају, али идаље обављају државне управне послове.[24] У правном систему Србије, Закон о државној управи наводи да државну управу у Србији чине министарства, органи управе у саставу министарства и посебне управне организације.[25]

Министарства представљају самосталне државне органе који се образују за послове државне управе у једној или више међусобно повезаних управних области.[26] Она се образују законом, а њихов облик, назив и делатности зависе од политичких циљева и усмерења државне политике, што утиче на честе измене њиховог назива, организационе структуре и делокруг послова. Наведена појава није добра са аспекта стабилног и квалитетног обављања послова државне управе, јер се приликом промена делокруга и надлежности спроводи премештање државних службеника и прерасподела предмета и архиве. То уноси немир у њихов рад и доводи до размишљања о будућој позицији датих службеника унутар органа, уместо до посвећености квалитетном обављању послова. У тренутку израде истраживања у Србији постоји већи број министарстава.[27]

---

[24] Упор. С. Лилић (2013), 166.

[25] Чл. 1, став 2, Закона о државној управи. За више о организацији државне управе у Србији, вид. П. Димитријевић (2012), 73-89.

[26] Чл. 22, Закона о државној управи.

[27] То су: министарство спољних послова, министарство унутрашњих послова, министарство финансија, министарство привреде, министарство пољопривреде, шумарства и водопривреде, министарство заштите животне средине, министарство трговине, туризма и телекомуникација, министарство правде, министарство државне управе и локалне самоуправе, министарство одбране, министарство за европске интеграције, министарство рударства и енергетике, министарство просвете, науке и технолошког развоја, министарство здравља, министарство за рад, запошљавање, борачка и социјална питања, министарство омладине и спорта, министарство културе и информисања и министарство грађевинарства, саобраћаја и инфраструктуре. Чл. 2, Закона о министарствима, *Службени гласник* РС, бр. 44/2014, 14/2015, 54/2015, 96/2015- др. закон и 62/2017

Свако министарство може да има један или више органа управе у свом саставу. Органи управе у саставу министарства обављају послове везане за делокруг министарства, а образују се ради извршења стручних и инспекцијских послова. Они се могу образовати у облику управе, инспектората и дирекција.[28] Примера ради, неки од постојећих органа управе у саставу министарства у Србији су Војнобезбедносна агенција и Војно-обавештајна агенција (у саставу Министарства одбране), Управа за ветерину и Управа за заштиту биља (у саставу Министарства пољопривреде, шумарства и водопривреде), Агенција за заштиту животне средине (у саставу Министарства заштите животне средине), итд.

Посебне организације формирају се за обављање стручних и других повезаних послова када се јавља потреба за већом самосталношћу органа у раду у односу на ону коју има орган управе у саставу.[29] У Србији постоји неколико посебних управних организација и оне су образоване Законом о министарствима, иако се могу установити и посебним законима (као што је случај са Безбедносно-информативном агенцијом).[30]

Закон о министарствима познаје различите облике посебних организација.[31] По својој правној природи, посебне организације трајнијег су карактера и нису подложне честим променама назива и надлежности, као што је то случај са министарствима.

1.4.2. Органи недржавне јавне управе

Друга група органа која чини јавну управу припада недржавној (јавној) управи.[32] У теорији се наводи да недржавну јавну управу у Србији чини функционално децентрализована јавна управа (имаоци јавних овлашћења) и територијално децентрализована јавна управа (покрајинска управа и локална

[28] Вид. чл. 28 и чл. 29, Закона о државној управи.
[29] С. Лилић (2013), 215.
[30] Закон о безбедносно-информативној агенцији, *Службени гласник* РС, бр. 42/2002, 111/2009, 65/2014-одлука УС, 66/2014.
[31] Републички секретаријат за законодавство, Републичка дирекција за робне резерве, Републички завод за статистику, Републички хидрометеоролошки завод, Републички геодетски завод, Републичка дирекција за имовину Републике Србије, Центар за разминирање, Завод за интелектуалну својину, Завод за социјално осигурање, Републички секретаријат за јавне политике. Чл. 23, Закона о министарствима.
[32] За више о настанку недржавне управе вид. Eugen Pusić, *Nauka o upravi – knjiga I – Uvodna pitanja, uprava u društvu, uprava kao ljudska djelatnost*, Narodne novine, Zagreb 1989, 106-134.

самоуправа).[33] Субјекти недржавне јавне управе не налазе се у саставу државне управе што значи да „немају изворна овлашћења за вршење управних активности, већ им се та овлашћења морају посебно законом поверити“.[34] Појам недржавне јавне управе не постоји у позитивном законодавству Србије, али се имплицитно помиње у појединим актима који уређују питања од значаја за управу и њен рад.[35]

Захваљујући јавним овлашћењима која су им делегирана законом, група органа који чине функционално децентрализовану недржавну јавну управу добија епитет „јавни“. Ова група обухвата јавне установе, јавна предузећа и јавне агенције. Поједини аутори овој групи додају и Народну банку Србије, као централну емисиону банку државе Србије која поседује ауторитативна овлашћења, која су неодвојива од њене укупне делатности.[36]

Јавне установе могу се одредити као организације чији основни циљ није стицање профита, већ обављање друштвено корисних делатности од интереса за друштво. Због таквог циља, ове организације се оснивају у секторима културе, науке, образовања, физичке културе и спорта, итд. Као пример јавне установа можемо навести јавне библиотеке.[37]

Јавна предузећа се разликују од приватних предузећа једино по интересу који теже да задовоље. За разлику од приватних, јавна предузећа теже да задовоље јавни (општи) интерес и поред тога што своје делатности обављају ради стицања добити. Основана од стране државе, аутономне покрајине или јединице локалне самоуправе, јавна предузећа теже да редовно и трајно пружају услуге својим корисницима, односно грађанима. У Србији, јавна предузећа уређена су Законом о јавним предузећима.[38] Као пример јавног предузећа које је основала Република Србија, можемо навести Електропривреду Србије, које обавља послове везане за производњу, снабдевање и дистрибуцију електричне енергије. У пракси се често недовољно разуме да овај својински облик није опредељујући да ли ће

[33] З. Томић (2012), 177.
[34] S. Lilić, „Organizacioni pojam uprave“, *Pravni zbornik – časopis za pravnu teoriju i praksu*, br. 2-3/95, Podgorica 1995, 101.
[35] Такав је случај са Стратегијом реформе јавне управе у Републици Србији, Законом о Националној академији за јавну управу, итд.
[36] За више о одређењу Народне банке Србије као дела функционално децентрализоване недржавне јавне управе вид. З. Томић (2012), 177-178.
[37] Закон о библиотичко-информационој делатности, *Службени гласник* РС, бр. 52/2011.
[38] Закон о јавним предузећима, *Службени гласник* РС, бр. 15/2016.

неко предузеће имати статус јавног или приватног. Наиме, кључна разлика је у том што та предузећа обављају делатности од стратешког значаја за друштво.[39]

Јавне агенције представљају организације које се оснивају за развојне, стручне и регулаторне делатности ради задовољења јавног (општег) интереса.[40] Оне се оснивају када развојни, стручни и регулаторни послови не захтевају трајни и директни надзор политичке природе и уколико јавна агенција може ефикасније и делотворније обављати поменуте послове у односу на органе државне управе, при чему се обављање њихових задатака може финансирати од стране корисника њихових услуга.[41]

У одређеном броју случајева и појединцима (или појединцима удруженим у посебне облике организовања) се поверавају јавна овлашћења. Такав је случај са јавним бележницима (нотарима), који представљају „службу од јавног поверења".[42] Јавни бележници су овлашћени, између осталог, да састављају, оверавају и издају јавне исправе о правним пословима, где штите приватни интерес грађана, али и јавни интерес и правну сигурност.

У оквиру недржавне јавне управе, можемо издвојити посебну групу органа која припада територијално децентрализованој недржавној јавној управи. За ову групу органа можемо рећи да представљају својеврсно остварење основних права грађана. То су право грађана на покрајинску аутономију и право грађана на локалну самоуправу. Органи територијалне аутономије и јединица локалне самоуправе обављају послове који су од ширег друштвеног значаја, а тичу се грађана који живе на одређеној територији ужој од државне (аутономне покрајине, града или општине). Такође, постоји могућност да Република Србија аутономној покрајини законски повери поједина питања из своје надлежности.[43]

У односу на територијалну аутономију, органи који обављају управне послове јесу влада аутономне покрајине, покрајински секретаријати и покрајинске

[39] Као пример можемо узети Нафтну индустрију Србије, где државно власништво није 100%, већ 51% према 49%, али своје делатности обавља као стратешке.
[40] Закон о јавним агенцијама, *Службени гласник* РС, бр. 18/2005 и 81/2005- испр. За више о положају и улози јавних агенција вид. Зорица Урошевић, „Положај и улога јавних агенција у нашем правном систему", *Правни живот*, Београд 2005, 283-296.
[41] Чл. 2, Закона о јавним агенцијама.
[42] Закон о јавном бележништву, *Службени гласник* РС, бр. 31/2011, 85/2012, 19/2013, 55/2014- др. закон, 93/2014- др. закон, 121/2014, 6/2015, 106/2015.
[43] З. Томић (2012), 184.

организације. Они обављају различите послове (решавање у управним стварима) од општег интереса за локално становништво у областима попут: просторног планирања, регионалног развоја, пољопривреде, водопривреде, туризма, угоститељства, ловства и риболова, заштите животне средине, итд.[44]

Јединице локалне самоуправе преко којих се остварује локална самоуправа у Србији су општине, градови и Град Београд. Осим изворних послова, ови органи могу обављати и поверене државне послове. Као поверене послове поменути органи преузимају послове инспекцијског надзора у просвети, здравству, пољопривреди и др. Управне послове у овим јединицама обављају општинска већа и општинске управе.[45]

Из изложеног видимо да су органи јавне управе веома бројни и разноврсни. Такво стање последица је непрестаног повећања броја државних послова и одговора на нове изазове и циљеве које држава покушава да оствари. Наравно, сви органи јавне управе постоје превасходно због грађана чије интересе теже да задовоље. У тежњи за остварење тог циља, органи јавне управе имају одређен делокруг послова који обављају у вршењу своје управне делатности, на основу чега их и квалификујемо у органе јавне управе.

Због тога, незаобилазни елемент у одређењу појма јавне управе односи се на послове које обављају ови органи, што говори о функционалном појму јавне управе, па ће наредни део истраживања анализирати (управне) послове које обављају органи јавне управе.

1.6. Послови јавне управе

Бројност органа јавне управе утиче на разноврсност (управних) послова које ти органи обављају. Послови органа јавне управе одређују се законима, док се конкретизују и обликују кроз подзаконске опште правне акте. На овом месту, важно је направити разлику терминолошке природе. Наиме, у теорији се прави разлика између задатака и послова јавне управе. Тако, задаци јавне управе

[44] Закон о утврђивању надлежности аутономне покрајине Војводине, *Службени гласник* РС, бр. 99/2009 и 67/2012- одлука УС.
[45] Закон о локалној самоуправи, *Службени гласник* РС, бр. 129/2007 и 83/2014- др. закон.

представљају конкретизоване циљеве у оквиру делатности органа управе, док се под пословима подразумевају мање радне целине које се гранају из задатака.[46]

У Србији не постоји пропис који на јединствен начин уређује послове јавне управе. Са друге стране, Законом о државној управи прецизно су уређени послови државне управе које су од суштинске важности за функционисање државе и нормално одвијање друштвених токова. Аналогијом, ове послове обављају, у својству поверених, и органи недржавне јавне управе.

Као послови државне управе одређени су: учествовање у обликовању политике Владе, праћење стања из свог делокруга, извршавање закона, прописа и других аката, инспекцијски надзор, старање о јавним службама, развојни послови и остали стручни послови. Поједини послови државне управе могу се поверити и органима недржавне јавне управе, односно органима аутономних покрајина, јединицама локалне самоуправе, јавним предузећима, јавним агенцијама, јавним установама и другим организацијама.[47] За ове послове државне управе, аутори закључују да су нормативно одређени према модерним стандардима и савременим тенденцијама у пословању јавне управе.[48] Укратко ћемо се осврнути на основне карактеристике поменутих послова.

Учествовање у обликовању политике Владе значи то да органи државне управе учествују у креирању политике државе. Наравно, органи државне управе то чине посредно, преко политичко-извршног дела извршне власти, односно Владе. Припремањем нацрта закона и других општих правних аката, предлагањем стратегија развоја и мера којима се утиче на политику Владе, органи управе практично утичу на стратешко-политички развој државе. Наглашавам да се ова врста послова, која се односи на обликовање политике Владе, не може поверити.[49]

Праћење стања у својим областима представља важан задатак органа управе, будући да се они старају о редовном одвијању друштвених токова. Како су органи управе у обављању својих послова усмерени према грађанима, они су дужни да ослушкују и проучавају потребе друштва. Овај посао обавља се на тај

[46] Ратко Марковић, *Управно право*, Слово, Београд 2002, 228.
[47] Чл. 4. Закона о државној управи.
[48] S. Lilić, *Evropsko upravno pravo – sa osvrtom na upravno pravo Srbije u kontekstu evropskih integracija*, Pravni fakultet Univerziteta u Beogradu, Beograd 2011, 126.
[49] Чл. 54, ст. 1, Закона о државној управи

начин што се Влади предлажу мере (у форми предлога измена закона и предлога за предузимањем конкретних мера) или предузимају различите правне и материјалне мере како би се грађанима омогућило остваривање права и интереса.

Овај посао је у пракси недовољно присутан упркос огромном значају који има за правилно обликовање политике Владе. Наиме, правилним праћењем стања могу се уочити проблеми, али и њихови узроци, чиме се избегава да се, примера ради, предложи усвајање новог закона, иако су узроци проблема на сасвим другој страни (недовољни капацитети у државној управи или недовољно разумевање на страни субјеката на које се пропис примењује). Кључну улогу у овом послу имају инспектори који су при вршењу инспекцијског надзора свакодневно у прилици да омогуће квалитетно праћење стања.

Извршавање закона, других прописа и општих аката представља најзначајнију групу послова органа управе, који представља специфичну одлику управних органа, али и целокупног управног права. Органи управе старају се да сви општи и појединачни (управни) правни акти „оживе“ у пракси. Када се ови послови не би обављали, закон и други правни акти остали би само слово на папиру, те не би постојала могућност за непосредним спровођењем државне политике и општих правних норми у свакодневни живот. Доношењем прописа (подзаконских општих правних аката) којима се ближе уређују ситуације предвиђене законом, решавањем у управним стварима (доношењем управних аката, решавањем о правни средствима грађана изјављеним против тих аката и предузимањем управних радњи), вођењем разних евиденција и издавањем исправа, органи управе обављају послове извршења закона и других прописа.

Инспекцијски надзор[50] представља врсту корективних послова органа управе. Контролом и испитивањем начина спровођења закона, управни органи осигуравају правилну примену закона и других општих аката. У оквиру обављања инспекцијског надзора органи управе предузимају различите правне и материјалне мере, како би надзор служио својој контролној сврси. Новим Законом

[50] За више о појму инспекцијског надзора вид. Милан Влатковић, Зоран Јовановић, *Управни надзор*, Правни факултет у Крагујевцу, Крагујевац 2016, 113-115.

о инспекцијском надзору, знатно темељније је уређен овај органа управе и стављен је већи нагласак на превенцију у односу на ранији модел.[51]

Старањем о јавним службама, развојним и осталим стручним пословима подстиче се развој стања у делокругу појединог органа, омогућава се квалитетнији рад целокупне управе и побољшава однос грађана са управом. Укратко, овом групом послова се на посредан начин омогућује ефикасно функционисање државе и остварују свакодневне потребе друштва.

Закон о општем управном поступку уводи управне уговоре,[52] као нову врсту именованих уговора који се закључују у јавном интересу и гарантне акте.[53] То проширење појма управне ствари требало би да се одрази и на проширење круга управних послова предвиђених Законом о државној управи, у смислу закључења управних уговора и издавања гарантних аката.

Бројност изложених послова условљава и потребу за њиховом класификацијом. Најчешћа и можда најзначајнија подела јесте подела на управне и неуправне послове јавне управе.[54] Ова подела је значајна због тога што се у појединим делатностима органи јавне управе приближавају законодавној грани власти, као што је случај са доношењем прописа (подзаконских општих правних аката). На тај начин они формално обављају исти посао као и органи законодавне власти, али материјално остају у сфери извршавања прописа, чиме се остварује управна природа ових органа. Такође, одређени послови не могу се одредити као чисто управни, будући да имају универзални карактер и да их предузимају органи свих грана власти (као што је случај са праћењем стања у својим областима и

[51] За више о инспекцијском надзору вид. Милан Стефановић, Душан Радовановић, Даница Јоловић, *Водич за примену Закона о инспекцијском надзору*, Представништво Cardno Emerging Markets USA Ltd, Београд 2017.

[52] На потребу за званичним увођењем управних уговора у српско законодавство указивали су аутори и пре доношења Закона о општем управном поступку. Вид. Добросав Миловановић, „Визионарска мисао професора Славољуба Поповића о управним уговорима, *Зборник радова правног факултета у Нишу – Тематски број посвећен Славољубу Поповићу*, Правни факултет Универзитета у Нишу, Ниш 2011, 134. За више о управним уговорима у позитивно-правном законодавству вид. Зоран Томић, Добросав Миловановић, Вук Цуцић, *Практикум за примену Закона о општем управном поступку*, Службени гласник, Београд, 2017, 48-52.

[53] Детаљно о гарантном акту вид. Добросав Миловановић, Вук Цуцић, „Унапређење пословног окружења у Србији у светлу нових решења Нацрта закона о општем управном поступку“, Усклађивање пословног права Србије са правом ЕУ (ур. В. Радовић), Правни факултет Универзитета у Београду, Београд 2015, 454-463.

[54] Драган Васиљевић, *Управно право*, Криминалистичко-полицијска академија, Београд 2015, 161.

обављањем анализа, сачињавањем извештаја и другим стручним и развојним пословима).

Према природи и начину извршавања послова који се обављају, могућа је подела послова јавне управе на ауторитативне и неауторитативне. Ауторитативни послови се предузимају из позиције „јачег“, са ауторитетом јавне власти и подразумевају, по потреби, употребу државног монопола силе, као облика легитимне и законите принуде у случају непоступања по прописима. Са друге стране, неауторитативни послови државне управе предузимају се из „једнаке позиције“ са грађанима, односно из позиције друге једнаке стране која у том односу (послу) учествује. Орган јавне управе у том случају не поступа са позиције ауторитета, већ представља једнаку страну у односу (такав је случај са управним уговорима).[55] У крајњој линији, можемо рећи да класификација послова јавне управе представља чисто теоријску конструкцију, без већих импликација у предузимању управних послова.

На основу изложеног можемо закључити да су послови јавне управе бројни, разноврсни и да захтевају специфичне методе рада које су неопходне како би се друштвени токови нормално одвијали у складу са потребама грађана. Такође, начини извршавања послова јавне управе су у директној корелацији са изазовима модерних друштвених потреба. Због тога, методологија извршавања послова трпела је бројне промене током развоја система јавне управе. Уз то, систем и методологија рада условљени су улогом органа јавне управе у друштву.

[55] У Француској постоји нешто јача позиција органа који штити јавни интерес, што се одражава и на другачији правни режим коме су подвргнути управни уговори у односу на уговоре грађанског права. У Немачкој се више инсистира на равноправности уговорних страна. За више о разлици управних уговора у немачком и француском праву вид. З. Томић (2012), 197-199. Према Закону о општем управном поступку Србије, орган може да раскине уговор под одређеним околностима, а противна страна то није у могућности да учини, већ само може да изјави приговор, што представља средишње решење, у односу на поменута решења иностраног права.

1.7. Улога јавне управе у друштву

Органи јавне управе обављају многобројне делатности у различитим областима друштвеног живота. На основу тога поставља се питање који је крајњи циљ обављања свих тих делатности и због чега органи јавне управе предузимају те послове ? Прецизније формулисано, поставља се питање, која је улога јавне управе у савременом друштву ?

Одговор на постављено питање суштински је везан за улогу државе у животу појединца. Држава представља облик и начин организовања појединаца и група који су повезани заједничким личним, социјалним, историјским, културним и другим карактеристикама. Грађани теже да уреде међусобне приватне, пословне и јавне односе постављањем одговарајућих правила понашања у својој заједници, стварајући властиту и друштвену будућност, у одређеној мери, предвидљивом и погодном за живот. У таквој тежњи настаје држава као посебан организациони систем који се идентификује са заједницом свих лица, органа и организација који живе на њеној територији и чији су они припадници. Зато се може рећи да држава представља систем функционисања материјалних и људских фактора у оквиру кога су прописана правила понашања у облику правних норми, при чему је примена правила понашања гарантована монополом државне принуде.

Сва лица која су држављани једне државе дају јој легитимитет за извршавање мера и задатака неопходних за опстанак организоване друштвене заједнице. То значи да је држава усмерена на остваривање јавних и појединачних интереса. Држава омогућава остваривање свих интереса преко својих органа (законодавних, извршних и судских) и преко изабраних представника који би требали да представљају интересе грађана. У обављању својих делатности, држава је потчињена праву као систему правила који уређује функционисање једне заједнице.

У таквом систему јавна управа има задатак да примењује прописе који уређују односе између појединаца, организација и државе. Органи јавне управе свакодневно обављају послове од значаја за друштвену заједницу и приватне интересе у оквиру те заједнице чиме омогућава нормално одвијање свакодневних друштвених токова. Активно делујући у областима здравља, културе, рада, спорта, унутрашње и спољне безбедности и многим другим областима, органи

јавне управе омогућавају услове за остваривање права и интереса грађана, дајући им осећај сигурности од опасности по њихова права и интересе. Зато се наводи да „нови системи јавне управе у модерним земљама настају и почивају на промењеним потребама и мотивацији грађана као корисника услуга јавне управе, а не само контролисаних субјеката“.[56]

Области деловања органа јавне управе свакодневно се шире и обухватају нове друштвене области које се раније нису могле ни замислити. Задаци јавне управе постају сложенији, обимнији и захтевају више информација како би били успешно обављени. Данас, у ери информационо-комуникационих технологија, јавна управа има све већу потребу за информацијама и подацима о физичким и правним лицима, њиховим делатностима, активностима, проблемима и изазовима са којима се сусрећу. Информације представљају основну валуту и полазни елемент који подстиче органе јавне управе на покретање одговарајућих управних механизама и предузимање мера како би се живот заједнице наставио нормалним и предвидљивим током. У таквим односима, информације и подаци представљају суштинску вредност која помаже органима управе у планирању, анализи и примени правила понашања и остваривању њене регулаторне улоге у друштву.

Измена структуре друштва и образаца на којима грађани функционишу, утиче и на облик и деловања органа јавне управе. У остваривању нових државних и друштвених задатака у свету информационих технологија и интернета, посебну улогу има процес дигитализације рада органа јавне управе. Ова последња велика иновација у развоју отворила је потпуно ново поглавље у начину функционисања и природи јавне управе. На тај начин долази и до измене њене улоге у друштву. Ново доба у постојању и развоју јавне управе може се одредити као доба електронске јавне управе.

[56] D. Kavran (2005), 22.

2. ОПШТА ПИТАЊА ЕЛЕКТРОНСКЕ ЈАВНЕ УПРАВЕ

2.1. Употреба нових технологија у раду јавне управе

Нови задаци и послови које органи јавне управе преузимају последица су развоја друштва, нових технологија, иновација и повећања људских потреба. Они захтевају посебна дигитална знања и вештине у раду, посебно у вези са информационо-комуникационим технологијама и интернетом.[57] Значај техничких иновација и технолошких знања за функционисање управе препознали су теоретичари пре више од једног века, што говори о непролазној потреби усавршавања начина обављања послова у различитим формама организовања.

Још у 19. веку, један од најважнијих мислилаца свога доба, Макс Вебер (*Max Weber*) се у својим радовима бавио бирократијом као формом државног управљања. Овај аутор наводи да „основни извор супериорности бирократског облика управљања (државом) лежи у техничком знању које, због развоја модерне технологије и пословних производних метода, постаје потпуно неопходно“.[58] Ове речи данас имају већи значај него икада пре, будући да су уткане у реалност модерних јавних управа.

Како би успешно обављала нове послове јавна управа мора да одржава корак са друштвом и да прати његов развој. То се посебно односи на дигиталну писменост и употребу информационо-комуникационих технологија у свакодневним пословима и делатностима. У прихватању измењене друштвене улоге и нових послова, јавна управа је морала да изврши својеврсну трансформацију. Употреба информационо-комуникационих система и интернета, увела је јавну управу у ново раздобље свог постојања које се одразило на њену правну природу, начин обављања послова, друштвену улогу и отворила бројна правна питања у вези са традиционалним и новим правним институтима.

[57] За више о улози и развоју интернета у савременом друштву вид. Далибор Петровић, „Друштвена конструкција интерперсоналних медија – од телеграфа до интернета“, у *Интернет и друштво*, (ур. Д. Тодоровић, Д. Петровић, Д. Прља), Српско социолошко друштво, Универзитет у Нишу – Филозофски факултет, Институт за упоредно право, Ниш – Београд 2014, 16-19.

[58] Max Weber, *Economy and Society: An Outline of Interpretative Sociology*, University of California Press, Berkeley - Los Angeles - London 1978, 223.

2.2. Информационо-комуникационе технологије у јавној управи

Тренд дигитализације из темеља је утицао на многе друштвене делатности, чиме је оставио траг на државу и њене органе. Дигитализацијом рада и средстава којима се служи у обављању својих делатности управа је добила нови облик и правну природу који се осликава појмом електронске јавне управе.[59]

У циљу одређења појма електронске јавне управе, поред појма јавне управе, неопходно је одредити и појам информационо-комуникационих технологија, будући да тај појам објашњава основна средства и методе у раду јавне управе. Без разумевања овог појма не може се разумети ни појам електронске јавне управе.

Информационо-комуникационе технологије користе се као средство остваривања аудио-визуелних начина комуникације и средство размене података. Употреба комуникационо-информационих технологија данас укључује велике сервере, умрежене рачунаре, базе података, повезане дигиталне мреже органа управе и друге електронске мреже путем којих субјекти комуницирају једни са другима.[60]

Појам информационо-комуникационих технологија може се рашчланити на два основна елемента: информационе технологије и комуникационе технологије. „Информациона технологија је технологија која користи рачунаре за прикупљање, обраду, чување, заштиту и пренос информација. Информационим технологијама придружене су комуникационе технологије, јер је данас незамислив рад са рачунаром ако он није повезан у мрежу, тако да се говори о информационо-комуникационој технологији.“[61] То значи да информационо-комуникационе технологије, у материјалном смислу, подразумевају коришћење нових технолошких средстава у циљу размене и коришћења дигитализованих информација. У техничком смислу, ови системи представљају збирни назив за

[59] Mirjana Drakulić, Ratimir Drakulić, „Elektronska upotreba i zloupotrebe“, *Pravni život,* br. 9/2003, Beograd 2003, 988.
[60] Упор. Paul Henman, *Governing Electronically, E-Government and the Reconfiguration of Public Administration, Policy and Power,* Palgrave Macmillan, UK 2010, 28.
[61] Дарио Илија Рендулић, *ITdesk.info – пројекат рачунарске е-едукације са слободним приступом – Приручник за дигиталну писменост*, Отворено друштво за размену идеја, Загреб 2013, 1.

различите појавне облике хардвера и софтвера који су међусобно повезани путем каблова или дигиталних сигнала.

Иако је циљ истраживања искључиво усмерен на правне аспекте теме истраживања, неопходно је у кратким цртама и разумној мери осврнути се на основне техничке елементе информационо-комуникационих технологија, како би се боље разумели правни аспекти заштите података и сам процес обраде података.

Основне компоненте од којих се састоје информационо-комуникационе технологије јесу хардвер („тврди део“) и софтвер („меки део“). Хардвер и софтвер представљају техничке компоненте које своју употребну вредност остварују увођењем у одређени друштвени систем или подсистем (правни, медицински, економски, спортски, итд.) у коме остварују своју сврху као средство и метода рада. Ове компоненте представљају основне јединице информационо-комуникационих технологија, па самим тим имају велики значај као средство рада органа управе.

Хардвер (*hardware*) се може разумети као систем физички опипљивих (материјалних) елемената који у свом јединству чине „тврди“ део рачунарског система. Како се наводи: „хардвер је платформа за процесуирање информација која се састоји од:

1. улазних уређаја: тастатуре, уређаја за показивање (миш), читача бар кодова, микрофона, уређаја који примају улазне информације из окружења и представљају интерфејс између корисника и CPU рачунара,

2. Процесора (*CPU*): „мозак“ рачунара који процесуира информације извршавајући аритметичке прорачуне и логичке операције и доноси основне одлуке на бази поређења вредности информација, а обухвата микропроцесор, матичну плочу, примарну меморију (*PAM*), јединицу за напајање и додатне наменске (експанзионе) картице,

3. Излазне уређаје: мониторе који у окружење шаљу визуелне излазне информације, штампаче – штампане информације и звучнике – аудио и тонске информације,

4. Меморије и уређаје за складиштење информација: меморија рачунара се често назива примарна меморија, главна меморија или само меморија, најчешће *RAM* (*Random Access Memory*) типа, а користе се за складиштење програма и

података којима *CPU* непосредно треба да приступи, уређаји за складиштење укључујући чврсти диск који се често назива интерна, секундарна меморија и други спољни уређаји за складиштење, ЗИП дискови, магнетне траке и флеш меморије, који су истовремено улазни и излазни уређаји, у зависности да ли се информације учитавају или се очитавају".[62]

Софтвер (*software*), са друге стране, представља одређени рачунарски програм (системски повезане информације рачунарског језика) који омогућава функционисање рачунарског система. Према томе, софтвер, односно рачунарски програм, представља повезане машинске и логичке кодове (инструкције) који упућују рачунарски програм на обављање одређених задатака. За разлику од хардвера, софтвер не представља опипљиви део рачунарског система, већ он представља „збир информатичких програма, процеса, правила, документације и датотека, који чине део операција једног информатичког система".[63]

Софтвер, метафорички говорећи, представља душу рачунарског система и омогућава „оживљавање хардвера". Један рачунарски систем не може постојати без поменута два елемента. Уколико софтвер није повезан са хардвером, или хардвер не садржи софтвер, информационо-комуникациони систем неће функционисати.

2.3. Значај информационо-комуникационих технологија у јавној управи

За јавну управу, као вишестепену организациону структуру, неопходна је одлична повезаност између свих саставних елемената. То се пре свега односи на људске и материјалне ресурсе. Људи и материјални ресурси морају бити системски повезани како би се циљеви и задаци управе успешно извршили.

Значај умрежавања људи и средстава у органима јавне управе препознат је у теорији и у пракси. У литератури се наводи да „..увођење рачунарских информационих и комуникационих технологија, посебно интернета, омогућава организацијама да развију флексибилност и прилагодљивост, чиме потврђују своју еволуциону природу. Истовремено, ове технологије омогућавају

[62] Милан Милосављевић, Младен Веиновић, Гојко Грубор, *Информатика*, Универзитет Сингидунум, Београд 2009, 44.
[63] IEEE Software Engineering Standard 729-1993: Glossary of Software Engineering Terminology, IEEE Computer Society Press, 1993, нав. према: М. Милосављевић, М. Веиновић, Г. Грубор (2009), 113.

координацију задатака и управљање сложеним процесима. Без преседана, ово резултира комбинацијом флексибилности и обављањем задатака, координираним доношењем одлука и децентрализацију извршења тих одлука, индивидуализовање ситуације и глобалне, хоризонталне комуникације, чиме се пружа супериорна организациона форма људских делатности".[64] Изложени став наглашава важност информационо-комуникационих технологија за напредак јавне управе, али и за остваривање боље сарадње између државе и грађана.

Модерне технологије омогућавају да се велике количине информација и података брзо обраде и лако користе приликом одлучивања у управним стварима. Користећи се рачунарским програмима (чак и оним који се користе у свакодневној употребе за личне потребе попут *Word-a, Excel-a, PowerPoint-a*), органи управе убрзавају свој рад и успешно га унапређују. Поменути процеси још више су изражени када се користе посебни рачунарски програми који су специјализовани и прилагођени појединим областима и пословима органе управе.

Информационо-комуникационе технологије доприносе и остваривању основних вредности којима управа тежи, као што су ефикасност, транспарентност[65] и остварење права и интереса грађана, будући да они добијају могућност да изврше увид у то шта и колико брзо раде органи управе. Захваљујући свеопштој повезаности информационо-комуникационих система, грађани су у могућности да лако приступе различитим подацима о раду јавне управе и тиме лакше остваре своја права и интересе.[66] Органи управе добијају могућност да квантификују резултате свога рада и да своја остварења поделе са заинтересованом јавношћу. На тај начин остварује се принцип одговорности управе. Непостојање жеље да се обелодане различити акти или предузете мере може бити индикатор да одређени орган не жели да буде подвргнут суду јавности, односно да избегава одговорност, што представља кочницу развоја. Уколико би управа остала изван таквих токова, не би могла у могућности да испуни своју друштвену улогу. Зато је неопходно да се органи управе константно усавршавају

[64] Manuel Castells, *THE Internet Galaxy - Reflections on the Internet, Business, and Society*, Oxford University Press, Oxford 2001, 2.
[65] Исто, Branislav Simonović, Zoran Jovanović, „Elektronska uprava i prevencija korupcije", *Pravni život*, br. 10/2017, Beograd 2017, 433.
[66] Stephen Godsmith, Susan Crawford, *The Responsive city*, Jossey-Bass: A Wiley Brand, San Francisco 2014, 157.

и прате кретања и развој друштва. На том путу најважнији елемент јесте употреба информационо-комуникационих технологија у раду.

Дакле, у модерном свету и савременим условим живота, информационо-комуникационе технологије представљају важан део у функционисању јавне управе без којег се управни рад више не може замислити. Иако електронска јавна управа представља појаву новијег датума, могу се идентификовати зачеци употребе информационо-комуникационих технологија у јавној управи, који су широм отворили врата новинама информационе револуције.

2.4. Историјски развој електронске јавне управе

Тешко је прецизно говорити о историјској перспективи електронске јавне управе, будући да она представља појам који је практично, али и теоријски, у почетним фазама развоја. У литератури налазимо податак да појам „електронска управа“ први пут „званично“ улази у јавни дискурс 1993. године у часопису *Government Computer News*, док се шира јавност боље и детаљније упознаје са овим појмом 1999. године у часопису *Computer Weekly*.[67] Значајну улогу у развоју овог појма имао је један други појам. То је био појам електронске трговине,[68] као иновационе идеје приватног сектора, за коју је убрзо постају заинтересоване и државе. Даља разрада могућности и потенцијала трговине електронским путем и употреба информационо-комуникационих уређаја, подстакла је развој идеје о дигиталном начину управљања ужим локалним и ширим државним заједницама.

За разлику од данашњег схватања, првобитна употреба појма електронске јавне управе упућивала је само на основне везе информационо-комуникационих технологија и послова јавне управе. У том контексту, под електронском јавном управом подразумевала се употреба фиксних телефона, мобилних телефона, пејџера, нешто касније рачунара и других технолошких средстава у функционисању јавне управе.

Развојем информационо-комуникационих технологија појам електронске управе служи за означавање феномена дигиталног (виртуелног) приказа

[67] P. Henman (2010), 34.
[68] За више о електронској трговини вид. Milan Milosavljević, Vladislav Miškovic, *Elektronska trgovina*, Univerzitet Singidunum, Beograd 2016.

појединих информација о одређеном органу и његовим пословима. У једном тренутку свог развоја, појам електронске управе односио се на постојање интернет презентације државног органа. Са појавом првих интернет страница (примера ради у Сједињеним Америчким државама (САД)) је 1997. године отворена интернет презентација Владе САД-а) јављају и примарни облици електронске јавне управе у облику у коме је познајемо. Ово раздобље у развоју електронске јавне управе поједини аутори називају „аматерским добом".[69] Ипак, већ у овом периоду налазимо примере веома развијених информационо-комуникационих система којима се користе органи јавне власти за вршење својих управних делатности.[70]

Даљи развој појма електронске управе можемо пратити кроз његово дефинисање у прописима и документима међународних организација. Организација за економску сарадњу и развој (*OECD*) је 2003. године, као једна од првих међународних организација на свету, указала на значај електронске управе. У одређењу електронске управе, дефиниција OECD-а је указивала на то да је електронска управа уско повезана са коришћењем информационо-

---

[69] Szilárd Molnár, *E- Government in the European Union*, (online), Budapest 2007, 5, *https://s3.amazonaws.com/academia.edu.documents/8057421/09_molnar_final.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1535474281&Signature=7O6qeJ8biz965HTNVDM%2F%2FkA2PA8%3D&response-content-disposition=inline%3B%20filename%3DeGovernment_in_the_European_Union.pdf*, 28. август 2018.

[70] У пракси упоредних држава налазимо пример увођења програма електронских система у јавну управу још 1997. године, када је Аустралија увела посебан информациони систем у сектор социјалне сигурности. Ради олакшања обављања послова уведен је систем „*Centerlink*", као јединствено електронско управно место (један шалтер за целу управу у области социјалне сигурности). Овај програм превасходно се односио на извршење плаћања у оквиру система социјалног осигурања. Уз то, он је пружао информације и услуге о различитим делатностима аустралијске јавне управе у вези са пословима социјалне сигурности. Такав јединствени електронски прозор (шалтер) користио је и мобилне телефоне ради обавештавања клијената о новим радним местима, месту и датуму разговора за посао и могућностима за добијање савета о различитим питањима у вези са запослењем.

Овај систем је омогућавао бржи и ефикаснији контакт управе и грађана. У оквиру програма многе делатности органа јавне управе су аутоматизоване. Грађанима је омогућено да мењају годишње приходе за порезе или адресу за пријем поднесака путем електронске платформе управе. Главни човек „*Centerlink*", стао је на становиште да је увођењем оваквог система „срушена кула бирократског управљања и пружен јединствени увид сваком појединцу који жели приступ информацијама у услугама државне управе".[70] Међутим, долазак до те тачке није било лак посао, будући да је систем настао коришћењем пословне филозофије, одговарајућих партнерства са (приватним) организацијама, све у циљу бољег рада јавне управе. Основу овог система представљале су информационо-комуникационе технологије.

Овај подухват увођења електронских система у обављање послова јавне управе представља један од првих облика електронске јавне управе у свету, у правом смислу те речи. За више вид. P. Henman (2010), 51.

комуникационих технологија и интернета у вршењу управних делатности. Занимљиво је напоменути да се у истом тексту наводи да би електронска управа требала више да буде усмерена на појам управних активности, него на појам информационих технологија. На тај начин изражена је потреба да електронска управа буде основа квалитетнијим политичким идејама, повећању броја јавних услуга од значаја за модерно друштво и већом партиципацијом грађана у пословима органа управе, а не само иновативни (дигитални) метод обављања управних послова.[71]

Убрзо након тога, развој информационо-комуникационих технологија обезбедио је место новим технологијама у органима управе свих развијених држава. Државе су прихватиле електронску управу као неопходност модерног политичко-друштвеног уређења. Тако се уводе рачунари и други информационо-комуникациони системи који се користе интернетом и другим дигиталним начинима размене података и информација. На тај начин, готово неприметно, управа је ступила у доба „професионалне електронске управе“ које се скоро у потпуности заснива на употреби рачунара и других информационо-комуникационих технологија.

Нешто спорије, такви трендови прихваћени су и у законодавству Србије, где су основни облици информационо-комуникационих технологија предвиђени у општем управном поступку,[72] да би тек 2017. године електронска управа била системски уређена посебним Законом о електронској управи.[73]

Електронска управа је еволуирала током развоја, посебно у начину употребе и могућностима коришћења њеног потенцијала, што је имало утицаја и на одређење њеног појма. Основни чинилац еволуције јесте напредак друштва, односно науке и технологије, као и имплементација нових техничких идеја у вези са дигиталним технологијама у свакодневни живот. Због тога, основано је

[71] Organization for Economic Co-operation and Development, Policy Brief, *The e-government imperative: main findings*, online 2003, 1, *http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN015120.pdf*, 12. фебруар 2019.
[72] У Закону о општем управном поступку, *Службени лист* СРЈ, бр. 33/97 И 31/2001, *Службени гласник* РС, бр. 30/2010, можемо уочити појавне елементе употребе информационо комуникационих технологија у материји општег управног поступка. То се односило на исправе и решења у скраћеном поступку, за које је постојала могућност да буду израђени и у електронској форми.
[73] Закон о електронској управи, *Службени гласник* РС, бр. 27/2018.

очекивати да ће се изменом основних елемената мењати и општи појам електронске јавне управе.

2.5. О правној природи електронске јавне управе

Иако се у јавном дискурсу редовно користи појам електронска јавна управа, ретки су покушаји одређења њене правне природе. Основна препрека на том задатку јесте непрестани развој технике и вишезначност њеног појма који подразумева неколико елемената. Због тога, електронску јавну управу је лакше описати него дефинисати.

Основни чиниоци и кључни појмови за одређење правне природе електронске јавне управе јесу „електронизација“ и „јавна управа“.

Електронизација, у појму електронска јавна управа, односи се на дигиталне аспекте и начине рада органа управе. Може се извући погрешан закључак да се овај термин односи искључиво на дигиталне технологије које користе органи управе за обављање својих делатности. Дигитални (електронски) елементи у управи нису само инструменталне природе, већ они омогућавају брже и ефикасније обављање послова, али и преузимање нових послова који се без коришћења дигиталних технологија не могу извршавати. На тај начин, појам „електронизације“ из корена утиче на правну природу јавне управе.

За објашњење таквих појава могао би се користити и појам „дигитализације“ (дигитална јавна управа), али се појам електронске јавне управе одомаћио у теорији и пракси.

Са друге стране, појам јавне управе остаје кључна одредница која се подразумева све поменуте и обрађене аспекте и елементе јавне управе, као што су субјекти (органи), надлежности, делатности, послови и улоге, састави, итд.

На основу посебне анализе поменутих појмова, можемо издвојити два теоријска приступа у схватању појма јавне управе. На основу једног, електронску јавну управу можемо схватити као нови појавни облик јавне управе. Правна природа јавне управе мења се услед развоја друштва, стварања нових послова и начина њиховог обављања, нових могућности попут дигиталних начина комуникације са грађанима, иновативних облика интерне организације и другачије улоге управе у друштву. Електронска јавна управа не представља исту

ону бирократску организацију са великим бројем папира и документације у којој се не види шта заиста раде службеници и где постоји анимозитет грађана према било каквом контакту са управом, каква је била ситуација пре неколико десетина година.[74] Управа еволуира у праву јавну службу која дигиталним (електронским) путем решава проблеме грађана, комуницира са њима и омогућава квалитетнији однос државе према свим областима друштвеног живота у којима има улогу. Због тога, електронска јавна управа, према овом схватању, представља нови и напредни облик јавне управе.

Посматрајући из перспективе другог становишта, електронску јавну управу можемо посматрати инструментално, као помоћно средство обављања свакодневних делатности органа управе. Употребом информационо-комуникационих технологија уводе се промене у начин обављања послова јавних службеника који сада обављају своје послове на бржи и ефикаснији начин. То значи да јавна управа није изменила своју природу, већ је једино почела да употребљава нове информационо-комуникационе технологије у вршењу својих делатности. Због тога, електронска јавна управа није нови облик јавне управе, већ појам електронске јавне управе говори само о употреби нових техничких елемената у вршењу управних послова.

Сматрамо да је друго схватање уско и да занемарује стварну улогу и позицију електронске јавне управе у савременом друштву. Оно инструментализује „електронски“, односно дигитални елемент јавне управе и занемарује пропратне ефекте који објективно утичу на мењање правне природе јавне управе.[75]

Да ли би органи јавне управе могли да обављају све данашње послове брзо и ефикасно, уколико информационо-комуникациони системи не би постојали? Да ли би се променио начин рада органа управе и врста послова које обављају да није дошло до увођења информационо-комуникационих система у пословање? Одговор на постављена питања је негативан, што значи да се увођењем информационо-комуникационих система у функционисање јавне управе мења и

[74] Упор. С. Лилић (2013), 258.
[75] Због тога се и наводи да се електронизацијом јавна управа редефинише из основа као јавна служба. *Ibid.*

њена природа. Обављањем управних делатности помоћу дигиталних система, управа помаже и себи и грађанима, обављајући на тај начин функцију јавне службе и смањујући ауторитативности у свом деловању. У том смислу, јавна управа, као јавна служба, иде за тим да олакша и помогне грађанима у свакодневном животу, као и да промовише демократске вредности.[76]

Модерно доба је немогуће замислити без коришћења рачунара, мобилних телефона и других средстава електронске комуникације. Због тога, такви трендови захтевају и одређену реакцију органа управе. Како управа и постоји због грађана које води и којима служи, она мора да буде присутна на свим местима на којима се одвијају свакодневне друштвене активности. Да би била присутна и могла да усмерава нову друштвену стварност, јавна управа мора да еволуира и да достигне нове лествице у свом развоју.

Нове тенденције развоја технологије, као што су експертни системи и вештачка интелигенција, настављају да мењају систем рада не само јавне управе, већ и целокупне извршне власти.[77] Одређени послови органа управе, као што су учествовање у креирању и обликовању политике, праћење стања у својим областима, надзор и пружање јавних услуга грађанима остварују свој пун потенцијал тек у ери електронске јавне управе. Вршење ових послова драстично се убрзава и отвара могућност утицаја на нове изазове са којима се управа суочава у „дигиталном свету“.

[76] Драгутин Аврамовић, „Електронска демократија – пут ка непосредној демократији“, *Правни живот*, бр. 12/2012, Београд 2012, 926.

[77] Овај тренд превазилази и извршну власт, па тако долази до дигитализације услуга и судске гране власти, посебно судова који контролишу рад органа управе. За више о дигитализацији рада управног суда вид. Драган Прља, Стефан Андоновић, „Дигитализација рада Управног суда“, Савремена управа, бр. 1, Регула, Београд 2019, 17-22.

2.6. Теоријска одређења појма електронске јавне управе

Мали је број аутора који су покушали да одреде појам електронске јавне управе. Неки од њих су то чинили тако што су појам поделили на основне саставне елементе. У том смислу, Пери (*Perry*) објашњава електронску управу преко четири основна елемента. То су: електронска демократија, електронско пружање услуга, електронски менаџмент и електронско управљање.[78]

Под првим елементом, електронском демократијом, подразумевају се све активности јавне управе које су усмерене на остваривање демократских вредности и приниципа уз помоћ информационих технологија. Путем електронске демократије јавна управа приближава се грађанима олакшавајући им свакодневно остваривање права и интереса. Овај елемент није у толикој мери примењен у пракси држава. Разлог томе лежи у чињеници да су електронске технологије релативно нова друштвена појава, па имајући у виду различите генерације у друштву, још увек постоји потреба за електронским описмењавањем грађана. Сликовито речено, демократија треба електронски да се описмени. Такође, информационо-комуникационе технологије нису доступне свим грађанима, што води кршењу једнакости људи, као важном принципу демократије.

Ипак, идеја електронске демократије и њени појавни облици већ постоје, не само у теорији, већ и у пракси појединих држава. Електронска пријава за гласачки списак,[79] гласање електронским путем,[80] подношење електронских молба, петиција и захтева само су неки од начина остваривања демократије путем информационо-комуникационих технологија. Поменуте радње у основи предузимају органи управе у вршењу својих делатности, па тако електронска демократија садржи и део управно-правне природе. У наредним годинама, уз

[78] P. Perri 6, *E-governance Styles of Political Judgment in the Information Age Polity*, Palgrave Macmillan, UK 2004, 15-17.

[79] У републици Србији, грађани се могу електронским путем пријавити у гласачке спискове. Вид. *http://www.euprava.gov.rs/eusluge/opis_usluge?generatedServiceId=2888&title=Upis-u-bira%C4%8Dki-spisak&alphabet=lat*, 21. август 2018.

[80] Гласање електронским путем добија све више маха широм света. САД, Бразил, Канада су неке од држава у којима електронско гласање већ представља праксу. Такође, у појединим државама у Европи, оваквом начину гласања популарност све више расте, а већ се примењује у Естонији и Белгији. Laurens Cerulus, *E-Democracy entrepreneur: Online voting will boom in coming years*, Euractiv, online 2014, *https://www.euractiv.com/section/elections/interview/e-democracy-entrepreneur-online-voting-will-boom-in-coming-years/* , 21. август 2018.

развој информационо-комуникационих технологија, можемо очекивати даљи развој електронског упражњавања демократије.

Пружање електронских услуга представља други стуб електронске јавне управе. Јавна управа обавља разноврсне послове и пружа широк спектар јавних услуга грађанима. Уколико сама природа тих услуга дозвољава, оне се могу обављати и електронским путем. Тако јавне услуге постају дигитализоване. На овај начин јавна управа и грађани профитирају захваљујући брзини и ефикасности пружања јавних услуга. Као примере пружања услуга електронским путем можемо навести: омогућавање плаћања такси, јавних дажбина и других рачуна електронским путем, коришћење портала електронске управе за добијање потврда из различитих евиденција, пружање информација електронским средствима комуникације, и многе друге. Појавни облици другог елемента електронске јавне управе увелико су присутни у пракси држава и свакодневно се користе.

Електронски менаџмент представља трећи елемент електронске јавне управе који омогућава размену информација и добара унутар структуре и мреже органа јавне управе. Обављање „стандардних“ управних делатности олакшава се електронским начином комуницирања. У вези са електронским менаџментом наводи се да су границе раздвајања са електронским управљањем и електронским пружањем услуга теже уочљиве.[81] Под електронским менаџментом у изложеном смислу подразумева се управљање унутрашњом организацијом органа управе, што представља интерну ствар која има утицаја и у односу према грађанима. Појава овог елемента последица је великог броја активности органа јавне управе и мноштва постављених циљева у различитим делатностима, те је неопходан добро избалансиран систем јавне управе у коме сви делови заједнички комуницирају и тимски функционишу.

Најзад, под електронским управљањем, подразумева се низ различитих делатности које су усмерене у правцу пружања дигиталне подршке формирању државне политике, али и контроле у спровођењу утврђених политика. Овде мислимо на формирање целокупне политике државе, али и на основне начине

[81] P. Perri (2004), 16.

употребе интернета и комуникационих средстава ради остваривања брзине и смањивања трошкова комуникације између министарстава и других организација.

Важно је поменути то да сваки од ова четири стуба не може постојати и функционисати потпуно независно и засебно у односу на остале. Да би један елемент могао да се у потпуности да буде примењен, неопходна је подршка осталих елемената. Анализирајући свака од четири стуба, појединачно и заједно, можемо рећи да изложено схватање на свеобухватан начин одређује саставне делове електронске јавне управе, али на један шири начин, који превазилази оквире јавне управе. Ипак, због своје шаролике и широке делатности, јавна управа се мора разложити на одређене основне чиниоце. Ти чиниоци свакодневно функционишу у симбиози омогућавајући потпуни продор информационо-комуникационих технологија у јавну управу мењајући њену структуру и природу.

У истраживању смо пронашли и друге, сличне ставове. Лилић наводи да је електронска управа „концепт у оквиру којег се информатичка и комуникациона технологија користи на свим подручјима јавне управе и на основу којег се државна управа трансформише и редефинише као јавна служба. У оквиру концепта е-управе, информатичка технологија се широко користи у поступцима пружања низа различитих услуга грађанима…“.[82]

Овај аутор посматра електронску управу кроз три кључна елемента који се односе на: 1. Отвореност и транспарентност активности државних органа, 2. Дигиталне услуге које омогућавају клијентима коришћење интернета за регулисање дажбина, подношење захтева, учешће у поступцима и томе слично, 3. Повезивање органа државне управе. Схваћена на овај начин, електронска јавна управа има посебну природу у односу на „традиционално“ схватање јавне управе. Она по својој природи мање представља власт, а више јавну службу која је усмерена превасходно на остваривање права и интереса грађана. Кључно средство такве промене јесу информационо-комуникационе технологије.

Димитријевић посматра електронску управу као „социјално информациони управно-правни систем који користи *Web апликације* засноване на интернету и друге информационе технологије повезане са процедурама које омогућавају

[82] С. Лилић (2013), 257-258.

примену тих технологија, којима се олакшава приступ и испорука информација и управних служби грађанима, агенцијама и разним владиним органима“.[83] И овај аутор акценат ставља на трансформацију јавне управе, односно редефинисање јавне управе у јавну службу која се заснива на употреби информационо-комуникационих технологија и посебно на интернету.

Врчек и Муса наводе да „у најширем смислу, е-управа представља коришћење информацијско-комуникацијске технологије у јавној управи у сврху повећања ефикасности и учинковитости у пружању јавних услуга и функционирања унутарњих процеса, с једне стране, те повећања транспарентности и одговорности јавне управе, с друге стране.“[84] Ови аутори посматрају електронску јавну управу кроз призму вредности која се остварује новим обликом постојања јавне управе. Употреба информационо-комуникационих технологија омогућава лакшу комуникацију према грађанима, приватном сектору и другим субјектима јавног сектора, олакшава комуникацију унутар органа јавне управе, чиме прати тенденције савременог друштвеног развоја. Аутори стоје на становишту да електронска јавна управа представља нов начин функционисања јавне управе који треба да допринесе остваривању јавног интереса.[85]

Поједине елементе електронске јавне управе налазимо код свих аутора. Основни циљ електронске јавне управе тиче се задовољења потреба грађана и привредних субјеката. У остварењу тог циља велику улогу имају инофмрационо-комуникационе технологије које доприносе квалитету рада и услуга органа јавне управе, чиме се остварује јавни интерес. Нова улога и методологија рада, омогућила је еволуцију јавне управе у електронску јавну управу као нови облик дела извршне власти.

Ипак, нове технологије су дозволиле да одређени сегменти електронске јавне управе зађу дубоко у приватност и свакодневни живот грађана. Због тога, све области које покрива електронска јавна управа морају бити брижљиво

[83] П. Димитријевић, „Електронска управа и информационо друштво“, *Модерна управа- часопис за управно-правну теорију и праксу* (ур. Драгомир Кутлија), Агенција за државну управу Републике Српске, Бања Лука 2009, 121.
[84] Neven Vrček, Antonio Musa, „E-uprava u Hrvatskoj: Izazovi transformacije uprave u digitalnom društvu“, *Forum za javnu upravu- Uprava u digitalno doba*, Friedrich Ebert Stiftung, Zagreb 2016, 9.
[85] *Ibid.*

нормативно уређене да би пружале заштиту од ризика које нове технологије могу створити. Под ризицима се подразумева поштовање права и интереса грађана који долазе у контакт са органима управе у различитим областима друштвеног живота. Због тога је адекватна правна регулатива у посебним областима, основно средство заштите права грађана.

2.7. Појам електронске јавне управе у упоредном праву

2.7.1. Електронска јавна управа у међународним документима

Важност и значај електронске јавне управе препозната је и у документима највећих светских међународних организација. Међу њима свакако највећа јесте Организација Уједињених нација (у даљем тексту: УН). У оквиру Извештаја УН-а о спремности целог света за електронску управу дато је образложење тог појма. У извештају се наводи да „Електронска управа представља употребу информационо-комуникационих технологија и њену примену од стране држава ради пружања информација и услуга грађанима. Према томе, циљ електронске управе је да обезбеди ефикасно пружање информација и квалитетно пружање услуга грађанима, као и да оснажи њихово учешће у доношењу јавних одлука.“[86]

Одређење појма јавне управе налазимо и у документима Организације за економску сарадњу и развој, што представља једну од првих дефиниција на међународном плану у ери „професионалне електронске управе“. Организација за економску сарадњу и развој одредила је електронску управу као употребу информационо-комуникационих технологија и посебно интернета, за средство у остваривању квалитетније управе.[87]

Светска банка у својим студијама указује на значај електронске управе у свету. У једној од студија Светске банке налазимо следеће становиште: „Електронска управа је употреба информационе технологије, као што су рачунарске мреже, интернет, мобилне мреже од стране државних агенција у циљу промене односа према грађанима, компанијама и другим деловима државе.

[86] United Nations, *UN Global E-government Readiness Report 2005 - From Egovernment to E-inclusion, UN Department of Economic and Social Affairs*, Division for Public Administration and Development Management, New York 2005, 14.
[87] OECD (2003), 1.

Такође, то је недвосмислена обавеза доносилаца одлука о јачању сарадње између јавног сектора и приватних лица“.[88]

Значај електронске јавне управе препознат је и у Европској унији.[89] У њеним оквирима, електронска управа се посматра као основно средство за остваривање квалитетне (добре) јавне управе.[90] У једном од својих докумената, изражен је следећи став ЕУ у вези са електронском управом: „Електронском управом пружа се подршка управним поступцима, побољшава квалитет услуга и повећава унутрашња ефикасност јавног сектора. Дигиталне јавне услуге смањују притисак управе на правна лица и грађане, чинећи њихову интеракцију са јавном управом бржом, ефикаснијом, практичнијом, транспарентном и јефтинијом. Уз то, коришћењем дигиталних технологија као саставног дела стратегије модернизације управа могу се остварити додатне привредне и социјалне делатности за цело друштво. Дигитална трансформација управа кључан је елемент успеха јединственог тржишта“.[91]

Имајући у виду значај поменутих организација и њихових докумената на међународном плану, можемо закључити да електронска јавна управа представља глобални феномен који има важно место у развоју главних полуга и покретача друштвеног развоја.

2.7.2. Електронска јавна управа у појединим државама

2.7.2.1. Електронска јавна управа у Аустрији

Аустрија је једна од држава чланица ЕУ која највише улаже у област информационих технологија и активно ради на њиховом потпуном увођењу у јавну управу. У овој држави се већ неколико деценија формира инфраструктура електронске јавне управе. Федерални закон о електронској управи Аустрије донет

[88] Roberto Panzardi, Carlos Calcopietro, Enrique Fanta Ivanovic, *New-Economy Sector- Study Electronic Government and Governance: Lessons for Argentina*, The World Bank, Washington DC 2002, 2.
[89] У даљем тексту за појам Европске уније биће коришћена скраћеница - ЕУ.
[90] S. Lilić, „Legal Framework of E-Government in Europe of Knowledge“, *Legal, Political and Economic Initiatives Towards Europe of Knowledge* (ed. Kestutis Kriščiunas), Kaunas University of Technology, Kaunas 2006, 20.
[91] European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions EU, E-government Action Plan 2016-2020, Accelerating the digital transformation of governments*, European Commission, Brussels 2016, 2.

је 1. марта 2004. године,[92] да би у годинама које следе овај закон био неколико пута допуњен и измењен. Основни принципи на којима се заснива електронска управа у Аустрији јесу поштовање слободе избора у начину комуникације грађана и органа јавне управе, безбедност комуникације и заштита личних података који се размењују у таквој комуникацији.

Један од основних стубова електронске управе у Аустрији односи се на „грађанску карту". Грађанска карта представља документ који омогућава дигиталну идентификацију грађана у електронским односима са органима јавне управе. Она се осликава и кроз електронски потпис који замењује ручни потпис грађанима. Ради идентификације у односима користи се шифра која је јединствена за свако физичко лице и води се у Централном регистру грађана. Она се користи уз идентификационе интернет линкове који омогућавају приступ само овлашћеним лицима који познају своју шифру. На тај начин се остварује безбедност у комуникацији и сигурност података. Федерални закон о електронској управи Аустрије предвиђа и начине електронске потврде примања и слања података, чувања електронских података и казнене санкције за непоштовање одредаба овог закона.

У јавној управи Аустрије присутни су различити облици информационо-комуникационих технологија, па се електронска управа остварује преко рачунара, мобилних телефона и других уређаја који омогућавају размену података и информација.

[92] Пун назив овог закона јесте Федерални Закон о одредбама које олакшавају електронску комуникацију са органима јавне власти (Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen (E-Government-Gesetz – E-GovG) StF: BGBl. I Nr. 10/2004 (NR: GP XXII RV 252 AB 382 S. 46. BR: 6959 AB 6961 S. 705). Текст закона је доступан на: *https://www.ris.bka.gv.at/Dokumente/Erv/ERV_2004_1_10/ERV_2004_1_10.pdf*, 19. децембар 2018

2.7.2.2. Електронска јавна управа у Немачкој

Правна регулатива у вази са електронском јавном управом у Немачкој, као држави чланици ЕУ, новијег је датума. Најважнији закон у овој области, Закон о електронској управи[93] усвојен је 2013. године. Овај закон има за циљ да омогући електронску комуникацију између грађана, привредних субјеката и органа јавне управе. Такође, још један од циљева закона јесте да услуге јавне управе постану доступне путем информационих сервиса државе и њених органа.

Дигитализација рада и услуга представља обавезу свих органа јавне управе, који морају да омогуће електронску комуникацију, електронску обраду докумената и коришћење електронског потписа. Такође, органи морају омогућити и плаћање електронским путем. Закон прописује и начине поступања са електронским документима и комуникацијом, као и поступање са документима у папирном облику.

Сврха оваквих мера јесте шира употреба информационо-комуникационих технологија у јавној управи које омогућавају бржи и ефикаснији рад, као и квалитетнији однос са грађанима који користе електронске услуге. Електронска управа огледа се и у објављивању прописа и других општих аката у електронском облику, као начин остваривања демократских вредности.

Осим Закона о електронској управи, у Немачкој постоји и низ посебних закона који уређују поједина питања од значаја за функционисање електронске јавне управе. Примера ради, то су Закон о повезивању информационих система федералне и државних јединица, Закон о слободном приступу информација, Закон о заштити података, Закон о електронском потпису, Закон о електронској трговини и многи други.

Одредбе Закона о електронској управи примењене су у бројним програмима електронске управе и услугама које органи управе нуде, тако да су у пракси присутне електронске личне карте, електронски пасоши, итд. Такође, у Немачкој функционишу и бројни информациони системи органа јавне власти,

[93] Закон о електронској управи Немачке- Gesetz zur Förderung der elektronischen Verwaltung (E-Government-Gesetz - EGovG), vom 25. Juli 2013 (BGBl. I S. 2749), *https://www.gesetze-im-internet.de/egovg/EGovG.pdf*, 09. фебруар 2019.

попут Федералне електронске платформе јавних набавки, Регистра услуга, портала отворених података, итд.

2.7.2.3. Електронска јавна управа у Црној Гори

Црна Гора је није чланица ЕУ, већ је кандидат за чланство, па своје законодавство усклађује са европским, што је доводи у сличан положај као и Србију. У Црној Гори је 2014. године усвојен Закон о електронској управи.[94] Овај закон усмерен је на питања електронске комуникације између органа јавне управе, грађана и привредних субјеката у случајевима обраде, размене и објављивања података и информација у електронском облику.

Као основни стубови електронске управе у Црној Гори функционишу портал електронске управе и јединствени информациони систем за електронску размену података. Ова два стуба представљају информационе системе у оквиру којих се електронским путем размењују подаци између поменутих актера. Омогућено је електронско слање и пријем поднесака у комуникацији са органима управе. Предвиђене су и бројне казне за непоштовање одредаба овог закона, што говори о стратешкој важности овог питања у Црној Гори.

Прописивањем наведених решења, тежи се стварању друштвеног амбијента у коме ће органи јавне управе бити трансформисани у јавну службу, односно сервис грађана који служи остварењу демократских принципа и вредности. У процесу дигитализације јавне управе, посебну улогу има Директорат за електронску управи и информатичку безбедност, који се налази у саставу Министарства јавне управе. Поједине одредбе од значаја за електронску управу налазе се у Закону о електронској идентификацији и електронском потпису, Закону о информационој безбедности, Закону о заштити података о личности, итд.

[94] Закон о електронској управи Црне Горе, *Службени лист ЦГ*, бр. 32/2014.

3. ЕЛЕКТРОНСКА ЈАВНА УПРАВА У СРБИЈИ

3.1. Регулаторни оквир електронске јавне управе у Србији

3.1.1. Стратегија реформе државне управе из 2004. године

Електронска јавна управа представља младу појаву у правном систему Србије. Процес дигитализације (електронизације) јавне управе одвијао се заједно са свеобухватном реформом јавне управе, која је започета 2004. године. Те године, Влада Србије усвојила је стратешки документ под називом „Стратегија реформе државне управе у Републици Србији“.[95] Основни циљ ове Стратегије био је да унапреди, усаврши, модернизује и припреми државну управу за изазове европских интеграција, али и свеопштег друштвеног напретка. Главне области реформе односиле су се на децентрализацију, професионализацију и деполитизацију, рационализацију, координацију јавних политика, унапређење контролних механизама и модернизацију државне управе у Србији. Ради успешне реализације овог стратешког документа донети су и акциони планови за период од 2004-2008. год. и 2009-2012. год.

Једна од основних реформских области односила се на шире увођење информационо-комуникационих технологија у државну управу и њену припрему за дигитализацију. Током више година спровођења реформи усвојено је неколико важних закона који су се односили на електронски потпис, електронски документ и електронске комуникације. Такође, у низу закона усвајане су одредбе које су омогућавале увођење информационо-комуникационих технологија у различитим областима управног деловања.

Током реформског периода електронска управа постала је једна од кључних тачака реформе јавне управе, али и напретка друштва. На основу анализе постојећег оквира и потенцијала за функционисање електронске управе, констатовани су недостаци и потребна техничка подршка за њено успостављање у пуним капацитетима. У том периоду Србија је усвојила Уредбу о електронском канцеларијском пословању, као и Упутство за њену примену. У овом реформском

[95] Стратегија реформе државне управе у Републици Србији из 2004. год. Стратегија је доступна на интернет презентацији Владе Србије, *http://www.gs.gov.rs/lat/strategije-vs.html,* 30. август 2018.

периоду усвојена је и Стратегија развоја електронске управе у Републици Србији (2009. до 2013. год.), као и Стратегија развоја информационог друштва у Републици Србији (до 2020. год.).

Значајан корак у даљем развоју електронске управе представљао је Национални оквир интероперабилности, кога је донело Министарство спољне и унутрашње трговине и телекомуникација 2014. год. Овим документом истакнут је став о наставку увођења електронске јавне управе у Србији. У том процесу, значајну улогу има и интероперабилност, као кључни елемент квалитетне комуникације, ефикасног пружања услуга и брзе размене информација органа у оквирима јавне управе.

3.1.2. Стратегија реформе јавне управе из 2014. године

Период реформских промена унутар државне управе настављен је са тежњом да се ефекти реформе прошире на све органе јавне управе. Стога је 2014. године усвојена Стратегија реформе јавне управе у Републици Србији.[96] Једно од основних поглавља ове Стратегије односи се на развој електронске управе. Значај електронске јавне управе подразумева неколико нивоа развоја јавне управе. „Најпре, то је успостављање и квалитетније вођење евиденција, већа поузданост и ажурност података, међусобна повезаност и размена података. У вези са тим, електронска управа је од значаја за стратешко планирање, обликовање јавних политика и праћење њиховог спровођења, лакше утврђивање чињеничног стања, праћење тока предмета и евиденција донетих одлука при вођењу управног поступка и поступка инспекцијског надзора, праћењу управне и управносудске праксе. Поред тога, е-управа је од значаја за вођење евиденције о органима и организацијама јавне управе, запослених (са подацима о конкурсима, поступцима пријема у службу, компетенцијама, знањима и вештинама, стручном усавршавању, напредовању у служби, престанку радног односа)“.[97]

Према Стратегији, употреба информационо-комуникационих система треба да буде усмерена на ефикасност и економичност обављања послова органа

[96] Стратегија реформе јавне управе у Републици Србији, *Службени гласник* РС, бр. 9/2014 и 42/2014-исправка.
[97] Стратегија реформе јавне управе у Републици Србији, 27.

јавне управе, али и на пружање јавних услуга грађанима и правним лицима. Да би се то остварило, неопходно је направити електронску магистралу (магистрална мрежа) државних органа која ће функционисати на целој територији Србије.

Изражена је потреба да се смањи улога људског фактора у обављању електронских делатности органа јавне управе и тежња да се процеси унутар органа аутоматизују. Стратегија наводи и кључне изазове у развоју електронске управе у Србији. То су:

1. Координација и сарадња између органа државне управе по питању развоја е-управе,
2. Правна регулатива у области развоја е-управе,
3. Дигитализација и аутоматизација управних поступака и административних и пословних процеса,
4. Капацитет људских ресурса (успостављање информатичке писмености државних службеника),
5. Степен информационе безбедности у систему јавне управе.[98]

Поменути изазови представљају тачке од кључне важности за даљи развој електронске јавне управе у Србији. Да би информационо-комуникациони системи могли у потпуности да остваре своју улогу у вршењу делатности јавне управе, неопходно је установити адекватан правни оквир. Осим тога, техничка опремљеност мора бити на одговарајућем нивоу, јер без тог елемента нема ни дигитализације управних делатности.

Електронска писменост и припремљеност људских капацитета (јавних службеника) за нове методе обављања послова неопходан је услов за електронизацију јавне управе, што се може постићи образовањем и усавршавањем кадрова. На крају, важно је развијати степен информационе безбедности у систему јавне управе. Ово је можда и кључни елемент електронске јавне управе, будући да органи управе обављају различите послове и користе се важним личним подацима грађана у тим пословима. То говори у прилог тези да посебан акценат у развоју електронске управе мора бити постављен на сигурност

[98] Стратегија реформе јавне управе у Републици Србији, 28.

електронских система и безбедност података у оквирима електронске јавне управе.

3.1.3. Стратегија развоја електронске управе у Републици Србији

О важности развоја електронске управе у Србији сведочи и стратешки документ који је посвећен искључиво развоју електронске управе. То је Стратегија развоја електронске управе у Републици Србији за период од 2015-2018. год. Заједно са овом Стратегијом усвојен је и Акциони план за спровођење стратегије за период од 2015-2016. год.

Стратегија тежи да оствари дигиталну повезаност различитих области друштвеног живота у којима се обављају послови јавне управе. То се односи на здравство, образовање, учествовање грађана у одлучивању, сектор јавних набавки, социјалних политика, итд. Један од циљева Стратегије јесте да изврши утицај на развој информационог друштва, да обезбеди сигурност података и електронских трансакција, безбедност података о личности у поседу јавне управе и доступност и приступачност отворених података од значаја за ширу заједницу. Дакле, различити подаци који се размењују електронским средствима комуникације имају једно од централних места у електронској јавној управи.

Електронска управа треба да представља мотор развоја правних вредности и принципа који су садржани у Уставу, а који имају утицај на све области друштвеног живота. Вредности се односе на транспарентност државних органа, владавину права, заштиту од дискриминације, пружање информационе безбедности грађанима, итд. Да би се наведене вредности остариле, Стратегија одређује опште циљеве развоја које електронска управа треба да задовољи. То су:

1. Повећање задовољства корисника јавних услуга,
2. Смањење терета администрације за привредне субјекте и грађане,
3. Повећање ефикасности јавне управе употребом информационо-комуникационих технологија,

4. Национална и прекогранична интероперабилност (посебно са државама ЕУ).[99]

Као носећи стуб електронске управе партиципира национални „*Портал еУправа*“. Овај портал представља главну дигиталну саобраћајницу електронске размене информација са другим порталима и базама података свих органа управе. Циљ такве електронске комуникације јесте да повеже јавну управу, грађане и привреду како би се остварио пуни потенцијал јавних услуга која пружају органи управе.

Надлежност за уједначавање и усаглашавање информационо-комуникационих система поверена је Дирекцији за електронску управу, као органу у саставу Министарства државне управе и локалне самоуправе. Дирекција обавља административне, техничке и стручне послове у вези са функционисањем електронске управе. Осим дирекције, у Србији постоји и Савет за реформу јавне управе који даје предлоге развоја јавне управе уопште, али тиме неминовно залази и у области електронске управе.

3.2. Позитивно-правни прописи Србије у вези са електронском јавном управом

Норме које регулишу електронску управу у Србији тренутно се налазе у различитим позитивно-правним прописима. Поред појединачних решења о увођењу инофмрационо-комуникационих технологија у вези са општим управним поступком (Закон о општем управном поступку), у Србији постоји и закон који је посвећен искључиво питањима електронске управе. То је Закон о електронској управи. Поред поменутих закона, бројни облици дигиталног поступања и коришћења информационо-комуникационих технологија налазе се у законима који уређују посебне (управне) области.

[99] Вид. Стратегија развоја електронске управе у Републици Србији за период од 2015-2018. године, 16.

3.2.1. Закон о електронској управи

О значају електронске управе сведочи и посебна законска регулатива. Закон о електронској управи уређује питања употребе информационо-комуникационих технологија и електронске комуникације и размене података између органа јавне управе и грађана. Иако се различити елементи електронске управе налазе у посебним прописима, Закон о електронској управи наводи да се питања електронске управе уређена тим законом не могу уређивати, нити мењати посебним законима. То значи да је потребно извршити свеобухватно усклађивање законских и подзаконских прописа како би у пракси заживела поменута одредба. Ово је од посебног значаја како би се обезбедила стандардизација која је неопходна за квалитетно функционисање електронске управе и одговарајући степен заштите грађана.

Основна начела на којима почива електронска управа су: начело ефикасности управљања опремом, начело сигурности електронске управе и забрана дискриминације. Наравно, у коришћењу информационо-комуникационих технологија морају се примењивати уставна начела и основна начела управног поступка.

Начело ефикасности управљања опремом значи да орган мора да обезбеди ефикасну и економичну примену информационо-комуникационих технологија у складу са техничким правилима и правилима управних поступака, било општег било посебних. Технологије се не смеју користити супротно циљу ради кога су уведене у јавну управу, а то су задовољење јавног интереса и потреба грађана.

Начело сигурности електронске управе односи се на то да „информациони системи, електронске комуникационе мреже и опрема која се користи за вршење електронског управног поступања морају да испуњавају услове и стандарде информационе безбедности“[100]. Информациона безбедност је изузетно важна компонента електронске управе, будући да од њеног квалитета зависи и остваривање правне сигурности. Установљавањем адекватне заштите чува се интегритет учесника у управном поступку и пружа се безбедност личним подацима који се у истом поступку користе.

[100] Чл. 6, Закона о електронској управи.

Забрана дискриминације нашла је своје место и у сфери електронске управе. Она се односи на два момента. Прво, сва лица имају право да користе услуге електронских сервиса и електронског управног поступања, што значи да свима мора бити омогућен електронски приступ понуђеним јавним услугама, без обзира на било које лично својство. Друго, лицима која нису у могућности (примера ради, лица са инвалидитетом) да користе услуге електронске управе у изворном облику, мора бити омогућено да користе услуге адекватно околностима конкретног случаја и у складу са својим могућностима. Закон не говори ништа о конкретизацији овог начела, па је то остављено прописима ниже правне снаге и пракси да ближе уреде ову проблематику.

3.2.2. Основни елементи електронске јавне управе у Србији

Можемо рећи да се систем електронске јавне управе у Србији заснива на два носећа стуба. То су инфраструктура електронске управе и електронско управно поступање. Око централних стубова гради се посебна регулатива која чини систем функционисања електронске јавне управе.

Као део инфраструктуре електронске јавне управе, уведена је јединствена информационо-комуникациона мрежа органа управе, као мрежа преко које се врши пренос података између управних органа. Како би се омогућио сигуран приступ мрежи и осигурала безбедност података установљена је надлежност Центра за безбедност информационо-комуникационих система републичких органа (ЦЕРТ), који функционише као део службе Владе. Овај орган је задужен за одобравање приступа информационо-комуникационој мрежи и врши друге безбедносне провере мреже.

Електронски портали представљају други део инфраструктуре електронске јавне управе у Србији. Најзначајнија „спољна“ контактна тачка са грађанима и привредом је „*Портал еУправа*“. Портал се ослања на Јединствену информационо-комуникациону мрежу управних органа и служи као „дигитални прозор“ у комуникацији управних органа и грађана. Грађани и привредни субјекти могу преко овог портала захтевати остваривање дигитализованих услуга управе, плаћати таксе, накнаде и друге трошкове, пријављивати неправилности рада појединих органа и томе слично. Орган на Порталу еУправа може

успоставити јединствено електронско управно место.[101] Портал отворених података је још један информациони портал на коме сва заинтересована лица могу приступити отвореним подацима који су од значаја за друштво, доступни свима, машински читљиви и дозвољавају употребу у сврху другачије од оне за коју су прибављени, а налазе се у поседу органа управе.

Од осталих инфраструктурних елемената електронске управе, неопходно је поменути регистре података и евиденција. Ради сигурности, лакше доступности и ефикасности коришћења података из ових база, прописано је да се оне сачињавају и чувају у електронском облику. Осим база података којима се користе у свом пословању, овим законом успостављен је и електронски регистар мета података-метарегистар.[102] Метарегистар служи за евиденцију и чување података од посредног значаја за обављање послова јавне управе, али од непосредног значаја за вођење евиденције приступа и коришћењу података неопходних за обављање тих послова.

Веб презентације, односно интернет сајтови, представљају обавезни део у изградњи електронске јавне управе. Сваки управни орган има дужност да сачини, али и одржава веб презентацију. У електронском свету интернет презентација представља најлакши начин приступа услугама и комуникацији са органима јавне управе. Тиме се остварује ближи и бржи контакт управе са грађанима. Такође, овим се остварује и транспарентност, као једно од кључних принципа у функционисању јавне управе.

Електронско управно поступање представља други основни стуб око кога је саздана електронска управа у Србији. Данас није довољно само да управни орган и његове услуге буду електронски видљиве грађанима и привредним субјектима. Брз темпо живота и потребе привреде условљавају да се услуге

[101] Члан 18, Закона о електронској управи. Јединствено управно место се оснива када је за остваривање једног или више права потребно поступање једног или више органа, при чему странка не мора да се обраћа свим тим органима, већ се обраћа само јединственом управном месту, где може бити поучена о даљем току свог захтева, предати захтев за признавање права и обавештена о другим могућностима у вези са својим захтевом. У Србији, 2018. године, Министарство државне управе и локалне самоуправе ради на пилот пројектима успостављања јединственог управног места у неколико општина. Пројекат је првобитно бити усмерен на олакшавање управних процедура у вези са купопродајом половних аутомобила. Нав. према: *http://www.subotica.rs/index/page/lg/cp/id/11862*, 13. септембар 2018.

електронске управе убрзају, постану ефикасније и приступачније. Због тога, неопходно је да органи јавне управе обављају своје послове електронским путем, пруже дигиталне јавне услуге и да омогуће њихову комуникацију са грађанима и привредом.

Постоји низ послова и области органа управе који се морају дигитализовати како би јавна управа испунила своју улогу јавне службе. То препознаје и Закон, па прописује услове за прибављање и уступања података и електронских докумената, начине приступа електронским захтевима и порталима, електронско достављање и електронску комуникацију са другим органима.[103] Ради правилне примене закона, у оквиру казнених одредаба, прописана је и казнена одговорност за одговорна лица у органима управе у случају незаконитог или немарног поступања.

3.2.3. Закон о општем управном поступку

Други пропис од значаја за електронско поступање органа управе јесте Закон о општем управном поступку. Овим законом уређују се правила општег управног поступка, што отвара простор за електронско поступање које је промовисано у Закону о електронској управи. То се односи на могућност органа да поучавају подносиоце захтева, примају захтеве за признање права или друге врсте поднесака у управним стварима и да обавештавају подносиоца захтева о току поступка електронским путем.[104] Као пример увођења дигитализације рада у рад управних органа, наводимо обавезу прибављања и обрађивања података о чињеницама о којима се води службена евиденција, а који су неопходни за одлучивање, по службеној дужности. Такве податке органи могу да размењују и електронским путем.[105] Такав начин поступања је повезан са начелима делотворности и економичности, али и са завршним одредбама, где је речено да престају да важе одредбе посебних закона којима се од странака захтева да

[103] Вид. чл. 32-42, Закона о електронској управи.
[104] Чл. 42, Закона о општем управном поступку.
[105] Чл. 103, Закона о општем управном поступку.

достављају документа којима се доказују чињенице о којима органи воде службене евиденције.[106]

Дакле, технологија се користи превасходно у сврху лакшег и бржег остваривања комуникације између органа и странке (Закон о општем управном поступку то назива „електронским општењем“). Чување база података и различитих докумената у електронском облику омогућава и разгледање списа предмета у дигиталном облику.

Једна од најзначајнијих радњи у управном поступку јесте достављање, које иако представља вид обавештавања учесника поступка, има велики утицај на права, обавезе и интересе странака. Сви облици достављања (лично и посредно), могу се вршити и електронским путем, под условом да су странке на то пристале.[107] Доставница, као потврда о томе да је лично или посредно достављање извршено, може бити у електронском облику. Решење, као најважнији акт у управном поступку ради чијег доношења се управни поступак и покреће, може бити издат у форми електронског документа. Сматрамо да у општем управном поступку има још простора за увођење дигиталних елемената, што се односи на начин одржавања целокупног поступка, извођење доказа и доношење одлуке. Закон о општем управном поступку познаје институт видеоконференцијске усмене расправе, али само за оне органе који има техничке могућности да такву врсту расправе закаже и одржи.[108] Овакав начин дигиталног одржавања расправе треба полако уводити као правило. На тај начин уштедело би се и време и новац неопходан да сва лица приступе органу ради одржавања поступка. Већом дигитализацијом општег управног поступка, отвара се простор за увођење дигиталних елемената и у посебне управне поступке.

[106] Чл. 215, Закона о општем управном поступку.
[107] Чл. 72, Закона о општем управном поступку.
[108] Чл. 111, Закона о општем управном поступку.

3.2.4. Закон о пореском поступку и пореској администрацији

Одредбе Закона о општем управном поступку и Закона о електронској управи прате закони који уређују посебне управне области. Такав је случај са Законом о пореском поступку и пореској администрацији (у даљем тексту ЗППА).[109] ЗППА има у виду то да су грађани и привредни субјекти одавно у својим пословима прешли на електронске начине комуникације и дигиталну документацију. Због тога, када је неопходно приступити подацима од значаја за утврђивање пореза, порески обвезници морају уступити потребне документе и у електронској форми на електронским носачима података.[110]

Омогућена је електронска комуникација између странака и пореско-управних органа. Пореским обвезницима омогућено је да и електронске пријаве пореза достављају у електронском облику. На сличан начин као и у материји општег управног поступка, ЗППА уређује форму аката које издају порески (управни органи). Порески управни акт, као посебни облик управног акта, може се донети у електронском облику. Иста ситуација је и са осталим пореско – управним актима који се доносе ради вођења и одлучивања у пореском поступку.[111]

3.2.5. Царински закон

Продор и афирмацију у посебне управне поступке информационо-комуникационе технологије остварile су и у области царина. Мноштво информација и података који царински органи морају да размене са другим органима управе и грађанима, захтева ефикасну размену великих количина података и брзу комуникацију. Због тога, важност информационо-комуникационих технологија у вршењу надлежности царинских управних органа препознаје и основни закон у овој области - Царински закон.[112] Овај закон уређује правила и поступке који се примењују на робу која се уноси и износи из

[109] Закон о пореском поступку и пореској администрацији, *Службени гласник* РС, бр. 80/2002 и 30/2018.
[110] За све податке који морају бити достављени пореском органу у електронском облику вид. чл. 37а, ЗППА.
[111] Вид. чл. 35, ЗППА.
[112] Царински закон, *Службени гласник* РС, бр. 18/2010, 111/2012 и 113/2017- др. закон.

царинског подручја Србије. Царински органи треба да уведу и примене информационо-комуникационе технологије, када је то исплативо и ефикасно за Управу царина, као и за привреду уопште.[113]

Под информационо-комуникационим технологијама подразумевају се методе електронске трговине и методе електронског утврђивања исправности података и робе. Одређене радње могу се вршити електронским путем, као што је случај са подношењем декларације и сажете декларације. Уопште узев, царински органи морају омогућити да се комуникација са привредним субјектима одвија електронским путем, чиме се уважавају потребе друштва и привреде.

Треба подвући то да уколико неко од питања није детаљно регулисано посебним законом, на њега се имају применити норме општег управног поступка, што аналогијом важи и за поменуте „дигиталне одредбе“ посебних управних поступака.

3.2.6. Закон о државном премеру и катастру

Закон о државном премеру и катастру[114] представља још један од закона који уређује посебну управну област. Предмет уређења овог закона јесу стручни послови и послови државне управе које се односе на државни премер, катастар непокретности, катастар водова, адресни регистар, итд. Као важна институција у друштву, катастар мора брзо и ефикасно обављати свој посао будући да остваривање права својине, као једног од основних људских права, али и остварење многих других права и интереса, зависи управо од квалитета функционисања овог органа.

Ради лакшег и ефикаснијег приступа његовим подацима и услугама катастар развија геодетско-катастарски информациони систем који садржи бројне податке о непокретностима, адресама непокретности, водовима и томе слично. Због тога, преко геодетско-катастарског информационог система могу се издавати документа у електронском облику. Такође, катастар се стара о електронским начинима пружања услуга пословног промета за коришћење података и сервиса

[113] Чл. 4, Царинског закона.
[114] Закон о државном премеру и катастру, *Службени гласник* РС, бр. 72/2009, 65/2013, 15/2015 – одлука УС, 96/2015, 47/2017 и 41/2018 – др. закон.

катастра.[115] Као и сви други органи јавне управе, катастар је прописао увођење канцеларијског електронског пословања.

***

На основу изложеног можемо закључити да се управни поступци, општи и посебни, полако дигитализују и у Србији. Пре свега, Законом о електронској управи и појединим одредбама Закона о општем управном поступку, створене су претпоставке које уводе информационо-комуникационе технологије у обављање управних делатности. Те претпоставке су делимично прихваћене и у законима који уређују посебне управне области.

Ипак, простора за напредак у овом пољу има много. За потпуну трансформацију јавне управе у електронску јавну управу неопходно је омогућити дигитално вођење управних поступака. Наравно, није могуће дигитализовати све управне поступке, али они поступци који се могу окончати забелешком на спису предмета, без узимања изјаве странака у поступку или у једноставнији једностраначки управни поступци могу се потпуно трансформисати у дигитални облик. То би водило још ефикаснијем обављању управног одлучивања и што је још важније, остварила би се велика новчана и временска уштеда, како странкама, тако и поступајућим органима. За потпуни прелазак неопходно је обезбедити сигурност информација и података који се користе у управним поступцима, будући да интегритет личности грађана зависи од безбедности информационог система и заштите података.

3.3. Практични аспекти електронске јавне управе у Србији

Стратешки и законски документи садрже општа правила понашања која се конкретизују кроз различите практичне појавне облике. Када се томе дода и стално усавршавање информационо-комуникационих технологија долазимо до закључка да је електронска јавна управа променљива категорија која се непрестано усавршава и развија. Због тога, неопходна је анализа стања електронске јавне управе у пракси, како би се уочили стварни друштвени аспекти ове појаве. Због тога, аутор ће посветити пажњу тренутном стању електронске

[115] Чл. 158, Закона о државном премеру и катастру.

управе и њених сервиса у Србији. На тај начин, доћи ћемо до целовите слике електронске јавне управе у српском друштву.

3.3.1. Портал еУправе Републике Србије

Портал еУправе представља најзначајнији облик електронске комуникације грађана, привредних субјеката и органа управе. Овај портал представља електронски јавни сервис преко кога грађани могу захтевати одређене дигитализоване услуге које пружају управни органи и остварити различита права и интересе. Као јавни сервис, Портал служи остваривању демократских вредности и принципа у раду јавне управе. Сви подаци и информације које су објављене на овом сервису представљају информације од јавног значаја, па се могу прегледати, копирати и даље употребљавати у личне и некомерцијалне сврхе. Наравно, лични подаци грађана не смеју се јавно објављивати.

Приступ порталу је упрошћен, будући да се грађани за коришћење услуга са овог портала могу пријавити само на основу своје електронске адресе и изабране шифре за приступ. За овлашћена лица у правном лицу поступак је сличан, уз допунски услов да администратор портала добије потврду о томе да је то лице званично овлашћено од стране правног лица. Порталу се може приступити и путем електронског сертификата. Пријавом на портал, корисник добија могућност да користи понуђене електронске услуге органа управе, да испуњава понуђене јавне обавезе у дигиталној форми, да прати статус свог предмета у вези са поднетим захтевима у управном поступку, право да електронски учествује у актуелним јавним расправама о законима и другим општим актима, као и друге омогућене радње.

На овом порталу, у тренутку израде истраживања, могу се наћи услуге које обухватају више од 150 органа јавне управе, са тенденцијом даљег раста. У оквиру тих органа може се приступити електронским услугама свих државних министарстава, 5 судова, преко 18 градова, 8 градских општина, 35 општина, канцеларија, дирекција, агенција, инспектората, завода, Народне банке, управних округа и других.

Категоризација услуга је извршена према више критеријума. Први се односи на субјекте који траже или на кога се односе услуге, па тако се јавља подела на:

1. Грађане,
2. Привреду,
3. Управу[116]

У оквиру сваке од примарних области, даља класификација се врши према животним областима у оквиру којих се остварује одређено право, обавеза или правни интерес грађана.

У оквиру понуђених услуга које се односе на грађане, предвиђено је неколико подобласти у оквиру којих постоји могућност за приступ потребној документацији, извршењу услуга, заказивању датума пријема у органима јавне управе, и томе слично. Те области се тичу породичних питања (деца и социјална помоћ), образовања (високо образовање, јавне библиотеке, стручно усавршавање, курсеви, едукација у дијаспори), здравља (здравствено осигурање, здравствена заштита, социјална заштита, биомедицина), документације (лична документа, потврде и уверења, матичне књиге, упутства), саобраћаја (возила, документа, кампање), рада (запослени, незапослени, јавни конкурси за радна места), становања и животне средине (урбанизам и непокретности, животна средина, природни ресурси, комуналне услуге, водопривреда, пољопривреда), финансија (порези, конкурси), пословања (регистрација предузетника, изводи, потврде, уверења, кредити, званична статистика), јавног реда и мира (Републичко јавно тужилаштво, кривична пријава, инспекције), спорта и омладине (спорт, кредити), особа са инвалидитетом (у вези са правима особа са инвалидитетом, социјална заштита, возила и паркирање, пореске и царинске олакшице, закони), катастра (катастар непокретности, катастар водова), људских права (слободан приступ информацијама, заштита података о личности), ванредних догађаја (ванредне ситуације), туризма (смештај), пољопривреде и водопривреде (земљиште,

[116] Портал еУправа Републике Србије, *https://www.euprava.gov.rs/*, 14. септембар 2018.

документа) и Град Београда (области за које је надлежан град Београд као посебна јединица локалне самоуправе).[117]

У делу који се односи на привреду, као понуђене области у оквиру којих се може електронски приступити одређеним услугама јавне управе, јављају се; пословање (подобласти: регистрација предузећа, изводи, потврде, уверења, технички прописи, кредити, званична статистика), јавне набавке (јавне набавке, потврде и уверења), животна средина и просторно планирање (урбанизам, животна средина, рударство и геологија, комуналне услуге), финансије (велики порески обвезници, порески обвезници), увоз/извоз (царина, извоз), образовање (стручно усавршавање), саобраћај (возила, документа), статистика (званична статистика), здравље (здравствена заштита, регулатива лекова у хуманој медицини, регулатива лекова у ветеринарској медицини, регулатива медицинских средстава), спорт и омладина (кредити, спорт), катастар (катастар непокретности, катастар водова), енергија (рационално коришћење енергије), рударство (природни ресурси), туризам (смештај), услуге Града Београда (све области које град Београд извршава као посебна јединица локалне самоуправе), водопривреда и пољопривреда (документа).

Област која носи назив „Управа“ садржи списак услуга које пружају државни органи, а које се поклапају са претходно поменутим областима којима се може приступити путем портала.

У оквиру поменутих области, налази се Интернет линк који упућује до новог интернет прозора који објашњава начин пружања поједине услуге. Ипак, како је развијање дигиталне документације и електронских услуга у току, није могуће извршити све услуге електронским путем. Због тога, јасно су обележене услуге које је могуће извршити електронски. Неке од понуђених услуга садрже оригинални образац, што је посебно назначено. Највећи број услуга односи се на остваривање различитих захтева грађана, односно привредних субјеката. Примера ради, то су захтев за издавање уверења о способности за склапање брака, захтев за

[117] То су области финансија и јавних прихода, урбанизам и грађевински послови, послови легализације објеката, комунални и стамбени послови, енергетика, имовински и правни послови, саобраћај, заштита животне средине, привреда, култура, образовање и дечија заштита, спорт и омладина, здравство, социјална заштита, инспекцијски надзор, лична стања грађана, комунална полиција, јавни превоз.

упис промене података у јединствени бирачки списак, захтев за издавање електронског сертификата за територију града Београда, захтев за продужење регистрације возила на овлашћеним техничким прегледима, захтев за издавање пореског уверења физичком лицу, захтев за добијање информације о локацији, итд.

Осим електронског подношења захтева и приступа обрасцима, коришћењем овог портала могуће је доћи и до посебних дигиталних портала које воде поједини органи управе. То су, примера ради, еКатастар и геопортал „геоСрбија“. Такође, могуће је приступити појединим јавним информацијама као што су јавни конкурси за попуњавање радних места, јавни позиви за финансирање друштвених програма и јавни позиви за подношење пројеката које објављују органи јавне управе. Значајно је поменути да је преко овог портала могуће заказати термине за добијање личних и других докумената које издају органи јавне управе (издавање личних карата, издавање квалификованог сертификата за електронски потпис, итд.).

Важан сегмент портала еУправе односи се на партиципацију грађана у друштвеном и државном животу. То значи да је грађанима омогућено да електронским путем достављају своје коментаре, сугестије и податке у вези са јавним расправа о прописима. Као што је речено, дигитална партиципација грађана данас представља основну потребу сваког демократског друштва. Електронска управа пружањем грађанима могућности да учествују у дискусијама о нацртима закона и других општих аката, остварује начело транспарентности, али и јача демократске вредности.

Према доступним статистичким подацима, број корисника електронских услуга, који се констатује на основу креираних налога, износи преко 590.000 активних корисника. Број услуга непрестано расте, па је тако на порталу доступно 710 услуга различитих органа јавне управе. У протеклом периоду, најчешће коришћене услуге су биле замене папирних здравствених књижица за нове електронске, као и прибављање извода из матичних књига рођених.[118]

[118] Портал електронске управе Републике Србије, 350.000 нових корисника и 160 нових електронских услуга на националном Порталу еУправа у 2016. години, *https://www.euprava.gov.rs/vesti/247/350-000-160-2016.html?alphabet=lat* , 14. септембар 2018.

Према својој правној природи, Портал еУправе можемо означити као основни информациони систем преко кога се остварују најзначајније услуге електронске јавне управе у Србији. Шта више, можемо рећи да овај портал представља „јединствено дигитално управно место“.

Поред овог портала, постоји још неколико посебних пројеката информационих система у појединим областима деловања јавне управе. Они су неопходни због претежности интереса који треба да се задовољи у тој области, али и ради побољшања услуга које пружају управни органи.

3.3.2. Пројекат „Бебо добро дошла на свет“

Један од значајнијих пројеката електронске јавне управе у Србији јесте пројекат „Бебо добро дошла на свет“ (колоквијално, овај пројекат се назива „е беба“) који имплементирају Министарство државне управе и локалне самоуправе, Министарство здравља и Министарство унутрашњих послова у области здравства и породичних односа. Пројекат је усмерен ка изградњи информационо-комуникационог система који олакшава управне процедуре у вези са пријављивањем ново рођене деце, њихових имена, пребивалишта и других административних питања у вези са рођења детета.

Уместо прикупљања документације у папирном облику родитељи могу већ у породилишту да дају пристанак за електронску пријаву рођења детета, што се врши преко заједничког информационог система. Пријава садржи лично име детета, адресу његовог пребивалишта и пријаву на здравствено осигурање. Електронским путем, на интернет адресу или поруком на мобилни телефон, родитељи добијају повратну информацију након успешног окончања предмета.[119] Пројекат је у развоју са тенденцијом ширења услуга и на друга питања у вези са родитељским правом.

Законом о финансијској подршци породици са децом[120] предвиђен је информациони систем за исплате корисницима у вези са дотацијама везаним за

[119] Пројекат „Бебо добродошла на свет“, *http://gakfront.org/A3d2HmiN/assets/files/OBAVESTENJA/Prezentacija_bebo_dobrodosla.pdf*, 14. септембар 2018.
[120] Закон о финансијској подршци породици са децом, *Службени гласник* РС, бр. 113/2017 и 50/2018.

родитељско право. У овај систем, по службеној дужности, уносе се подаци из захтева за остваривање права, прибављених доказа, решења донетих по таквим захтевима и подаци из других докумената релевантних за питања исплата у вези са родитељским правом.[121]

Бенефити коришћења оваквог информационог система нису мале. Иако не треба занемарити материјалну уштеду у виду умножавања папирне документације која више није потребна, акценат је стављен на олакшавање приступа услугама од стране родитеља, чиме се истовремено олакшава вођење посебних управних поступака. Велики број родитеља је прихватио могућност електронског коришћења ових услуга. Чак 90 % родитеља од укупног броја ново рођених беба (родитељу 95.524 бебе) се определило за коришћење електронских услуга овог пројекта.[122] То сведочи о значају и препознавању услуга електронске јавне управе у овој материји.

3.3.3. Информациони систем Републичког геодетског завода

Дигитализација услуга Републичког геодетског завода (у даљем тексту: Геодетски завод) представља још један пројекат путем кога се остварује електронска јавна управа у Србији. Овај пројекат тиче се стицања права својине на непокретностима, промета непокретности и другим питањима у погледу остваривања права и обавеза у вези са непокретностима, где значајну улогу имају органи управе, будући да се уписом у књиге стиче и престаје право својине, врше забележбе спорова, итд. О значају ове службе сведочи статистика, према којој је у 2017. години Геодетском заводу поднесено 2.026.165 захтева грађана у вези са различитим правима, обавезама и интересима у вези са непокретностима.[123]

Пројекат остварује Геодетски завод, као посебна управна организација која обавља управне и стручне послове државног премера, катастра непокретности и

[121] Чл. 46, ст. 2, Закона о финансијској подршци породици са децом.

[122] Подаци су наведени према: РТС, Систем „Бебо добро дошла на свет“ усклађен са изменама закона, *http://www.rts.rs/page/stories/sr/story/125/drustvo/3186661/bebo-dobrodosla-na-svet-uskladjeno-za-izmenama-zakona.html* , 14. септембар 2018.

[123] Статистика је доступна на сајту Републичког геодетског завода. Доступно на: *http://www.rgz.gov.rs/*, 17. септембар 2018.

управљања гео-просторним подацима на националном нивоу.[124] Основни циљ пројекта јесте да се дигитализују услуге које пружа Геодетски завод, што ће побољшати и убрзати поступке у вези са пословима катастра. На тај начин остварују се основна начела која Геодетски завод тежи да оствари у обављању својих активности и пружању услуга грађанима.

Дигитализација геодетско-катастарског система представља и својеврсно остваривање појединих начела Закона о државном премеру и катастру која се односи на издавање докумената у електронском облику и пружање услуга електронског пословног промета.[125] Нека од тих начела су: усклађеност са Дигиталном агендом Владе која тежи да оствари доступност услуга корисницима путем јединственог виртуелног шалтера, ажурност (редовно ажурирање података и подизање свести корисницима о начину ажурирања), рационалност процедура и поступака, ефикасност, доступност јавних података применом концепта отворених података, транспарентност, итд.[126]

Основни циљеви пројекта остварују се електронским приступом дигитализованим услугама и базама података које води Геодетски завод. Постоји неколико одвојених сегмената електронских услуга завода. *еЗаказивање* представља један од сегмената који омогућава електронски заказивање за предају захтева на шалтеру. У оквиру ове услуге корисници апликације могу одабрати место, датум и термин предаје захтева.[127] Осим тога, могуће је електронским путем заказати састанак са службеником катастра и електронски проверити статус предмета, уношењем броја предмета и надлежне службе у апликацију.

У оквиру сегмента *еКатастар* могуће је извршити увид у стање катастра непокретности, као и електронско подношење захтева. Да би остварили електронски увид у базе података, корисници се морају регистровати. Регистровани корисници могу приступити бази података која представља централну базу података непокретности коју одржавају службе Геодетског завода.

[124] Републички геодетски завод, Стратегија развоја Републичког геодетског завода 2020, Београд, 2017, 4.
[125] Чл. 158, Закона о државном премеру и катастру.
[126] Републички геодетски завод (2017), 6.
[127] Ипак, ова електронска услуга је на зачетку свог развоја. За потпуно остваривање принципа електронске управе неопходно је потпуно дигитализовати услуге и омогућити електронски начин предаје захтева за све услуге и за све јединице Завода.

Доступни подаци су класификовани по катастарским општинама. Друга опција еКатастра је електронско подношење захтева. Услуге Геодетског завода за које се може поднети електронски захтев су: издавање копије плана непокретности, издавање копије вода, издавање листа непокретности, издавање листа вода, издавање уверења о називу улице и кућном броју и издавање уверења о поседовању непокретности на нивоу општине.[128]

Национална инфраструктура геопросторних података представља још једну дигиталну услугу коју нуди Геодетски завод. Инфраструктура геопросторних података представља информациони систем отворених података који омогућавају корисницима да идентификују и приступе просторним (географским) информацијама добијеним из различитих извора, од локалног, преко националног до глобалног нивоа.[129]

Систем омогућава и олакшава приступ различитим географским подацима, који се на овај начин чине доступни грађанима и привредним субјектима. Они их даље могу користити у различите приватне и јавне сврхе, као што су одрживи развој, одрживо управљање ресурсима, итд. У вези са електронским услугама, омогућено је и подношење примедби на рад служби Геодетског завода. На овај начин, корисницима услуга Геодетског завода омогућено је сигурно и лако подношење примедби чиме се остварује одговорност у раду јавне управе.

3.3.4. Интегрисани здравствени информациони систем Републике Србије

Јавно здравље представља област друштвеног живота у којој је улога органа управе од изузетног значаја. Велики број информација и личних података који се свакодневно користи за решавање здравствених питања грађана захтевају централизовано вођење и брзу размену података између здравствених радника и здравствених организација. Због тога, електронизација рада органа управе у овом сектору заузима важно место у целокупном процесу дигитализације јавне управе.

Ради дигитализације сектора здравства створен је интегрисани здравствени информациони систем који се назива „*Мој доктор*“. „Интегрисани здравствени

[128] Увид у списак услуга Завода које се могу захтевати електронским путем извршен је 17.09.2018. год.

[129] Систем Националне инфраструктуре геопросторних података доступан је на: *http://www.geosrbija.rs/*, 17. септембар 2018.

информациони систем Републике Србије представља централни електронски систем у коме се чувају и обрађују сви медицински и здравствени подаци пацијената, подаци здравствених радника и сарадника, подаци здравствених установа, здравствене интервенције и услуге у здравственим установама, подаци електронских упута и електронских рецепта, подаци о заказивању за специјалистичке прегледе, дијагностичке процедуре и хируршке интервенције“.[130] Стварање оваквог система утиче на побољшање положаја пацијената, али уједно олакшава рад запослених који могу свој посао брже и једноставније обавити. Информациони систем је конструисан тако да омогућава олакшан приступ, прецизан унос и правовремену измену података који се чувају у централизованој бази података.

Грађани могу приступити електронским листама чекања, подацима о слободним терминима њиховог лекара или апарата који користе у лечењу, дигиталној мапи пута до своје здравствене установе или лекара, итд. Са друге стране, сваки здравствени радник (лекар, медицински брат и сестра, директор установе и др.) поседује јединствени електронски кориснички налог преко кога учествује у информационом систему. Ова лица могу приступити само одређеним подацима који су неопходни за обављање њиховог посла, што омогућава одговорност и повећава ниво заштите личних података.

Грађани остварују приступ информационом систему путем пријаве за коју је потребно унети корисничко име и електронску шифру. Грађани се могу обратити здравственим установама, исказати незадовољство или поставити питање администратору система електронским путем или телефонским позивом. На интернет презентацији могуће је приступити опису процедуре за заказивање, упућивање, креирање и реализацију рецепта на информационом систему.

[130] Интегрисани здравствени информациони систем Републике Србије, Министарство здравља, *https://www.mojdoktor.gov.rs/about*, 17. децембар 2018.

3.3.5. Портал отворених података

Портал отворених података представља значајан аспект електронске јавне управе будући да се знања, информације и подаци органа управе дигитализују и отварају јавности на увид. Отворени подаци представљају знање похрањено у различитим документима органа управе који су отворени за сва заинтересована лица која им могу слободно приступити и даље их користити.

Да би један податак представљао отворени податак, он мора да буде слободно доступан, приступачан, машински читљив и доступан у отвореним форматима.[131] Слободан приступ значи да се објављени подаци могу неограничени број пута умножавати, даље размењивати и усклађивати према потребама лица које их користи. Приступачност означава својство података да им се може приступити без остваривања посебних услова и подношењем захтева, већ се може до њих доћи непосредно путем информационо-комуникационих система, односно путем интернета. Машинска читљивост значи да се подаци могу обрађивати и користити коришћењем рачунарских програма. Доступност у отворених форматима подразумева да је формат у коме се налази податак доступан коришћењем рачунара и Интернета, без додатних услова.

Национални портал отворених података суштински представља информационо чвориште на коме се може приступити отвореним подацима објављеним од стране органа јавне управе Србије. У тренутку истраживања, Портал садржи преко 100 база различитих података. У базама отворених података посебно се истиче Градска управа града Шапца са 14, затим Повереник за информације од јавног значаја и заштиту података о личности 13, Агенција за лекове и медицинска средства Србије (11), Градска управа града Београда (7). Базе отворених података су сачинили и објавили и други органи јавне управе, као што су министарства (Министарство просвете, науке и технолошког развоја, Министарство правде, итд.), агенције (Регулаторна агенција за електронске комуникације и поштанске услуге, Агенција за заштиту животне средине, итд.), Институт Батут, заводи, канцеларије, итд.

[131] Портал отворених података, Отворени подаци, *https://data.gov.rs/sr/discover/*, 17. септембар 2018.

Портал отворених података представља облик остваривања електронске јавне управе кроз објављивање информација које су потребне грађанима за обављање различитих активности. Овим порталом остварује се значајнија веза између грађана и управе, будући да органи јавне управе „деле знање“ са грађинима, чиме остварују функцију јавне службе која служи свеопштем напретку друштва.

4. НОВЕ ТЕНДЕНЦИЈЕ У РАЗВОЈУ ЕЛЕКТРОНСКЕ ЈАВНЕ УПРАВЕ

Модерни свет утемељен је на размени информација и њиховој употреби ради задовољења различитих потреба и интереса. Основно средство размене информација у савременом свету јесу информационе технологије и интернет. Због великих могућности и значајне улоге, оне представљају основни мотор развоја и напретка друштва. Ипак, оне саме по себи немају вредност већ једино у односу са човеком, као интелигентним бићем које их употребљава за остварење своји жеља и циљева. Ипак, брз развој науке и технике доводи до тога да информациони системи могу на неким пословима чак и заменити човека.

Побољшањем рачунарских програма развијају се могућности и потенцијали информационо-комуникационих технологија. Нови рачунарски системи омогућавају замену човека у физичким пословима, али и у оним пословима које захтевају комплексне мисаоне радње. Човек је симулирајући сопствени начин размишљања, а користећи се напретком технологије, створио програме који могу да управљају возилима и авионима, да играју шах и рачунарске игре, да предвиђају земљотресе и поплаве, итд. У многима од ових делатности, рачунарски системи превазишли су интелект и могућности човека.

4.1. Вештачка интелигенција као део информационих технологија у јавној управи

Вештачка интелигенција представља посебан облик интелигенције, односно способност информационих система и рачунара да сами изводе закључке и решења на бази информација и предвиђених структура извођења закључка. „Вештачка интелигенција бави се, превасходно, проблемима у којима се јавља комбинаторна експлозија, проблемима чије решавање захтева разматрање

огромног броја могућности. Решавање таквих проблема обично се своди на неку врсту претраге, систематичног поступка обраде великог броја могућности".[132] Као таква, вештачка интелигенција омогућава аутоматизацију и упрошћавање задатака које човек мора „физичким путем" сам да обавља.

Употреба вештачке интелигенције могућа је у скоро свим областима друштвеног живота које имају потребу за прецизном селекцијом великог броја информација и података, као и калкулацију различитих фактора у доношењу одређене одлуке. Отуда је и даље актуелан став Џона Несбита (*John Nesbit*), од пре више од 30 година, који наводи: „Јасно је да са средствима којима данас располажемо не можемо изаћи на крај са толиким мноштвом информација. Неконтролисане и неорганизоване информације престају бити извор богатства савременог друштва. Напротив, постају нам непријатељи…информатичка технологија уноси ред у хаос информацијског загађења и осмишљава податке који би иначе били неупотребљиви."[133]

Одређени појавни облици вештачке интелигенције постоје и примењују се у свакодневном животу. Наравно, вештачка интелигенција се превасходно користи у сектору који се бави технологијама и технолошким напретком. Тако је *Google* купио компанију *Deep Mind* како би употребио њихово знање из машинског учења и вештачке интелигенције за оптимизовање својих рачунарских система. Цена ове трансакције износила је чак 500 милиона америчких долара.[134]

Осим технолошког сектора, банкарство је још једна друштвена област у којој се вештачка интелигенција користи у великој мери. Према испитивањима, чак 86% водећих компанија у банкарству користи се услугама вештачке интелигенције. Примера ради, *Swiss Bank UBS* се одлучила за коришћењем робота у трговини на берзама, како би се повећала ефикасност брокера. *Barclays* банка припрема софтвер који омогућава да корисници сазнају више о битним трансакцијама, као и пружање помоћи приликом доношења одлука корисника о

[132] Предраг Јаничић, Младен Николић, *Вештачка интелигенција*, електронско издање 2016, 13, *file:///C:/Users/Win/Downloads/Vestacka%20Inteligencija,%20prof.%20Predrag%20Janicic.pdf*, 18. септембар 2018.
[133] John Naisbitt, *Megatrendovi- Deset novih smejrova razvoja koji mijenjaju naš život*, Globus, Zagreb 1985, 131.
[134] Branislav Bubanja, „Google koristi AI za kontrolu hlađenja u data centrima", *PC Press*, (online) 2018, *https://pcpress.rs/google-koristi-ai-za-kontrolu-hladenja-u-data-centrima/*, 18. септембар 2018.

позајмицама и кредитима. Дакле, банке улажу своја средства и у инвестирање технологија које помажу у сектору банкарства.[135]

Зачеци вештачке интелигенције појављују се и у сектору здравства, образовања, пољопривреде и водопривреде, транспорта, спорта, и многим другим. Као „последња реч технологије“, вештачка интелигенција превасходно налази употребу у приватном сектору. Један од разлога за такво стање ствари је висока цена коју треба платити за ове технолошки напредне производе, што се може једино покрити ценом услуга коју приватна лица и привредни субјекту могу остварити продајом својих услуга и производа. Због тога, вештачка интелигенција теже „улази“ у јавни сектор.

Ипак, области друштвеног живота у којима долази до примене вештачке интелигенције у највећем броју случајева поклапају се са областима у којима органи управе имају одређену улогу. Због тога, вештачка интелигенција представља један од вероватних праваца развоја електронске управе. У зависности од послова и области у којој се примењује, вештачка интелигенција може вршити различите делатности и успешно заменити људски фактор у низу послова који захтевају анализу великог броја информација и извођење закључка. Увођење вештачке интелигенције у јавни сектор подразумева узајамну сарадњу великог броја људи, јавног и приватног сектора, као и усклађивање правних прописа. „Вештачка интелигенција у јавној управи подразумева пројектовање, изградњу, употребу и еволуцију когнитивног рачунарства и машинског учења у циљу побољшања рада јавних агенција. Како би се омогућило успешно коришћење вештачке интелигенције у јавној управи, лидери морају да осмисле и имплементирају политику и управљање које промовише стручне раднике које сарађују са академским и приватним сектором, оквирима за управљање ризицима, сигурносним системом и модерним технологијама“.[136]

Као најбољи показатељ тежње држава за увођењем и коришћењем вештачке интелигенције у јавној управи налазимо у Уједињеним Арапским Емиратима. Приликом реконструкције Владе, 2017. године, основано је

[135] Darko Topalović, „Kako veštačka inteligencija transformiše bankarski sektor?“, *PC Press*, (online) 2018, *https://pcpress.rs/kako-vestacka-inteligencija-transformise-bankarski-sektor/*, 18. септембар 2018.
[136] Kevin Desouza, *Delivering Artificial Intelligence in Government: Challenges and Opportunities*, IBM Center for The Business of Government, Washington 2018, 5.

Министарство вештачке интелигенције. Ово је прво министарство вештачке интелигенције у свету. Омар бин Султан Ал Олама (*Omar bin Sultan Al Olama*) постављен је за првог министра у области вештачке интелигенције. Надлежности министарства односе се на повећање ефикасности и способности Владе помоћу развијања и улагање у најновије технологије и средства вештачке интелигенције. Развијање и улагање ових технологија има за циљ да се уложе у различите области друштвеног живота чији развој подстиче Влада.

Министарство је промовисало „Стратегију вештачке интелигенције 2031“, који има за циљ развијање паметне електронске јавне управе. Основне области у којима треба применити принципе вештачке интелигенцију су образовање (смањење трошкова и повећање мотивисаности за учењем), транспорта (смањење незгода и операционалних трошкова), енергија (олакшање управљањем и паметне потрошње), свемира (прецизна тестирања и смањење процента грешака), технологија (повећање процента производње и ефективности комуникације).

Предвиђања су да ће увођењем вештачке интелигенције у ове области донети велике уштеде, чак до 50% и то смањењем 250 милиона папирних трансакција у вези са радом Владе и јавне управе на државном нивоу, 190 милиона часова утрошених на те трансакције и преко 1000 милиона километара који се данас прелазе ради финализирања трансакција.[137] Уз све претходно речено, треба имати у виду да Уједињени Арапски Емирати представљају релативно мању државу која је финансијски стабилна, што су је велика предност за увођење вештачке интелигенције у јавну управу. То су важни социолошки фактори који утичу на развој електронизације јавне управе. Очекивани развој технологије у наредним годинама и деценијама треба да олакшава примену система вештачке интелигенције у јавним управама широм света.

Будући да у Србији електронска управа представља релативно нову појаву, вештачка интелигенција није још предвиђена као следећа степеница развоја. Наравно, посматрајући досадашњи развој науке и технологије вештачка интелигенција врло брзо може да постане део јавне управе у Србији, за шта су потребни већа улагања у технолошки развој и развој *startup-a*. До тада, важно је и

[137] UAE, *UAE Artificial Inteligence Strategy 2031*, online 2018, *http://www.uaeai.ae/en/*, 19. септембар 2018.

поставити одговарајуће правне темеље система заштите различитих области у вези са ризицима које вештачка интелигенција може донети у односу на грађане и друштво, па је у том смислу важно уредити питање аутоматизованог доношења одлука.

Употреба вештачке интелигенције у јавној управи отвара многа питања у вези са правима и интересима грађана. У првом реду стоји приватност грађана. Како би функционисала и успешно обављала своје задатке, вештачка интелигенција мора да се користи информацијама и подацима које јој служе као средство обављања послова. То се посебно односи на јавну управу где би вештачка интелигенција морала да користи личне податке грађана у свом раду.

На тај начин, отвара се питање заштите података и могућности очувања приватности у ери вештачке интелигенције. Како се наводи: „за разлику од физичке имовине, подаци су другачији. Они се могу умножавати неограничени број пута. Следећа деценија ће поставити питања, не само о томе ко поседује податке и која права имају појединци у вези са њима, већ и како ће изгледати наша веза са подацима у повезаном свету“.[138]

Такође, треба указати и на потенцијални ризик самосталног (аутономног) развијања вештачке интелигенције које може да доведе до тога да она самостално одлучује о својим потребама, развоју и употреби. У том случају, она би се од корисног средства, које унапређује делотворност, ефикасност и економичност делатности јавне управе, могла да постане опасно оружје које угрожава грађане. Зато је од великог значаја да вештачка интелигенција остане средство напретка, а не циљ коме треба тежити.

[138] Pallavi Agrawal, „Public Administration Challenges in the World of AI and Bots“, *Public Administration Review*, vol. 78, issue 6, (ed. Paul Battaglio), American Society for Public Administration, Washington 2018, 920.

4.2. Експертни системи у јавној управи

Још један од облика напредне употребе рачунара и информационо-комуникационих технологија јесу експертни системи. Код експертних система реч је о рачунарским програмима који замењују рад стручњака у одређеној области друштвеног живота. Стручњак је особа која поседује посебна стручна и техничка знања у појединој области, па је за употребу таквог система неопходан исти или виши ниво знања од стручњака. Такви системи се превасходно користе у приватном сектору као замена за стручњаке који својим саветима утичу на доношење пословних одлука и усмеравања обавља послова у одређеном смеру, ради повећања ефикасности и економичности.

Дакле, под експертским системима подразумева се „успостављање, унутар рачунарског дела, вештине неког експерта који се базира на знању, у таквом облику да систем може да понуди интелигентан савет или да преузме интелигентну одлуку о функцији која се обрађује. Експертни систем поседује и карактеристику да на захтев верификује своју линију резоновања, тако да директно обавештава корисника који поставља питање“.[139] Ови системи имају могућност да замене стручњаке у појединим друштвеним областима. Таква тенденција представља израз тежње за убрзањем послова и јефтинијим начином доношења стручних одлука.

Покушаја примене експортних система има и у јавном сектору, међутим, њихово увођење се одвија изузетно споро и обазриво због потребе за даљим развојем технике и технологије, али и због потребе за поштовањем људских права. Корист од ових система у јавној управи може бити изузетно велика јер ови системи „разликују од традиционалних система решавања у коришћењу приступа решавању проблема на бази повезивања, претраге резултата, контролних задатака и метаподатака које замењују недостајуће податке“.[140]

---

[139] Alempije Veljović, Miroslav Radojčić, Jasmina Vesić, *Menadžment informacioni sistemi*, Tehnički fakultet u Čačku, Čačak 2008, 90.

[140] Joseph Weintraub, „Expert Systems in Government Administration“, *AI Magayine*, Vol. 10, online 1989, *file:///C:/Users/Win/Downloads/730-Article%20Text-727-1-10-20080129.pdf*, 19. децембар 2018.

Један од примера увођења експертних система у јавну управу је *EDGE expert system*[141], који је уведен у Аустралији. Овај експертни систем сачињен је ради пружања помоћи у доношењу одлука приликом одлучивања о потенцијалном давању финансијске подршке аустралијске јавне управе грађанима у вези са породичним стварима. *EDGE* је створен да олакша приступ бројној регулативи и пракси у вези са породичним стварима чиме се долази до ефикасности у управном одлучивању. Експертни систем тежи да анализира унете информације, укаже на правила која треба применити (сузи избор од многобројних) и симулира одлучивање о могућем признавању права на основу унетих података.

На овај начин, руководеће лице (запослени у јавној управи) не мора детаљно да пролази кроз масивне законске текстове, опште правне акте и управну праксу. Неки од циљева увођења овог система су стварање предвидљивости управног одлучивања, организациона ефикасност и побољшање система пружања информација. Будући да функционише по устаљеним алгоритамским налозима који су претходно унети, експертни систем нема могућност дискреционог одлучивања приликом анализе информација, већ свој рад заснива на претходно унетим параметрима и статистичким подацима. Организациона ефикасност се осликава у уштедама у износу од више десетина милиона долара годишње.[142] Целокупан пројекат увођења система коштао је 64 милиона аустралијских долара.[143]

Ипак, било је и бројних проблема у пракси. Пре свега, јавио се проблем техничке природе. Различити програмски језици на којима је функционисао овај експертни систем, са једне стране, и базе података правних норми јавне управе, са друге стране, створили су застоје и пропусте у тражењу информација. Друго, одлучивање о добијању права из породичних ствари омогућавало је и одређени степен дискреционе оцене управних органа, што није било могуће применити у рачунарском систему. Треће, атипични случајеви који су се појављивали захтевали су дубље улажење у материју, те нису могли да буду решени

[141] За више информација о EDGE expert system-у, вид. *https://www.anao.gov.au/work/performance-audit/edge-project,* 10. децембар 2018.
[142] Вид.: P. Henman (2010), 55.
[143] *Ibid*., 51.

једноставним указивањем на релевантне правне норме. Због наведених проблема, Аустралија је ипак обуставила пројекат *EDGE expert system*, само пар година након његовог развијања, 2003. год. Такође, и поред неуспеха овог пројекта, Аустралијска Влада је одржала поверење у увођење експертских система у јавну управу, што је и озваничила документом из 2007. године.[144] Покушаји увођења експертни система, било је и на европском подручју. Тако је у Холандији испробан експертни систем у вези са питањима из социјалног рада. Овај систем је генерално функционисао, али је и пружао нетачне резултате.[145]

И у области експертних система, као и у сфери вештачке интелигенције, мора се водити рачуна о изазовима законитости и правилности рада органа управе. Употреба ових система сусреће се са бројним ризицима, што може довести до настанка штете и повреде људских права и интереса. Како би се спречио такав сценарио неопходно је, са правне тачке гледишта, уредити најважније сегменте у којима долази до контакта јавне управе, информационих технологија и људских права. То значи да је важно прописати правила понашања у електронској јавној управи, установити систем информационе безбедности и установити адекватне механизме заштите личних података у односу на ове системе. Тако се стварају предуслови за имплементацију нових технологија у јавну управу, са смањеним ризицима по приватност и друга права грађана. Неопходно је развијати свест о улози личних података у савременом свету, јер једино адекватна правна регулатива може представљати брану опасностима које неминовно доносе нове технологије.

[144] Department of Finance and Administration, Australian Government, *Automated Assistance in Administrative Decision-Making Better Practice Guide*, Australian Government Information Management Office, Canbera 2007.

[145] Hugo de Bruin, Henry Prakken, Jorgen Svensson, „The Use of Legal Knowledge-Based Systems in Public Administration: What Can ¨ Go Wrong?“, *Legal Knowledge and Information Systems*, (eds. T.J.M. Bench-Capon, A. Daskalopulu and R.G.F. Winkels), Jurix, The Fifteenth Annual Conference. Amsterdam: IOS Press, Amsterdam 2002, 123.

***

На овај начин заокружили смо излагање о електронској јавној управи, њеној улози, вредностима, могућностима и тенденцијама у развоју. У овом делу истраживања установили смо кључне тачке које треба истражити и уредити правним нормама.

У ери информационо-комуникационих технологија и интернета основно средство у раду електронске јавне управе јесу лични подаци. Без личних података, не може се замислити рад електронске управе. Међутим, лични подаци представљају део личности грађана и самим тим представљају основни супстрат приватности који захтева јаку заштиту. Због тога, у даљем истраживању усмерићемо пажњу на основна питања у вези са личним подацима, како бисмо на могли да анализирамо механизме правне заштите личних података у електронској јавној управи.

III ПОДАЦИ О ЛИЧНОСТИ

1. ОДРЕЂЕЊЕ ПОЈМА ПОДАТКА

Осим појма електронске јавне управе, за разумевање заштите података у електронској јавној управи, неопходно је претходно обрадити појам и улогу података о личности у савременом друштву и модерној држави. Разјашњење улоге и значаја личних података помоћи ће разумевању начина и механизама њихове заштите у електронској јавној управи. Иако је истраживање усмерено на правна питања података о личности, темељан приступ подразумева кратак социолошки и психилошки осврт, јер се једино свеобухватном анализом може одредити природа личних података и установити друштвени чиниоци који диктирају потребу за њиховом правном заштитом.

1.1. Уводна разматрања о човековој личности

Упрошћено речено, лични подаци представљају опредмећени део одређеног дела човекове личности. Због тога, како би се разумео појам података о личности и улога коју они имају у друштвеном и државном животу, неопходно је укратко учинити заокрет ка појму човекове личности, будући да од овог појма зависи и правни појам података о личности. Истраживање ће посветити пажњу одређењу човекове личности у кратким цртама, без детаљнијег улажења у ову проблематику.

Човекова личност[146] представља комплексну појаву, која се изучава у оквирима различитих научних дисциплина. Међу њима, због великог броја теорија и ставова о природи ове појаве, истиче се психологија. Психилошка становишта у вези са човековом личношћу користе се и другим друштвеним научним дисциплинама. Може се рећи да „појам личности спада у најфундаменталније и највише употребљаване категорије у психологији, па ипак је узрок многим супротним гледиштима у оквиру те научне дисциплине. Настојећи да дође до дефиниције личности, Алпорт је показао да постоји око 80 разних дефиниција личности, но све се оне могу свести на два у основу супротна

[146] Енглески термин за личност (*personality*) потиче од латинског термина persona који означава маске глумаца у римским позориштима које су приказивале карактер глумаца.

схватања. По једном, бихевиористичком, личност је, пре свега понашање које човек показује у односу према средини и људима око себе…На другој страни се налазе школе дубинске психологије које сматрају да је личност оно што условљава и регулише понашање, што се налази „иза“ или „испод“ спољашњег понашања: то су разни мотиви, интереси, ставови, итд. То је жеља да се испод спољних, површинских слојева и реакција човека уочи тенденција за захватањем оних „слојева“ у људској свести или подсвести које представљају најдубљу језгру човекових личности.“[147]

Осим психолога, појам личности покушали су да одреде и социолози. Социолошке теорије личности иду за тим да укажу на значај узајамног деловања поједине личности на друштво, као и деловање друштва на човекову личност. Личност се у социологији обично посматра у контексту функционисања друштвене заједнице. „Личност као јединствена организација особина формира се узајамним деловањем појединца и друштвене средине. Битна својства личности су њена стваралачка способност (која се испољава у способности да мења спољашњи свет и унутрашњом потребом за стваралаштвом), социјалитет (укорењеност у друштвеној заједници и друштвени карактер људске природе), субјективитет (израз својеврсне индивидуалности) и интегритет (у којем се изражава кохерентна организација са свим психо-социјалним карактеристика и омогућава релативно јединство у понашању и ставовима у различитим ситуацијама)…“[148].

Данас постоје бројна одређења човекове личности „које на разне и разноврсне начине и из различитих углова и сазнајних нивоа покушавају да одгонетну тајну људске самобитности, али без обзира на који део личности се нека теорија односи, да ли се углавном, претежно и суштински усмерава на социјални, духовни, телесни, историјски, психички живот човека или углавном вредности, знања и врлине личности, или пак идеје и мудрости које заступа личност и њену улогу у светско-историјским догађајима, мора се знати да личности изнад свега подразумева вредног, врсног човека, човека знања, врлина и

[147] Mladen Zvonarević, *Socijalna psihologija*, Školska knjiga, Zagreb 1985, 135.
[148] Данило Марковић, *Општа социологија*, Савремена администрација, Београд 1993, 187.

великих достигнућа и да је ту реч о таквом и ретком човеку који има лични значај и огромно значење у својој заједници“.[149]

На основну изложеног увиђамо значај човекове личности за самог човека. Можемо закључити да човекова личност представља друштвену појаву која својом ширином и важношћу утиче на различите научне дисциплине. Централно место појединца у друштву додатно наглашава потребу да се природа и личност човека проучи, анализира и да се на основу тих специфичности боље разумеју друштвена дешавања. Управо тамо где има људи и њихових дела, јавља се потреба и за правним уређењем.

1.2. Правне норме и човекова личност

Као важна друштвена категорија, човекова личност представља предмет интересовања правне науке и праксе. Сваки правни систем тежи да правним нормама систематски уреди и усмери понашања људи како би се обезбедила правна сигурност и предвидљивост у друштву. Како су понашања људи суштински везана за човекову личност, она се јавља као непосредни и посредни предмет норми различитих грана права.

Наравно, правне норме не уређују природу човекове личности, будући да је то природна појава на коју се не може и не сме утицати. Правни системи прихватају непоновљиву природу личности и теже да јој пруже заштиту у слободном развоју од свих недозвољених утицаја појединца и друштва. Због комплексне правне природе, човекова личност као предмет правне заштите налази се на граници између приватног и јавног права. Из перспективе јавног права, човекова личност се посматра у односу са државом и њеним органима. Тачније, човекова личност се штити у таквом односу, будући да држава и њени органи поседују монопол физичке силе који се не сме злоупотребљавати према „слабијој“ страни, односно грађанима. Нормама јавног права (управног, уставног и кривичног) штите се вредности које су од значаја за читаву друштвену заједницу, али и за појединце. То значи да држава на једнак начин гарантује свим људима

[149] Илија Кајтез, „Личност и живот друштвене заједнице“, *Infinitas,* Српско лекарско друштво, Београд 2012, 383-384.

различите механизме правне заштите пред државним органима, у случају настале повреде или штете у вези са личношћу човека.

Са друге стране, приватно правна заштита значи то да појединац може самостално захтевати заштиту пред државним органима у циљу заштите својих личних интереса. На тај начин, појединац преузима активну улогу у циљу заштите своје друштвене и правне позиције која може бити угрожена чињењем и нечињењем трећих лица. И код приватно правне заштите долази до активирања норми јавног права, тако што у тој заштити учествују државни органи са јавним овлашћењима, који штите и приватне и јавне интересе. Међутим, централно место у таквој заштити припада појединцу. Приватно правна заштита уређена је нормама грађанског права (облигационог, породичног, наследног, итд.).[150]

На значај човекове личности указује и чињеница да она своје место налази у уставима, као највишим правни актима држава. Такав је случај и са Србијом, где је Уставом зајамчено да сваки човек има право на слободан развој личности, ако тиме не угрожава права других.[151] Дакле, човекова личност представља (уставно) правну категорију. Она се доводи у везу са слободом, као основном вредношћу која је неопходна за развој и напредак. Како би се очувала посебност човекове личности, држава гарантује услове за њен слободан развој и унапређење, али до тачке у којој се не угрожава развој личности других појединаца. За развој личности човека важно је то да је људски живот неприкосновен и да је забрањено клонирање људских бића.[152] Забраном клонирања људских бића спречава се вештачко стварање, односно репродукција непоновљивог склопа човекове личности.

Гарантовање неповредивости психичког и физичког интегритета представља још један стуб који доприноси слободном развоју личности. Као један од правних елемената човекове личности, Устав Србије предвиђа и право на

[150] Упор. Ивана Симовић, Мирослав Лазић, „Грађанско правна заштита права личности“, *Зборник радова Правног факултета у Нишу*, бр. 68, (ур. Ирена Пејић), Ниш 2014, 272-273.
[151] У истом члану у коме се гарантује слободан развој личности, Устав обезбеђује и људско достојанство, као саставни елемент човека и његове личности. Као такво, оно је неприкосновено и сви су дужни да га поштују и штите. На овај начин људско достојанство ужива исти степен заштите као сам људски живот, који је неприкосновен. Међутим, упитна је обавеза „свих“ да штите људско достојанство, које је при том неповредиво, што може водити у различите логичке и правне недоследности. Вид. Чл. 23, Устава РС.
[152] Чл. 24, Устава РС.

правну личност. Правна личност представља појавни облик човекове личности у правним односима. Она се може разумети као јединство правне и пословне способности. Правна способност значи то да свако физичко и правно лице има способност да буде ималац права и обавеза у правном животу, док пословна способност представља могућност да се самостално одлучује о својима правима о и обавезама.[153]

Можемо закључити да се делови човекове личности штите различитим људским правима и институтима, па се ни сама човекова личност не може посматрати једнострано, већ једино у садејству са блиским правним институтима и правима.

Такав је случај и са подацима о личности, који представљају део човекове личности који је „ангажован“ у правном промету. Као појавни облик човекове личности различити подаци о личности свакодневно се употребљавају и размењују, означавајући и ближе одређујући субјекте и друге елементе правног односа. Због јаке везе са самом личности човека, повреда личних података уједно представља и повреду човекове личности. Како је за опстанак појединца и друштва неопходна заштита приватности и интегритета личности, значајно место у очувању човекове личности има заштита личних података. Због тога, неопходна је квалитетна заштита и темељено уређење начина поступања са личним подацима.

[153] Физичка лица постају имаоци правне способности самим рођењем, док је правна лица њу стичу посебним поступком признања правне личности односно правног субјективитета. Правна способност заједно са пословном и деликтном способношћу чине правни субјективитет једног лица. Раденка Цветић, „Правна способност и биомедицина – биомедицинска дискриминација“, *Зборник радова Правног факултета у Новом Саду*, 3/2011, (ур. Драгиша Дакић), Нови Сад 2011, 349-350.

2. О ПРАВНОЈ ПРИРОДИ ПОДАТАКА

2.1. Разлика између податка и информације

За разумевање система правне заштите личних података нужно је одредити правну природу личних података, односно самих података. У циљу одређења правне природе података о личности, неопходно је претходно терминолошки разграничити две сличне појаве које се неретко мешају у правном дискурсу. То су појам податка и појам информације. У свакодневном животу, али и у прописима, често долази до коришћења два појма за објашњење истих појава, иако они суштински представљају различите појаве.

Информација представља један од најактуелнијих појмова данашњице. Суштински, она представља крајњи резултат анализе података о неком предмету или појави, па у том смислу више повезаних података представља информацију. Овај појам употребљава се у свакодневном говору и у различитим околностима, па тако добијамо појмове попут информационог доба, информационог друштва, информационе револуције, информационе технологије, итд. Информације чине толико снажан утицај на савремено друштво да се модерне генерације називају информационим друштвом, а доба у коме живимо се означава као информационо доба.[154] Употреба појма информације заступљена је и у научном дискурсу, приликом вршења безбедносних провера, медијским извештајима, итд.

Са друге стране, појам податка се користи за означавање одређене карактеристике неког бића, предмета или појаве. Када добије контекстуално значење и практичну вредност податак постаје информација. Сам термин податак своју примену проналази превасходно у правном дискурсу и правничкој терминологији у вези са различитим правним институтима попут закључења уговора, судских и управних поступака, идентификовања одређеног лица од стране органа јавне власти и томе слично.

Посматрано из правне перспективе, између ова два појма постоји значајна разлика која повлачи за собом различито поступање и различите правне последице. Правничка терминологија познаје и појам податка и појам

[154] За више о појму информационог друштва вид. László Z. Karvalics, *Information Society – what is it exactly? (The meaning, history and conceptual framework of an expression*), Budapest 2007, 5-21.

информације. Да ова два појма нису синоними у управном праву Србије сведочи Закон о општем управном поступку, који у оквиру својих начела познаје и „начело приступа информацијама и заштите података“.[155] Дакле, у односу на органе управе, информација и податак представљају различите појаве. Закон о општем управном поступку у вези са информацијама наводи да су управни органи дужни да грађанима омогуће приступ информацијама (од јавног значаја или од значаја за конкретно лице). Са друге стране, исти закон у односу на податке наводи да тајни и лични подаци уживају заштиту у управном поступку. Међутим, иако је јасно да постоји разлика, Закон терминолошки не одређује ни појам информације ни појам података.

Што се тиче других позитивно-правних прописа, одређење појма податка можемо пронаћи у Закону о заштити података о личности. Податак о личности представља 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.[156] Из изложене дефиниције закључујемо да податак представља конкретизовану информацију. Тачније, да би један податак постао информација, он мора да носи у себи одређени садржај (значење) о поједином предмету или појави (у случају података о личности, податак се односи на одређену карактеристику физичког лица). На основу ове разлике можемо закључити да информација представља квалификован податак који је испуњен одређеним садржајем и контекстом.

Сличан приступ одређењу појма податка можемо пронаћи у Закону о тајности података, који одређује „податке од интереса за Републику Србију“. Подаци од интереса су сви они подаци којима располаже орган јавне власти, а који се односе на територијални интегритет, сувереност, заштиту уставног поретка, људских и мањинских права и слобода, националну и јавну безбедност,

[155] Чл. 15. Закона о општем управном поступку.
[156] Чл. 4., ст. 1, тач. 1, Закона о заштити података о личности (2018), *Службени гласник* РС, бр. 87/2018.

одбрану, унутрашње и спољне послове.[157] Као и у претходном случају, информација представља податак испуњен одређеним садржајем (у овом случају садржај се односи на питања од значаја за функционисање државе и друштва), која се даље преноси у физичком или електронском облику.

Нибле (*Niblett*) наводи да „информацију није лако дефинисати, обзиром да се овом изразу придају различита значења. Она се користи за означавање одређених операција у процесу управљања, за обавештења која су садржана у књигама, документима, чланцима, новинама, различитим евиденцијама и досијеима који се могу обрађивати електронским путем“.[158] Овај аутор такође стоји на становишту да информацију треба разликовати од појма податка. У том смислу наводи да се „податак односи на чињенице или појмове који могу бити формализовани и као такви подобни за комуникациону манипулацију, док информација нужно подразумева смисао, односно значење које се том податку признаје“.[159]

Осим података, и појам информације проналазимо и у позитивно-правним изворима. Појам информације налазимо у Закону о слободном приступу информацијама од јавног значаја. Овај закон дефинише информацију од јавног значаја као информацију којом располаже орган јавне власти, која је настала у раду или у вези са радом органа јавне власти, а садржана у одређеном документу и односи се на све оно о чему јавност има оправдан интерес да зна.[160] Дакле, информација представља одређено сазнање, односно запис о одређеној појави (податку) која је забележена, описана или ближе одређена у неком документу. Са техничке стране посматрано, информација представља систем знакова које носе одређено значење и преносе поруку са одређеним значењем.

На основу свега изложеног, можемо закључити да је у правничком дискурсу неопходно разликовати податак од информације. Податак представља појавни облик информације која се односи на одређено лице или предмет и која носи одређену поруку и значење.

---

[157] Чл. 3., ст. 1, тач. 2, Закона о тајности података, *Службени гласник* РС, бр. 104/2009.
[158] G.B. F. Niblett, *Digital Information and the Privacy Problem, Organization for Economic Co-operation and Development*, Paris, 1971, 9.
[159] *Ibid*.
[160] Чл. 2., ст. 1. Закона о слободном приступу информацијама од јавног значаја, *Службени гласник* РС, бр. 120/2004, 54/2007, 104/2009, 36/2010.

Једна информација увек носи податак, па без одређеног податка не постоји ни информација. Такође, за податак није важно на шта се односи, осим у случају податка у информацији који је повезан са конкретно одређеним лицем или предметом.

2.2. Правна класификација података

У свету права свакодневно се користи огроман број података у различите сврхе. Подаци представљају нераскидиви део правних односа, па се користе за идентификацију или распознавање лица или предмета, доношење одлука, предузимање мера, итд. Они представљају чињенице које су неопходне за остваривање права и интереса, иницирање правних послова и остваривање правних последица. Податке користе сви учесници у правном саобраћају када остварују права, штите интересе или извршавају обавезе према другим лицима. Како непрестано расте број правних односа који су регулисани правним нормама, тако је и број података који се користе у пракси у непрестаном порасту.

Наравно, немају сви подаци једнаку важност и исту улогу у правним односима. Поједини подаци уживају правну заштиту (матични број грађана), док други не уживају такву заштиту (подаци о седишту одређеног државног органа). Даље, могуће је извршити поделу података на оне који су доступни свима (отворени подаци) и оне податке којима има приступ само уско одређен круг лица (тајни подаци државних органа). Подаци се разликују и по томе да ли се односе на лица (подаци о држављанству), предмете (подаци о броју мотора аутомобила) или појаве (подаци о стању на путевима).

2.2.1. Класификација података према степену правне заштите

Подела података према степену правне заштите, фактички се своди на питање улоге поједине врсте података у правном систему. Огроман број података свакодневно се употребљава у правној пракси, међутим, само неки од њих уживају посебан статус који је гарантован општим актима. Тако, лични подаци грађана уживају управну и судску заштиту коју правни систем гарантује, обично уставом, као највишим општим правним актом, док се конкретне мере заштите остварују законским и подзаконским актима.

Са друге стране, поједини подаци, иако регулисани правни нормама, не уживају правну заштиту, из разлога што информација коју они носе не представља заштитни објект будући да је доступна свима или се не може ни на који начин повредити, па не заврђује правну заштиту. Такав је случај са великим бројем података. На пример, седиште и назив државног органа или правног лица представљају податке који су доступни свима и који се не могу повредити од стране трећих лица. Због тога, иако су уређени правним нормама, ови подаци не уживају правну заштиту пред органима јавне власти, на начин на који уживају лични подаци.

2.2.2. Подаци отворени за јавност и подаци затворени за јавност

Једна од правних подела података јесте на оне податке који су отворени и доступни јавности и оне податке којима може приступити само уско одређен и овлашћен круг лица, па су самим тим затворени за јавност.

У прву категорију спадају они подаци за које јавност има оправдан интерес да зна, па су доступни јавности путем јавних средстава комуникације. Овде убрајамо податке од јавног значаја и отворене податке. У одређеном броју случајева, закон омогућава грађанима да се упознају са подацима који носе информације од јавног интереса, односно од интереса за ширу друштвену заједницу. Тако, у Србији, Закон о слободном приступу информацијама од јавног значаја предвиђа посебан поступак у коме грађани могу да затраже информације (податке) од јавног значаја.[161] Информацијом од јавног значаја сматра се информација којом располаже орган јавне власти, настала у раду или у вези са радом органа јавне власти, садржана у одређеном документу, а односи се на све оно о чему јавност има оправдан интерес да зна, при чему није битан ни извор информације, нити носач на коме се налази информација.[162] Иако се ради о информацијама, могуће је да се оне јаве у облику податка од јавног интереса. Међутим, чак и у овим ситуацијама, податак од јавног интереса није отворен у потпуности, већ је доступан грађанима под одређеним, законом прописаним

[161] Чл. 15-29, Закона о слободном приступу информацијама од јавног значаја.
[162] Чл. 2, Закона о слободном приступу информацијама од јавног значаја.

условима. До њега се долази кроз посебни поступак, који се покреће захтевом за приступ, односно захтевом за достављање податка.

Отворени подаци представљају другу групу података који су доступни јавности. Они се по својој правној природи разликују од података који садрже информацију од јавног значаја. Наравно, оба концепта утемељена су у тежњи да се рад органа управе учини јавно доступним. Међутим, кључна разлика између ове две врсте података лежи у томе што се отворени подаци (након сазнавања) могу користити и у друге сврхе (комерцијалне или некомерцијалне)[163] у односу на оне због којих су првобитно прикупљени. Да би један податак представљао отворен податак, он мора испуњавати карактеристике отворености, читљивости и доступности. Такве особине не морају да испуњавају информације од јавног значаја.

У другу групу, затворених података, спадају подаци који су строго личне природе, па само лице о чијим подацима је реч или овлашћена лице имају право да приступе таквим подацима, да их користе и обрађују. Такође, овој групи припадају и подаци који су од значаја за друштвену заједницу и шире интересе, па су због тога проглашени за тајне. У ову групу података, која није доступна јавности, спада већина података о личности (личних података) и „државних" тајних података. Као што је већ речено, подаци о личности тичу се одређене карактеристике физичког лица, па јавност нема право да буде упозната са њима, осим уколико их њихов ималац не објави. „Државни" тајни подаци представљају податке од интереса за државу и друштво који су законом, другим прописом или одлуком надлежног органа одређени и означени одређеним степеном тајности.[164] Тајни подаци обично се односе на националну безбедност, јавну безбедност, односе са другим државама, системе, уређаје, пројекте и планове од значаја за државу, итд.[165]

[163] Đorđe Krivokapić *et al., Share@Work 2016: Monitoring digitalnih prava i sloboda u Srbiji,* Share fondacija, Beograd 2017, 104.
[164] Чл. 2, ст. 1, тач 2, Закона о тајности података.
[165] Вид. Чл. 8, Закона о тајности података. За више о тајним подацима у Републици Србији вид. Dejan Milenković, „Zašto je Srbiji potreban zakon o klasifikaciji tajnih podataka", *Zaštita podataka o ličnosti i poverljivi podaci- Pravni standardi*, Fond za otvoreno društvo, Beograd 2005, 107-116.

2.2.3. Подаци који се односе на личности и подаци који се односе на предмете

Једна од подела која можда има најзначајније последице у правној пракси јесте она која врши разликовање података који се односе на лица и података који се односе на предмете (ствари). Подаци који се односе на личности (лични подаци) тичу се физичких и правних лица и садрже знање о појединим посебном својству лица, по коме се оно разликује од других лица у правном систему. Они су последица чињенице да су физичка и правна лица носиоци правног субјективитета, па постоји потреба за њиховим разликовањем у свакодневном животу и правном промету (као субјекти у правним односима). Дакле, ова група података се односи на личности које својом вољом или вољом овлашћеног представника могу предузимати правно релевантне поступке. Постоји пуно примера ових података. Између осталих, то су место рођења, јединствени матични број грађана, адреса правног лица, порески идентификациони број правног лица, итд.

Подаци који се односе на предмете носе појединy карактеристику предмета, по чему се један предмет разликује од другог предмета исте врсте. Предмети, односно ствари, нису носиоци правног субјективитета, али у правном животу учествују као објекти у правним односима, те је неопходна њихова идентификација ради сигурности промета. Они немају могућност да мењају правне ситуације својом вољом, будући да је ни немају. Пример за податке о предмету јесу број шасије мотора возила, број катастарске непокретности, јачина снаге мотора пловила, итд.

Све наведене врсте података имају одређену улогу у правном животу и пракси. Помоћу њих се конкретизују правни односи и врши се разликовање између сличних лица или ствари, што олакшава одвијање правног промета. Даља анализа биће усмерена на личне податке, као једину врсту података која ужива правну заштиту због саме своје природе и улоге у правном животу.

3. ПОДАЦИ О ЛИЧНОСТИ – ПРАВНИ АСПЕКТИ

3.1. Теоријски приступ личним подацима

Лични подаци представљају карактеристичну особину одређеног лица. Они се користе у свакодневним животним ситуацијама, служећи као средство конкретизације и остваривања правних односа. Међутим, лични подаци не представљају само средство идентификације. Заправо, они представљају појавни облик одређене личности у правном животу који служи за остваривање различитих права и интереса.

У литератури није било много покушаја да се одреди појам личних података. Шварц (*Schwartz*) је сликовито одредио личне податке као „важну валуту у новом миленијуму“.[166] Ово одређење иде за тим да укаже на огромну важност коју имају лични подаци у савременом свету, па чак да је њихова улога изједначена са улогом новца. Коришћење друштвених мрежа и учествовање у електронској комуникацији мање захтева новац, а више личне податке који представљају основно средство размене.

Лилић наводи да се „за податак може рећи да представља неку врсту „основне сировине“ која се након обраде, тј. процесирања претвара у „информацију“. Информације се могу користити у најразличитије сврхе, односно регистровати и чувати у компјутеризованим информационим системима.“[167]

Кривокапић и остали аутори *Водича за органе власти – Заштита података о личности,* одређују појам података о личности. Они наводе да податак о личности представља „сваку информацију која се односи на физичко лице, које се у неком тренутку може идентификовати. Дакле, да би се констатовао податак о личности неопходно је утврдити четири одвојена елемента: 1. Информацију, 2. која се односи, 3. на идентификовано или подложно идентификацији, 4. физичко лице“.[168]

---

[166] За ову валуту се наводи да је монетарна, да је велика и да идаље расте, па америчке корпорације брзо мењају своје пословање ка профиту од овог тренда. Paul Schwartz, „Property, Privacy and Personal Data“, *Harvard Law Review*, vol. 117, University of Harvard, Harvard 2003, 2056.

[167] С. Лилић, Правни аспекти заштите података у аутоматизованим службеним евиденцијама, Наша законитост, бр. 5, Загреб, 1989, 616.

[168] Данило Кривокапић *et al., Водич за органе власти – Заштита података о личности,* Share фондација, Београд 2016, 13.

Последње одређење указује на саставне делове податка који представља податак о личности. Дакле, податак о личности може се односити искључиво на физичко лице, не и на правна лица, при чему физичко лице мора бити одређено (идентификовано) или одредиво на основу осталих елемената.

3.2. О појму личних података у праву Србије

У правном систему Србије, појам личних података не можемо пронаћи у Уставу, иако овај акт уређује питање заштите података о личности. Одређење личних података остављено је прописима ниже правне снаге, односно посебном закону. Тако је појам личних података одређен у Закону о заштити личних података (2018).

Према законској дефиницији, податак о личности представља „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“.[169]

Да би један податак представљао податак о личности он мора да се односи на физичко лице, што искључује правна лица из обима заштите. Није важан начин и средство путем кога се сазнају, као ни која врста података у питању. На крају, податак о личности мора се односити на посебну карактеристику физичког лица која га чини јединственим, при чему је неопходно да се ради о конкретном лицу или о лицу које може бити одређено (одредиво) на основу чињеница конкретног случаја.

Ово одређење разликује се од дефиниције која је садржана у претходном Закону о заштити података о личности (2008). Претходни закон одређивао је податак о личности као „сваку информацију која односи на физичко лице, без обзира на облик у коме је изражена и на носач информације (папир, трака, филм, електронски медиј и слично), по чијем налогу, у чије име, односно за чији рачун

[169] Чл. 4, ст. 1, тач. 1, Закона о заштити података о личности (2018).

је информација похрањена, датум настанка информације, место похрањивања, начин сазнавања информације (непосредно, путем слушања, гледања, односно посредно путем увида у документ у којем је информација садржана) или без обзира на друго својство информације“.[170]

Претходни закон изједначавао је податак о личности са конкретизованом информацијом. Такво решење није било адекватно будући да се мора правити разлика између информације и податка, па је боље податак о личности одредити по својој правној природи, него га одређивати у односу са информацијом. У овом одређењу појма податка о личности више се ишло за тим да се релативизује начин сазнавања, носач, облик и врста конкретног личног податка.

3.3. Појам личних података у прописима европског права

Једно од првих одређења података о личности у упоредном праву налазимо у Конвенцији о заштити лица у односу на аутоматску обраду података,[171] коју је усвојио Савет Европе 1981. године. Ова конвенција предвиђа да лични подаци представљају све информације које се односе на идентификовано лице или лице подложно идентификацији. У односу на остале домаће и стране прописе ово је најшира дефиниција. Будући да је усвојена пре више од 35 година, ово одређење представљало је пионирску дефиницију личних података у свету права, које се није превише мењала у годинама које су следиле. Можемо рећи да је поменута дефиниција коришћена, у измењеном и допуњеном издању, и у каснијим европским прописима.

Директива ЕУ о заштити појединаца у вези са обрадом личних података и слободном протоку таквих података из 1995. године, садржала је одређење личних података. У оквирима Директиве, лични подаци су се односили на сваку информацију која се односи на одређено или одредиво лице, при чему се одредиво лице може идентификовати непосредно или посредног, посебно помоћу идентификационог броја или једног или више специфичних фактора који се

[170] Чл. 3, ст. 1, тач. 1, Закона о заштити података о личности (2008).
[171] Конвенција о заштити лица у односу на аутоматску обраду података, Савет Европе, бр. 108, Стразбур, 1981. год.

односе на његов телесни, физиолошки, психички, економски, културни или социјални идентитет.[172]

Основе ове дефиниције следио је и најважнији европски документ у вези са заштитом података, Уредба о заштити физичких лица у односу на обраду података о личности и о слободном кретању таквих података (Општа уредба о заштити података ЕУ - ГДПР (у даљем тексту: Општа уредба ЕУ),[173] чијим ступањем на снагу је укинута Директива из 1995. године.[174] Општа уредба ЕУ даје одређење појам личних података. У њој се наводи да су подаци о личности „сви подаци који се односе на физичко лице чији је идентитет одређен или се може одредити; физичко лице чији се идентитет може одредити је лице које се може идентификовати посредно или непосредно, посебно помоћу идентификатора као што су име, идентификациони број, подаци о локацији, мрежни идентификатор или помоћу једног или више фактора својствених за физички, физиолошки, генетски, ментални, економски, културни или друштвени идентитет тог физичког лица“.[175] Да би се један податак могао одредити као податак о личности он мора носити карактеристику која се односи на одређено физичко лице или физичко лице које се може одредити, при чему се добијена информација односи на одређено лично и јединствено својство конкретног физичког лица, што је решење прихваћено из Директиве.

Неки од личних података које обухвата претходна дефиниција јесу: име, презиме, надимак, електронска адреса, адреса и поштански број, пословна адреса или локација, држављанство, подаци из извода из матичне књиге рођених, пасоша, личне карте или путне визе, физичка обележја (боја косе, очију), физиолошка обележја (подаци из здравственог картона), културни идентитет (чланство у културним организацијама), социјални идентитет (профили на

[172] Чл. 2, ст. 1, тач. а, Директиве ЕУ о заштити појединаца у вези са обрадом личних података и слободном протоку таквих података из 1995. године.
[173] Општа уредба о заштити података ЕУ - Regulation 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95&46EC (General Data Protection Regulation), of 27. April 2016, *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL*, 12. децембар 2018.
[174] Упор. Andrej Diligenski, Dragan Prlja, Dražen Cerović, *Pravo zaštite podataka- GDPR*, Institut za uporedno pravo, Beograd 2018, 23.
[175] Чл. 4, ст. 1, тач. 1, Опште уредбе ЕУ.

друштвеним мрежама), број социјалног осигурања, аудио снимци, видео снимци, фотографије, бројеви телефона, подаци о локацији, историја претраживања сајтова, дигитални потпис и др.[176] Дефиниција Опште уредбе ЕУ идентична је одређењу личних података из Закона о заштити података о личности (2018) Србије, што значи да је право Србије усклађено са европским прописима у погледу одређења појма личних података.

4. СУБЈЕКТИ (НОСИОЦИ) ПОДАТАКА О ЛИЧНОСТИ

4.1. Физичка и правна лица као носиоци личних података

Да би један податак представљао податак о личности, он се мора односити на физико лице. Уз то, није довољно да се ради о било ком лицу, већ подаци морају упућивати на тачно одређено или одредиво физичко лице.

На овом месту постављамо питање законитости таквог става у светлу једнакости физичких и правних лица пред законом. Наиме, у Србији сва лица су једнака пред Уставом и законом. Међутим, правна заштита података о личности пружа се искључиво физичким лицима, док правна лица остају изван оквира правне заштите. Иста је ситуација и у ЕУ, где се изричито наводи да Општа уредба ЕУ не пружа заштиту подацима који се односе на правна лица, што се односи и на друштва која су основана као правна лица (укључујући њихов назив, седиште, правну форму и податке за контакт).[177]

Правним лицима се гарантује правни субјективитет, али им није омогућена заштита личних података у поменутим прописима. Сагледавајући целокупни контекст и однос правних лица и личних података, можемо рећи да постоје аргументи за и против, да и правна лица треба да буду носиоци личних података и самим тим субјекти права на заштиту. Основни аргумент да и правна лица треба да уживају заштиту личних података јесте да и она представљају „личности“, односно да имају правни субјективитет, да својом вољом могу да утичу на правне односе и да подједнако, као и физичка лица, учествују у правном саобраћају. Том

[176] Вид. A. Diligenski, D. Prlja, D. Cerović (2018), 27-29.
[177] Уредба наводи и то да ће се примењивати на сва физичка лица у оквиру ЕУ, без обзира на држављанство, пребивалиште или боравиште лица чији се подаци штите. Вид. тач . 14 Премабуле Опште уредбе ЕУ.

логиком, лични подаци правних лица у правном промету имају значајну улогу, будући да се могу односити на специфична својства и да могу носити поверљиве информације о правном лицу (као што су подаци о унутрашњој организацији, интерна организација, пословне одлуке, итд.).

Са друге стране, основни аргумент против тезе да и правна лица треба да уживају заштиту личних података заснива се на томе да она представљају „фиктивне творевине“ које су креиране „вештачки“, одлуком надлежног органа државе (органа јавне управе или суда). Уз то, ова лица немају своју вољу, већ њихову вољу представљају овлашћена физичка лица која имају главну улогу у свим односима правних лица. Сви подаци који су од значаја за правно лице морају бити доступни јавности (у Србији подаци о правним лицима могу се пронаћи на сајту Агенције за привредне регистре), због тога што се оснивају одлуком надлежног органа, па се на тај начин избегавају могуће злоупотребе.

Можемо рећи да се у пракси јављају одређене ситуације у којима може доћи до злоупотребе (личних) података који се односе на правна лица. Правно лице поседује низ података које користи у свакодневном правном промету (рачуни правног лица, интерни акти о унутрашњој организацији, пословне одлуке, потпис заступника правног лица, лични подаци заступника, стање на банковном рачуну правног лица и други). Уз то, правна лица уживају и одређени углед у друштву, односно репутацију.[178] Такви подаци могу носити информације које се могу злоупотребити или се могу користити у циљу нарушавања репутације правног лица.

У таквим ситуацијама правна лица немају могућности да остваре правну заштиту података, будући да они не представљају субјекте права на заштиту личних података. То нас доводи до закључка да би ради свеобухватне правне заштите личних података, будући да су они у централном фокусу заштите, а не лица на која се односе, требало проширити правну заштиту и на правна лица. Правна лица могу трпети штетне последице због злоупотребе њихових личних података. Уз то, у модерним правним системима правна лица поседују правни

[178] У теорији је прихваћен став да се правним лицима признаје право на част, као и право на репутацију, односно добар глас. За више о томе вид. Slavica Krneta, „Lična prava pravnih lica“, *Godišnjak Pravnog fakulteta u Sarajevu*, br. XXV, Sarajevo 1977, 162.

субјективитет, те његови органи представљају део правног лица, што значи да њихове радње представљају радње правног лица. Логиком ствари, подаци физичких лица, када они делују у својству представника или другог организационог дела правног лица, представљају и податке физичког лица и податке правног лица који би требали да уживају правну заштиту.

4.2. Правна лица као носиоци права на заштиту личних података у праву Аустрије и Немачке

Питање субјеката који су носиоци права на заштиту личних података представља предмет расправе и у европском праву, где је отворено питање доследне примене „начела једнакости“ у области заштите података (између физичких и правних лица). Посебно се истиче пример Аустрије, која је држава чланица ЕУ, па се на њеној територији примењује Општа уредба ЕУ. Како би конкретизовала поједине области уредбе, Аустрија је донела посебан закон којим се уређује заштита личних података. Федерални закон о заштити личних података Аустрије (*Bundesgesetz über den Schutz personenbezogener Daten)*[179] ступио је на снагу 25. маја 2018. године, у исто време када и Општа уредба ЕУ. Овим законом извршена је измена одредаба Закона о заштити података из 2000. године, који се разликовао од Директива ЕУ о заштити појединаца у вези са обрадом личних података и слободном протоку таквих података из 1995. године (стављена ван снаге ступањем на снагу Опште уредбе ЕУ).

Новим законом ван снаге је стављена већина одредаба Закона о заштити податка из 2000. год. Међутим, ван снаге није стављен део 1. тог закона којим се уређује надлежност, односно обим примене закона. У члану 1. који због природе норми има уставну снагу, закон гарантује право на заштиту података као основно људско право. У том члану се наводи да „свако лице има право на поверљивост личних података, посебно у вези са приватним и породичним животом, уколико то лице има интерес који заслужује такву заштиту. Такав интерес не постоји

[179] Текст овог закона на немачком и енглеском језику доступан је на: *https://www.ris.bka.gv.at/Dokumente/Erv/ERV_1999_1_165/ERV_1999_1_165.html*, 06. септембар 2018.

уколико су подаци доступни јавности или уколико се не могу довести у везу са лицем које тражи заштиту“.[180]

Језичким и системским тумачењем одредаба устава Аустрије (посебно начела једнакости свих лица пред законом) и поменутог закона, можемо извести закључак да осим физичких и правна лица имају право на заштиту личних података. Закон о заштититити података Аустрије из 2000 год. одређивао је податке о личности као информације о субјектима чији су подаци, па су се под субјектима подразумевала физичка и правна лица. Међутим, новим законом та дефиниција личних података стављена је ван снаге (део 4. Закона о заштити података Аустрије из 2000. год.), па је остало отворено питање који све субјекти имају право на заштиту личних података. Ово питање је додатно продубљено односом аустријског и европског права које могу доћи у сукоб, будући да се норме Опште уредбе ЕУ односе искључиво на физичка лица, а њене одредбе се примењују непосредно.

Према томе, тренутно стање ствари је такво да аустријски законодавац оставља одредбу са снагом устава у Закону о заштити података о личности и посредно пружа правну заштиту личних података и правним лицима. У пракси остаје да се види на који начин ће судови и органи јавне управе примењивати одредбе поменутих прописа, односно да ли ће пружати заштиту искључиво физичким лицима, на шта их обавезује Општа уредба ЕУ или физичким и правним лицима, на шта упућује закон.[181]

У упоредној пракси (Немачка) налазимо још један пример где је правним лицима омогућено да буду титулари личних података и самим тим носиоци права на заштиту личних података. У једној од својих пресуда, Уставни суд федералне јединице *Rheinlnad-Pfalz* стао је на становиште да и правна лица имају могућност заштите личних података, будући да су и они носиоци права на заштиту личних

[180] Чл. 1, ст. 1, Закона о заштити личних података Аустрије.
[181] Privacy matters, *Austria: Data protection for personal data of legal entities under the GDPR*?, online 2018, *https://blogs.dlapiper.com/privacymatters/austria-data-protection-for-personal-data-of-legal-entities-under-the-gdpr/*, 12. фебруар 2019.

података.[182] Међутим, ова одлука је донета пре ступања на снагу Опште уредбе ЕУ, па је упитно да ли би судови поновили такав став у тренутним околностима.

На основу наведеног сматрамо да би правна лица требала да буду препозната као носиоци личних података и права на заштиту личних података и у законодавству Србије. На тај начин осигурала би се доследна примена једног од основних уставних начела - начела једнакости. Сва лица, физичка и правна, треба да буду једнака пред законом. Како и код правних лица наилазимо на податке личне природе који могу да се обрађују и користе у различите сврхе, јављају се изазови од злоупотреба и повреда. Аргумент у прилог овој тези јесте да правна лица представљају носиоце правног и пословног субјективитета и самим тим субјекте које учествују у правним пословима, са свим правима, интересима и обавезама, на сличан начин као и физичка лица.

Због тога, сматрамо да правним лицима треба пружити правну заштиту личних података, јер се на тај начин остварују основни постулати Устава Србије који штите легитимна очекивања правних лица, као и интерес правне сигурности.

4.3. Субјекти правне заштите личних података у Србији

4.3.1. Заштита личних података малолетних лица у електронској јавној управи

Тренутно стање регулативе у Србији омогућава правну заштиту личним подацима искључиво физичким лицима. Међутим, поставља се питање, да ли је свим физичким лицима омогућена заштита личних података ? У складу са начелом једнакости и забране дискриминације сва физичка лица уживају заштиту личних података.

Ипак, постављена је старосна граница у вези са појединим питањима заштите података. У том смислу, лице које није навршило 15 година живота може дати пристанак за обраду његових личних података у вези са коришћењем услуга информационог друштва једино уз пристанак родитеља, односно законског заступника.[183] Када наврши 15 година живота, малолетно лице може самостално дати свој пристанак на обраду личних података у односу на услуге

[182] Пресуда Уставног суда федералне јединице *Rheinlnad-Pfalz*, бр. Б0035/12, од 13.05.2014. Нав. према A. Diligenski, D. Prlja, D. Cerović (2018), 26.
[183] Чл. 16, Закона о заштити података о личности (2018).

информационог друштва. То значи да је и малолетницима гарантована заштита, која има другачији модалитет остваривања у односу на остала физичка лица.

У случају када услуге информационог друштва нуде органи управе, они имају дужност да предузму адекватне и разумне мере у циљу провере да ли постоји пристанак родитеља или законског заступника, у случају обраде личних података малолетника који није навршио 15. година. Ова дужност органа управе усмерена је на спречавање злоупотреба информационих технологија код давања пристанка, будући да деца путем рачунара могу самостално дати пристанак, иако нису свесна последица таквог поступка.

Због тога је важна улога органа управе да изврши разумну проверу родитељског надзора над актима детета у вези са његовим личним подацима. У циљу заштите малолетника у информационом друштву значајну улогу има и Повереник за информације од јавног значаја и заштиту података о личности, чија је једна од основних обавеза подизање свести о ризицима и мерама заштите у вези са обрадом података малолетних лица. Ово су значајне новине у праву Србије, имајући у виду да претходни Закон о заштити података о личности (2008) није посебно регулисао питања заштите личних података у вези са малолетницима.

4.3.2. Заштита личних података преминулих лица и подобност за наслеђивање права на заштиту личних података

Да ли само жива физичка лица уживају заштиту личних података или се правна заштита односи и на преминула лица? Физичко лице рођењем стиче правни субјективитет, док смрћу правни субјективитет престаје. Ипак и након смрти у правном животу фигурирају одређена права и интереси у вези са преминулим лицима, које могу остваривати њихови наследници.

Поступање са подацима преминулих лица регулисао је претходни Закон о заштити података о личности (2008). Овај закон прописивао је две ситуације у вези са личним подацима преминулих лица. Прва се односи на случај када су лични подаци прикупљени на основу уговора или писмене сагласности преминулог лица. Такви подаци чували су се у складу са утврђеним уговором, односно у складу са датом сагласношћу.

Други случај односио се на личне податке прикупљене на основу закона или другог прописа. У случају смрти њиховог имаоца, постојала је обавеза

руковаоца или обрађивача да такве податке чува најмање годину дана од дана смрти тог лица. Заједничко за оба случаја је обавеза лица које чува податке да сачини белешку приликом њиховог уништавања.[184]

У претходном закону постојала је и одредба која је одређивала круг лица која су могла да дају дозволу за коришћење личних података преминулог у тачно одређене сврхе. Такво одобрење могло се дати ради сачињавања биографије, коришћења личних фотографија, употребе личног имена и томе слично. Пристанак за обраду података умрлих лица могла су дати лица које је преминули одредио, супружник тог лица, деца старија од 15 година, браћа и сестре и други законски наследници. Ова лица могла су да користе правна средства за заштиту личних података тог лица.

У актуелном законодавству Србије не постоји одредба која уређује питање да ли и преминула лица уживају заштиту личних података. Закон о заштити личних података (2018) пропустио је да регулише ово важно питање. Норме закона уређују „право на заштиту физичких лица у вези са обрадом података о личности“, а физичко лице, према одредбама Закона, представља „физичко лице чији се подаци обрађују“,[185] што не говори о томе да ли се под физичким лицима подразумевају и преминула лица.

Поступање са правима преминулих особа уређује Закон о наслеђивању.[186] Овим законом предвиђено је да се наслеђује заоставштина, а заоставштину чине „сва наслеђивању подобна права која су оставиоцу припадала у тренутку смрти“.[187] То отвара ново питање, да ли је право на заштиту личних података право које је подобно за наслеђивање ?

Сматрамо да је право на заштиту личних података, као право које се састоји од више ужих и посебних права, подобно за наслеђивање у односу на поједине личне податке. Наиме, смрћу лица не престаје потреба за заштитом његове личности, односно његових личних података. Механизме правне заштите могу иницирати наследници преминулог. Због тога, наследницима треба омогућити право на заштиту личних података преминулог, будући да до повреде

[184] Чл. 35, Закона о заштитити података о личности (2008).
[185] Чл. 4, ст. 1, тач. 2, Закона о заштити података о личности (2018).
[186] Закон о наслеђивању, *Службени гласник* РС, бр. 46/95, 101/2003.
[187] Чл. 1, ст. 1 и ст. 2, Закона о наслеђивању.

личних података може доћи и након смрти, а наследници, као непосредно и посредно заинтересована лица, треба да имају на располагању механизме заштите личних података преминулог.

4.4. Лица која уживају заштиту личних података у ЕУ

У правном систему ЕУ искључиво физичка лица уживају заштиту личних података.[188] Дакле, правна лица не уживају могућност заштите личних података. У односу на физичка лица, Општа уредба ЕУ предвиђа да се њене одредбе неће примењивати на податке о личности преминулих особа.[189] Ова одредба је тзв. отворена клаузула, будући је у односу на ово питање остављена могућност државама чланица да својим прописима уреде обраду личних података преминулих лица. На овај начин не дира се у обраде личних података које се врше у археолошке и историјске сврхе, на које се примењују одредбе Опште уредбе ЕУ.

За физичка лица предвиђена је старосна граница од које се стиче пуна способност за самостално одлучивање и давање пристанка за обраду личних података. „Пунолетство“ за давање сагласности на обраду личних података према праву ЕУ стиче се са 16 година живота, и то у вези са услугама информационог друштва. У вези са овом старосном границом, остављена је могућност државама чланицама да предвиде и нижу старосну границу, али да не иде испод 13 година живота. Међутим, ова одредба ни на који начин не утиче на регулативу општег уговорног права у државама чланицама, што треба да омогући нормално одвијање пословних токова и закључење различитих уговора.

Измену отворене клаузуле у вези са старосном границом за давање сагласности на обраду личних података учинила је Француска. То је учињено у Закону о заштитити личних података Француске, где се за законитост обраде података захтева да дете има најмање 15. година, чиме се снижава граница

[188] Као што је претходно наведено у истраживању, изузетак представља право Аустрије. Закон о заштити података о личности Аустрије садржи уставну одредбу о једнакости лица на која се примењује закон, па је остало отворено питање, да ли ће аустријско право пружати заштиту и правним лицима, иако то излази из оквира Опште уредбе ЕУ, која се примењује у свим државама чланицама ЕУ, па тако и у Аустрији.

[189] Парламент Француске је 20. јуна 2018. године усвојио Закон о заштити личних података бр. 2018-493, чиме је Француска изменила своје законодавство у области заштите података, које је било на снази од 1978. године. Усвајањем овог закона, Француска је ускладила своју регулативу са одредбама Уредбе. Тач. 27, Опште уредбе ЕУ.

„дигиталног пунолетства“ у француском праву у односу на ону из Опште уредбе ЕУ.[190]

Осим Француске и у Аустрији је померена старосна граница за самостално одлучивање о обради података у вези са услугама информационог друштва. У Аустрији, дете већ са 14. година живота стиче могућност да самостално одлучује о обради података које се врше у вези са информационим технологијама.[191]

У случају када је дете млађе од 16 година живота, пристанак за обраду његових личних података даје родитељ или законски заступник. У таквим ситуацијама постоји посебна обавеза руковаоца да изврши сва неопходна испитивања у циљу сазнања да ли је пристанак дат на законит начин и од стране овлашћеног лица, како би се заштитио посебан интерес детета.

5. КЛАСИФИКАЦИЈА ПОДАТАКА О ЛИЧНОСТИ

5.1. Врсте личних података

Подаци о личности у данашњем свету имају велику употребну вредност. Они се користе као средство распознавања лица, идентификациони фактор, информациони ресурс, итд. Они су потребни у великом броју правних односа како би ти односи произвели правне последице. Такође, они су неопходни да би се спровела казна, пребацила новчана средства на рачун, пренела својина, преписала одговарајућа терапија, доделило лично име, уручила спортска награда, итд. Како се користе у свакодневним односима и у различите сврхе, постоји и велики број личних података.

Значајну улогу у распрострањености података о личности имају информационо-комуникационе технологије преко којих се објављује и размењује велики број личних података. Самим тим, непрестано расте и број личних података који се употребљавају у свакодневном животу, па се тако и правна заштита пружа различитим категоријама података. Ипак, и поред велике распрострањености и широке употребе, правни системи не пружају физичким лицима могућност заштите свим подацима о личности.

[190] Вид. чл. 20, Француског закона о заштити личних података.
[191] Вид. чл. 2, поглавље 1., део 1., параграф 4., ст. 4, Закона о заштити личних података Аустрије.

Подаци о личности могу се класификовати на различите начине. Разлика се може правити између података у личној, историјској, финансијској, јавној и друштвеној сфери живота појединца.[192] Поменута подела се може сузити тако да прати податке у три основне области живота појединца. То су приватна, јавна и професионална област живота појединца. Физичко лице има своју личну сферу, коју обично не дели са јавношћу, јавну сферу која се дели са којом је обично упознат већи број људи или сви заинтересовани и професионалну сферу у коју се убрајају подаци у вези са пословним активностима лица. Ове области неретко се поклапају, па лични подаци који се употребљавају у једној области друштвеног живота имају велики значај и у остале две.

Поменуте поделе претежно су теоријске природе и зависе од начина класификације сфера живота појединца. Истраживање ће пажњу усмерити на последњу класификацију.

5.1.1. Лични подаци који се односе на лични живот појединца

У податке који се односе на лични живот појединца спадају: психо-физички елементи лица (године живота, физичке и психичке карактеристике као што су боја коже, тежина, висина, облик тела, развијеност, итд.), историја о личном животу (подаци о догађајима и дешавањима у животу тог лица и са њиме повезаних лица), уверења и мишљења (лична мишљења изражена у вези са одређеном темом, религијска уверења, филозофска уверења, итд.), лични ставови и наклоност лица према стварима, лицима и појавама (омиљена врста хране, омиљена боја, песма и друго).

У ову групу можемо сврстати и друге идентификационе податке личне природе, као што су подаци о етничком и социјалном пореклу лица (раса, национална и етничка припадност, језици које говоре, акценти којима се служи употребом језика, итд.), подаци о сексуалности (родна припадност, сексуална наклоност, историја љубавних односа, итд.), медицински подаци и подаци о здрављу (физичка и психичка зрелости и здравље, физички и психички недостаци, историја болести, крвна група, здравствени картон, итд).

[192] Enerprivacy Consulting Group, Categories of Personal Information, online, *https://enterprivacy.com/2017/03/01/categories-of-personal-information/*, 08. септембар 2018.

5.1.2. Лични подаци који се односе на јавни живот појединца

У личне податке који се тичу јавног живота појединца убрајају се они лични подаци који се односе на сегменте живота појединца у друштвеној заједници. Овде можемо сврстати податке о породичном животу (да ли лице има породицу, величина породице, односи у породици, итд.) податке о социјалном окружењу (пријатељи, конекције, припадност у формалним и неформалним организацијама, итд.), податке о криминалној прошлости лица (да ли је осуђивано, да ли се воде поступци против њега, итд.).

5.1.3. Лични подаци који се односе на професионалну област живота појединца

Подаци који се тичу професионалне сфере живота једног лица говоре о друштвеним активностима лица у вези са радом и обављањем професионалних делатности. То су подаци о образовању (да ли је и које форме образовања лице похађало и завршило, оцене, завршени курсеви, итд.), пословни подаци (да ли је лице запослено, на ком радном месту, оцене о резултатима рада, одсуству са посла, итд.), финансијски подаци (бројеви рачуна, банке у којима су ускладиштена средства тог лица, подаци о личној имовини лица, кредитни статус лица, итд.), радна историја (подаци о фирмама у којима је радило лице, подаци о запосленима у фирми тог лица, подаци о новчаним примањима и трансакцијама...).

Све наведене врсте података по својој правној природи представљају личне податке. Они садрже карактеристику о одређеном сегменту живота физичког лица, за кога су везани и на кога се односе. Ови подаци су некада доступни искључиво лицу на коме се односе, док су у одређеним случајевима доступни повезаним лицима или широј друштвеној заједници.

5.1.4. Подела на „обичне“ и „посебне“ категорије података о личности

Могуће је извршити поделу на „обичне“ личне податке и „осетљиве“ личне податке,[193] који се још називају и „посебна категорија“ личних података. Ова подела прави разлику личних података у зависности од степена поверљивости и значаја који лични податак има за физичко лице. „Обични“ лични подаци носе уобичајену информацију о физичком лицу, док „осетљиви“ лични подаци носе посебно значајну информацију о личном идентитету физичког лица.

Повреда осетљивих личних података, по правилу, производи значајнију последицу за физичко лице од повреде обичних личних података. Сходно овој подели, осетљиви лични подаци уживају већи степен правне заштите у односу на друге врсте личних података. У групу осетљивих личних података убрајају се подаци о верским и филозофским уверењима, расно и етничко порекло, генетски подаци, биометријски подаци, подаци о сексуалном животу и сексуалној оријентацији физичког лица и подаци о здравственом стању.[194] Остали лични подаци спадају у групу „обичних“ личних података.

5.1.5. Подела на личне податке малолетних лица и личне податке пунолетних лица

Могуће је направити разлику између личних података малолетних и пунолетних физичких лица. Ово разликовање заснива се на другачијим механизмима заштите и начину остваривања заштите личних података у зависности од субјеката којима припадају. Заштита личних података малолетних лица захтева присуство родитеља или другог законског заступника у вези са појединим питањима заштите, на начин како је то објашњено у посебном делу о старосној граници за уживање заштите личних података. Такође, у односу на личне податке малолетних лица у прописима се успостављају и посебне улоге

[193] У претходном Закону о заштити података о личности (2008), за ове податке користио се термин „нарочито осетљиви лични подаци“. Ипак, сматрамо да то није оправдан назив, будући да закон није помињао „осетљиве личне податке“, нити разлику између „осетљивих“ и „нарочито осетљивих“ личних података.

[194] Наравно, листа нарочито осетљивих личних података зависи од правног система и процене законодавца који то лични подаци треба да уживају већи степен заштите у односу на друге.

руковаоца и обрађивача података, попут дужности проверавања сагласности родитеља или старатеља.

5.2. Лични подаци који (не) уживају правну заштиту

5.2.1. Лични подаци који (не) уживају правну заштиту у правном систему Србије

Систем заштите тежи да обухвати што више података о личности како би се заштитио што већи део човекове личности и приватности. Ипак, одређене врсте података остају изван „кишобрана“ заштите. Такав је случај са оним личним подацима који су мање важни, који су доступни јавности или који се не могу злоупотребити. У позитивно-правном законодавству Србије обично се наводе категорије личних података који уживају заштиту и оне категорије код којих правна заштита изостаје.

У праву Србије изван сфере правне заштите личних података остају они подаци који се обрађују од стране физичких лица за личне потребе или потребе њиховог домаћинства. У овој ситуацији степен опасности од пропуста и злоупотреба није превише изражен, па самим тим изостаје и заштита државе. Када се обрада личних података врши у личне и породичне сврхе, физичко лице на које се односе ти подаци и које врши обраду, мора само водити рачуна о безбедности такве обраде. Ово је једина група личних података којима Закон о заштити података о личности (2018) ускраћује правну заштиту.

Ранији Закон о заштити личних података (2008) предвиђао је знатно шири круг личних података који су изостајали из домашаја правне заштите. Групе личних података код којих је изостајала правна заштита су:

1. Подаци који су доступни свакоме и објављени у јавним гласилима и публикацијама или приступачни у архивама, музејима и другим сличним организацијама,
2. Подаци који се обрађују за породичне и друге личне потребе и нису доступни трећим лицима,
3. Подаци о члановима политичких странака, удружења, синдиката, као и других облика удруживања који се обрађују од стране тих организација,

под условом писмене изјаве да се не примењују одредбе овог закона, најдуже до времена трајања чланства лица које је дало изјаву,

4. Подаци које је лице способно да се само стара о својим интересима објавило о себи.[195]

У првом случају, актом објављивања лични подаци постају доступни јавности, па им свако заинтересовано лице може приступити и даље их користити. Јавним објављивањем они губе гарантовану „приватност“. На тај начин, изостаје и заштита која држава уобичајено пружа. У ову категорију спадају подаци у писаним документима, фотографије, аудио записи и други јавно објављени лични подаци. Осим њих, ту су и лични подаци који су од значаја за ширу друштвену заједницу (историјска истраживања, музејске поставке, итд), па правна заштита која се пружа личним подацима не би била адекватна због интереса јавности да буде упозната са одређеним чињеницама и подацима.

Када се ради о личним подацима који се обрађују у породичне сврхе, полази се од претпоставке да је породица посебна група блиско повезаних чланова које знају податке једни о другима. Такав је случај са телефонским именицима, породичним књигама и записима, албумима са фотографијама, итд. Уколико нису доступни трећим лицима они остају у оквирима породице, па је заштита државе у овом случају изостаје.

Слична је ситуација и са личним подацима физичких лица која се удружују у посебне групе и удружења повезана заједничким интересима њихових чланова. Због тога се претпоставља да ће се приватност ових података штити у оквирима таквих група и организација. Овде припадају лични подаци чланова групе, задужења и начин обављања делатности у оквиру групе, подаци о финансијским и другим давањима организацији, и томе слично.

Када физичко лице само објави податке о свом личном животу правни систем прихвата његову слободу вољу да подели личне податке са трећим лицима. Међутим, тако објављени подаци више немају строго лични карактер, па самим тим изостају из државне заштите. То је случај са писаним објавама, аудио и видео записима и фотографијама објављеним на друштвеним мрежама. Да би

[195] Чл. 5, Закона о заштити података о личности (2008).

један податак представљао део ове групе, лице које га објављује мора бити пословно способно. У супротном је учињена објава ништава и такви подаци не смеју се обрађивати ни користити.

Ипак, предвиђен је и изузетак у односу на податке који не уживају правну заштиту. Наиме, правну заштиту је уживало лице коме су повређени такви подаци када у конкретном случају „очигледно претежу интереси тог лица“. Очигледну претежност морао је да утврди надлежни орган, на основу доказа и исказа лица о чијим подацима је реч.

Иако има оправдања за ускраћивање правне заштите поменутим групама личних података предвиђених Законом о заштити података о личности (2008), сматрамо да је боље решење новог закона који познаје само једну групу података која не ужива правну заштиту. На овај начин повећава се степен правне сигурности и предвидљивости, будући да већи број података остаје под „кишобраном“ правне заштите.

5.2.2. Лични подаци који (не) уживају правну заштиту у праву ЕУ

У правном систему заштите података ЕУ одређене категорије личних података такође остају изван правне заштите. Ови подаци задржавају лични карактер, али не уживају правну заштиту. У складу са Општом уредбом ЕУ, лични подаци који не уживају заштиту као подаци о личности су:

1. Подаци који се обрађују у оквиру делатности која није обухваћена подручјем примене права Уније,
2. Подаци које државе чланице ЕУ обрађују приликом објављивања активности које су обухваћене подручјем примене поглавља 5. дела Уговора о Европској Унији,
3. Податке које обрађује физичко лице за искључиво личне или породичне активности,
4. Подаци које обрађују надлежни органи у сврху спречавања истраге, откривања или гоњења учиниоца кривичних дела или извршења кривичног дела,[196]

[196] Чл. 2, ст. 2, Опште уредбе ЕУ.

5. Подаци који се односе на лица која нису жива.

У прву групу спадају они подаци који се обрађују изван територијалне и функционалне надлежности Опште уредбе ЕУ, односно органа ЕУ и њених држава чланица. Ради се о обрадама личних података који се одвијају у државама које нису чланице ЕУ, као и у међународним организацијама које нису повезане са ЕУ, под условом да се ти подаци не односе на држављане држава чланица ЕУ.

Важан део суверености који није пренет на европске институције од стране држава чланица односи се на њихову националну безбедност. Када државе чланице обрађују личне податке у вези са питањима националне или јавне безбедности, тада се не примењује право ЕУ, односно не могу се користити механизми заштите Опште уредбе ЕУ, већ посебни прописи држава чланица.

Механизми правне заштите Опште уредбе ЕУ не могу се користити ни приликом обраде личних података коју врше државе чланице у вези са заједничком спољном и безбедносном политиком ЕУ. То је материја коју уређује 5. део Уговора о функционисању ЕУ (односно Лисабонски споразум) - Деловање Уније на спољном плану. Овај део регулише питања попут заједничке трговинске политике држава чланица, сарадње са трећим државама и хуманитарну помоћ, међународне споразуме, односе Уније са трећим државама итд.[197] На неки начин и ова питања су повезана са безбедношћу и интегритетом уније и њених чланица. Сматрамо да су поменуте формулације апстрактне и да остављају простор за потенцијалне злоупотребе личних података, под паролом националне безбедности или безбедности Уније.

Трећу групу личних података који не уживају правну заштиту јесу подаци које физичка лица обрађују у личне и породичне сврхе. У овим ситуацијама изостаје реакција државе, јер не постоји потреба за упливом државе у строго личну сферу појединца. Самим тим, претпоставља се да је обрада личних података у личне или породичне сврхе приватна ствар о којој превасходно мора да води рачуна лице чији су подаци.

[197] Вид. део 5. Уговора о функционисању Европске уније, односно Уговор из Лисабона којим се мења Уговор о Европској Унији и Уговор о успостављању Европских заједница, бр. 207/С 306/01, део под називом „Спољне акције Уније“. Уговор из Лисабона, *https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:C:2007:306:FULL&from=HR,* 09. септембар 2018.

Лични подаци који обрађују надлежни органи (полиција, тужилаштво) у циљу примене одредаба кривичних и прекршајних прописа, а ради гоњења учиниоца кривичних и прекршајних дела остају изван заштите коју пружа Општа уредба ЕУ. Поступање са таквим личним подацима уређује се посебним прописима који уређују правила поступања органа који раде на расветљавању и гоњењу учиниоца кривичних дела.

Већ је поменуто да се правила о заштити личних података односе искључиво на физичка лица која су жива, па се личним подацима преминулих лица не пружа правна заштита.

5.2.3. Оправданост непружања правне заштите појединим категоријама личних података

Иако сви подаци о личности представљају важан део личности појединца, не пружа се свим личним подацима правна заштита. Разлози због којих изостаје правна заштита обично се односе на одређени облик јавног интереса или на јавну сферу живота појединца који, према прописима, оправдавају изостанак опште правне заштите која се пружа осталим личним подацима.

Сматрамо да такво решење није оправдано, јер не подстиче правну сигурност и предвидљивост, већ отвара могућност за злоупотребу личних података. Апстрактне формулације („интерес националне безбедности“, „интерес безбедности ЕУ“) које се користе приликом одређивања разлога због којих може изостати правна заштита, дозвољавају органима управе да их користе према сопственим потребама, које не морају увек бити легалне.

Због тога, можемо рећи да актуелно решење у правном систему Србије, које изоставља само једну категорију личних података из правне заштите (обрада личних података за сопствене потребе и потребе породичног домаћинства) јесте квалитетније од решења из претходног Закона о заштити података о личности (2008), али и од решења актуелног европског законодавства у области заштите података. Шира правна заштита која обухвата већи број личних података повећава правну сигурност и предвидљивост, што је грађанима од изузетног значаја.

5.3. Посебне категорије личних података

5.3.1. Посебне категорије личних података у праву Србије

Поједине врсте личних података не уживају правну заштиту. Међутим, постоје и друге врсте личних података које уживају већи степен заштите у односу на ону која се уобичајено пружа. Јављају се посебне категорије личних података које се не смеју обрађивати. Ове категорије уживају посебну заштиту, будући да се односе на карактеристике осетљиве природе и њиховом повредом или злоупотребом може доћи да значајних негативних последица по физичко лице на које се односе. Повреда ових категорија личних података може имати утицаја на друштвену позицију, углед и статус одређеног лица.

Посебне категорије личних података постоје и у правном систему Србије. Ова група података некада је носила назив (нарочито) осетљиви лични подаци, како их је именовао претходни Закон о заштити података о личности (2008). Актуелни Закон о заштити података о личности (2018) одређује ову врсту података, као „посебну категорију“ личних података, чија обрада није дозвољена, осим под одређеним условима.[198] У ову групу спадају подаци који се односе на:

1. Расно и етничко порекло,
2. Политичко мишљење,
3. Верско и филозофско уверење,
4. Чланство у синдикату,
5. Генетске податке,
6. Биометријске податке,
7. Податке о здравственом стању,
8. Податке о сексуалном животу и сексуалној оријентацији лица.[199]

Ипак постоје одређене ситуације у којима је дозвољена њихова обрада.[200] Такве ситуације односе се на постојање одређеног облика јавног интереса или

[198] За више о условима допуштености обраде посебних категорија података о личности у српском праву вид. чл. 17, ст. 2, Закона о заштити података о личности (2018).
[199] Чл. 17, ст. 1, Закона о заштити података о личности (2018).
[200] Посебни случајеви могућности обраде посебних врста података о личности предвиђени су у чл. 17, ст. 2, Закона о заштити података о личности (2018).

претежнијег приватног интереса у односу на интерес лица чији се подаци обрађују.

Уколико не би постојала могућност обраде посебних података, правни систем не би могао нормално да функционише и редовни друштвени токови би били спутани и успорени. Због тога, систем заштите личних података Србије предвиђа неколико ситуација у којима је могуће обрађивати посебне податке. Приликом обраде ових података неопходно је да орган управе предузме разумне и одговарајуће мере у циљу заштите права и интереса лица чији се подаци обрађују, као посебан услов обраде.

Обрада посебних категорија података може се вршити уз пристанак лица о чијим подацима је реч. Када постоји изричита и јасна сагласност, нема препрека обради посебних личних података. Сматра се да пристанак за обраду постоји и када је лице на које се подаци односе учинило јавним такве податке, па се и у таквим ситуацијама може вршити обрада.

Поједине посебне податке могу обрађивати и различите организације, попут удружења, фондација и задужбина, али искључиво у сврху функционисања организације. Могу се обрађивати једино подаци чланова организација или са организацијом повезаних лица, уз додатан услов да се такви подаци не објављују изван организације. Такође, у вези са органима управе, руковаоци у области рада, социјалног осигурања и социјалне заштите имају право да обрађују посебне податке када је таква обрада неопходан услов извршења обавезе организације. Таква обрада мора бити предвиђена посебним законом или колективним уговором о раду, што значи да није довољна појединачна одлука руковаоца.

Обраду посебних категорија података могу вршити и судски органи када поступају у пословима из своје надлежности. Потреба правичног вођења судског поступка и сазнавања истине у поступку захтева темељну анализу свих чињеница конкретног случаја, које се могу односити и на посебне категорије података. У вези са судским и другим правним поступцима, треба поменути да је дозвољена обрада посебних категорија података која се одвија у циљу подношења, остваривања или одбране од правног захтева.

Постоје ситуације у којима се могу обрађивати посебне подаци ради заштите јавног здравља. Тако, обрада може се предузети ради остваривања

превентивних дужности у медицини или медицини рада, а у циљу оцењивања радне способности запослених и будућих запослених, што мора бити утемељено на закону или колективном уговору. Дозвољене су обраде посебних категорија података ради остваривања здравља становништва, када посебним законом морају бити предвиђене додатне мере заштите.

Управни органи могу вршити обраду посебних категорија података када постоји потреба за остваривањем „значајног јавног интереса“. Постојање таквог интереса процењује поступајући орган у вршењу својих дужности, али он мора бити прописан законом. Чак и када постоји значајан јавни интерес, управни орган код обраде посебних категорија података мора водити рачуна о принципу сразмерности и поштовању суштине права физичких лица чији се подаци обрађују.

Ситуација која оставља највише простора за полемику јесте могућност обраде осетљивих података у сврхе архивирања у јавном интересу, у сврхе научног или историјског истраживања и у статистичке сврхе.[201]

Сматрамо да је ова одредба постављена сувише широко и дозвољава релативно лак приступ посебним категоријама података. Као додатни услов за вршење оваквих обрада предвиђено је поштовање суштине права на заштиту података и примена одговарајућих и посебних мера заштите података који се обрађују. Статистичке и историјске сврхе дозвољавају широко тумачење у оквиру кога се могу обрађивати значајни подаци грађана. Сматрамо да ову одредбу треба поставити знатно уже, тако да представља предмет посебног закона који би предвидео додатне услове, попут дужности образложења сваке обраде у поменуте сврхе.

За разлику од закона који је тренутно на снази, претходни Закон о заштити података о личности (2008) предвиђао је категорију „нарочито осетљивих података“. Он је садржао дужу листу „посебних“, односно нарочито осетљивих података. У односу на тренутно стање ствари, као нарочито осетљиви подаци били су предвиђени и пол, језик, припадност политичкој странци, подаци о

[201] Чл. 17, ст. 2, тач. 10, Закона о заштити података о личности (2018).

примању социјалне помоћи, подаци о жртвама насиља и подаци о осуди за учињено кривично дело.

Значајна одредба у односу на обраду нарочито осетљивих података односила се на то да је и мере заштите и начин архивирања података из ове категорије уређивала Влада, уз претходно прибављено мишљење Повереника. Ова одредба је изостала у новом закону. Сматрамо да је такво правило представљало додатни степен заштите осетљивих података, будући да су управни органи морали да поступају према одлуци Владе и мишљењу Повереника, што говори о већем степену важности ових података. Такав принцип треба широко прихватати у области заштите података, јер што је више степена заштите, мања је опасност од повреде (осетљивих) личних података.

5.3.2. Посебне категорије личних података у праву ЕУ

Општа уредба ЕУ такође познаје одређене категорије личних података који уживају посебну заштиту.[202] Ови подаци носе назив „посебне категорије личних података“.[203] Они се односе на расно и етничко порекло, политичко опредељење, верска и филозофска убеђења, припадност синдикату, обраду генетских и биометријских података, здравствено стање, сексуални живот и сексуалну оријентацију физичког лица.[204] У односу на домаће прописе, примећујемо да је листа „посебних категорија личних података“ нешто дужа у односу на „нарочито осетљиве податке“ из српског права.

За посебне категорије података сматра се да су „по својој природи посебно осетљиви у погледу основних права и слобода (које штите) и заслужују посебну заштиту, јер би у оквиру њихове обраде могло да дође до значајних ризика за основна права и слободе“.[205] Међутим, и у посебним категоријама личних података постоје подаци који уживају посебан третман. Наиме, државама чланицама је остављена могућност да унутрашњим прописима додатно уреде услове који се односе на обраду генетских података, биометријских података и

[202] За више вид. P. Lambert (2018), 112-115.
[203] У теорији се наводи да је за ову врсту података уобичајен назив „осетљиви подаци“. A. Diligenski, D. Prlja, D. Cerović (2018), 43.
[204] Чл. 9, Опште уредбе ЕУ.
[205] Тач. 52 Преамбуле, Опште уредбе ЕУ.

података о здравственом стању. Ове категорије података могу директно утицати на живот и психо-физички интегритет физичких лица, па њихова обрада заслужује регулативу која обухвата и посебности одређеног друштва и његових чланова.

Обрада посебних категорија података о личности у праву ЕУ је забрањена. Ипак, јављају се одређене ситуације које оправдавају и чине обраду ових категорија података легалном.

Прва група ситуација која оправдава обраду посебних категорија личних података тиче се појединца чији се подаци обрађују. Обрада посебних категорија је дозвољена уколико постоји изричит пристанак њиховог имаоца на обраду, када је неопходно да се изврши обрада ради заштите основних животних интереса лица на које се подаци односе и када је такве податке очигледно објавило лице на које се подаци односе.

Друга група ситуација односи се на посебне обраде личних података. Врсте обраде које оправдавају употребу посебних категорија личних података односе се на циљеве руковаоца и обрађивача у области рада, приликом запошљавања, остваривања права из социјалног осигурања и социјалне заштите и приликом обрада које предузимају фондације, удружења и други непрофитни облици удруживања, када су усмерене на податке њихових чланова.

Трећа група ситуација која оправдава обраду посебних категорија личних података тиче се остваривања значајних јавних интереса. То су ситуације када суд обрађује посебне категорије података ради испитивања правних захтева, када је обраду неопходно спровести у медицинске сврхе и сврхе јавног здравља, као и када обрадом треба да се оствари сврха научног, историјског или статистичког истраживања.

У свакој од ових ситуација, руковалац и обрађивач морају имати адекватан законски основ који је утемељен на конкретним чињеницама које оправдавају обраду посебних категорија личних података. Уз то, руковалац и обрађивач морају посветити посебну пажњу заштити људских права у вези са оваквим обрадама, при чему морају имати у виду право ЕУ и право државе чланице.

5.4. Базе личних података

5.4.1. Теоријски приступ базама података

У данашњем свету лични подаци прикупљају се у различите сврхе. Њих прикупљају приватни руковаоци и обрађивачи у пословне намене, али и органи државе, ради обављања јавних послова и омогућавања нормалног одвијања друштвених токова. Лични подаци који прикупе органи управе чувају се и користе, у највећем обиму, у дигиталној форми. У таквим ситуацијама, прикупљањем великог броја личних података стварају се базе података, односно организовани скупови личних података. „Базе података и технологија база података има огроман значај у развоју рачунара. Поштено је рећи да базе података имају одлучујућу улогу у скоро свим областима у којима се користе рачунари, попут пословања, електронске трговине, инжењерства, медицине, генетике, права, образовања и библиотекарства…“.[206] Ове речи ближе описују значај које имају базе података у данашњим информационим системима. Без база података информациони системи се не могу ни замислити. Њихова важност огледа се у структури информација које су похрањене и које се могу брзо и лако користити у различите сврхе у разним областима друштвеног живота.

Теоријски, базе података се одређују као организовани скуп личних података.[207] Дакле, није довољно прикупити личне податке, већ је неопходно систематизовати их и чувати их по одређеном обрасцу. Када говоримо о органима управе, њихове раније базе података састојале су се од великог броја папирних докумената са личним подацима. Развој информационо-комуникационих технологија омогућио је уштеду времена и простора, па су се базе података дигитализовале.

Данас се базе података обично чувају у електронском облику, похрањене у меморији рачунара или у виртуелном облику у „облацима“ (енг. *clouds*). Они представљају јединствено место где се може приступити сачуваним подацима одређене категорије или врсте, ради њиховог преузимања и даљег коришћења у

[206] Ramez Elmasri, Shamkant Navathe, *Fundamentals of Database Systems*, Addison-Wesely Publishing Company, Boston – Columbus - ets. 2010, 4.
[207] Рамез и Навте дају једноставније одређење база података као колекције повезаних података. Упор. R. Elmasri, S. Navathe (2010), 4.

одређене сврхе. Због тога, базе података нашле су своје место и у правним системима широм света, па и у Србији, посебно у вези са делатностима електронске јавне управе.

5.4.2. Базе података у правном систему Србије

Управљање базама података треба да буде уређено законом или другим подзаконским актима. У Србији, Закон о заштити података о личности (2018), не уређује на посебан начин управљање и вођење базама података, али на податке који чине одређену базу могу се применити одредбе о чувању и приступу подацима о личности.

Ипак, генерално руковођење базом података представља предмет законске регулативе и то Закона о информационом систему Републике Србије.[208] Овај закон уређује начин поступања органа управе приликом вођења евиденција и управљања подацима у вези са информационим системом Републике Србије. Садржај базе података чине подаци чије је вођење предвиђено законом, а тако формиране базе података представљају информациони подсистем друштвене области у вези са којим се и чувају лични подаци. Одређење појма базе података садржи и Закон о електронској управи, који одређује базу података као организован и уређен скуп међусобно повезаних структуираних података који може имати једну или више евиденција.[209]

Закон о информационом систему Републике Србије познаје и категорију заједничке базе података која представља централни регистар из којег органи и организације управе повлаче податке када су им неопходни за вођење посебних евиденција или посебних база података. Дакле, заједничке базе података представљају електронску магистралу којој се може приступити под одређеним условима ради преузимања појединог податка.

Од изузетног је значаја водити рачуна о могућности приступа овом регистру, јер постоји велики број органа управе, па је важно тачно одредити субјекте и разлог приступа бази, како би се избегле злоупотребе. Сваки корисник мора да прође кроз процес одобрења који се пролази употребом електронских

[208] Закон о информационом систему Републике Србије, *Службени гласник* РС, бр. 12/96.
[209] Чл. 4, ст. 1, тач. 1, Закона о електронској управи.

идентификационих података корисника. На тај начин, образовањем базе података, остварује се и заштита личних података, будући да се води евиденција субјеката који приступају бази.

Органи управе морају да воде и секундарне (алтернативне) базе података које омогућавају константност у раду, уколико се јаве проблеми на примарној бази података. Секундарне базе не смеју да се чувају на истом месту где и примарне базе података. Правило је и да се све базе података чувају у Србији, а само уз посебне мере безбедности могу да се износе ван територије Републике Србије. Осим тога, органи управе су дужни да воде речнике података информационих подсистема. Под речницима података информационих подсистема подразумева се опис и структура базе података, регистара и евиденција у надлежности тог органа.[210]

5.4.3. Значај база података за функционисање органа управе и друштва

Важност база података за обављање делатности органа управе и за нормално одвијање друштвених токова од великог је значаја.[211] Правилно доношење одлука и предузимање мера мора се заснивати на потпуно утврђеном чињеничном стању конкретног случаја. Међутим, чињенично стање је могуће потпуно утврдити једино узимањем у обзир свих елемената случаја који се неретко могу наћи похрањени у одговарајућој бази података. Имајући у виду да органи управе своје делатности врше у разним областима живота (здравство, култура, пољопривреда, водопривреда, итд.), отуда постоје и различите базе података која се чувају.

Различите базе података могу пружити значајне информације за решавање неспорних и спорних ситуација друштва и грађана, што може да буде од значаја за убрзање управног поступка. Такође, оне се користе као средство које помаже органима да брже и ефикасније обављају своје делатности, било да се ради о

[210] Чл. 11, Закона о информационом систему Републике Србије.

[211] Потреба за базама података последица је чињенице раста улоге и значаја информација у савременом свету и информационо оријентисаном друштву. Због тога, базе података имају велики значај као централно место где се може похранити велики број информација у виду текстова, података, слика, аудио и видео садржаја, итд. Mark Davison, *The Legal Protection of Databases*, Cambridge University Press, Cambridge – New York – Melbourne 2003, 2.

јавном интересу или о интересу странке, односно физичког лица чијим подацима се у бази приступа.

Због велике практичне примене у различитим областима живота базе података представљају средство који помаже развоју државе и друштва. Стога, напредак информационих технологија отвара нове могућности употребе база података. Лични подаци и базе личних података посебно добијају на значају и практичној примени у садејству са информационо-комуникационим технологијама. То се посебно односи на перспективну информациону област великих база података, односно *big data,* у коју се све више улаже и која се брзо развија.

5.5. Big data и лични подаци

5.5.1. Одређење појма *big data*

Велике базе личних података могу се користити као средство за ефикасније доношење пословних и државних одлука, унапређења техничких и стручних поступака и за предвиђање понашања субјеката на које се подаци из базе односе. То је од великог значаја за рад органа управе који могу користити групе података за доношење одлука, предузимање мера и радњи заснованим на резултатима анализе великог броја података који се односе на поједину област друштвеног живота, у којој они имају надлежност.[212]

Базе података који су на системски начин повезане и умрежене коришћењем информационо-комуникационих технологија носе назив *big data*. Теоријски посматрано, појам *big data* се „односи на пројектовање и реализацију поуздане, дистрибуиране и скалабилне инфраструктуре за управљање, анализу, дељење, складиштење и пренос великих количина података. Потреба за оваквом инфраструктуром настаје због скупова података који су толико велики да их није могуће обрадити помоћу стандардних приступа и алата“.[213] Други одређују појам *big data* преко основних карактеристика, односно основних саставних елемената.

[212] Упор. Christian Döpke, „The Importance of Big Data for Jurisprudence and Legal Practice“, у *Big Data in Context- legal, Social and Technological Insights*, (eds. Thomas Hoeren, Barbara Kolany-Raiser), Springer, online 2018, 14.
[213] Божидар Раденковић *et al., Електронско пословање*, Факултет организационих наука, Београд 2015, 278.

Сикулар (*Sicular*) наводи да *big data* представља „обиман, брз и разноврсан систем информација који омогућава штедљиве и иновативне облике обраде података који омогућавају квалитетније одлучивање и доношење одлука“.[214]

Велике скупове података карактерише различитост садржаја који се налазе у њима. Подаци могу бити у различитим облицима, попут текста, звука и слике. Такође, системска повезаност података омогућава велику брзину у њиховој размени и приступу, што је још једна од одлика *big data* система.

5.5.2. Концепт *Big data* у електронској јавној управи

Могућност примене *big data* система могућа је у свим областима у којима функционишу органи управе. Такав је случај са јавним здрављем, где велике количине личних података могу да се употребе као основа доношења мера заштите и предвиђање кретања појединих здравствених појава у зависности од бројних чинилаца. На основу анализе података из базе, може се установити потреба за набавком одређених медицинских средстава, потреба за улагањем у инфраструктуру или напредовањем у појединим областима здравства, усавршавањем стручњака у одређеним областима, итд.

У области јавне безбедности велике количине података могу служити као средство при одређивању мера затвореницима или као помоћ у доношењу одлуке о пуштању на слободу одређеног лица или затварању лица у одређени строжије чуван затвор. У области пољопривреде, велике количине података бити изузетно корисне приликом доношења одлуке о давању субвенција појединим субјектима, потреби за улагањем у поједине области пољопривреде или за предвиђање временских услова који ће бити предочени грађанима укљученим у ову област. Примена ових система података могућа је у готово свим областима друштвеног живота.

---

[214] Svetlana Sicular, „Gartner's Big Data Definition Consists of Three Parts, Not to Be Confused with Three 'V's", Forbes, online 2013, *http://www.forbes.com/sites/gartnergroup/2013/03/27/gartners-big-data-definition-consists-of-threeparts-not-to-be-confused-with-three-vs/*, 04. јануар 2019. Упор. Hugh Watson, “Tutorial: Big Data Analytics: Concepts”, *Technologies and Application, Communications of the Associations for Information Systems*, vol. 34, art. 65, The Berkeley Electronic Press, Berkeley 2014, 1249, *https://pdfs.semanticscholar.org/d392/0f02dbb15da19b04d782fc0546ef113e0bf7.pdf* , 04. јануар 2019.

Међутим, да би обрада података који се налазе у *big data* системима била законита, неопходно је усмерити пажњу на одређене елементе обраде. То значи да је пре састављања сваке базе са великом количином података неопходно предузети заштитне мере, попут процене ризика по податке свих лица чији се лични подаци налазе у таквом систему. Важно је водити рачуна и о односу сврхе обраде, због тога што се у бази налазе велике количине података, од којих неке не морају да имају везе са обрадом, па се не смеју обрађивати. Такође, не треба заборавити и „право на заборав“ приликом креирања ових система, будући да се захтевима у вези са брисањем података мора удовољити, чиме се јавља опасност по нормално функционисање *big data* система.[215]

У ери електронске јавне управе, *big data* системи ће представљати неопходно средство у решавању различитих државних и друштвених питања. Значајна помоћ који *big data* системи пружају у свакодневним и важним пословима управе, омогућава употребу личних података у циљу остварења најважнијих интереса друштва. Трендови употребе информационих система, у оквирима којих се посебно истиче *big data*, извршиће утицај и на начине обраде личних података.

Од посебног је значаја да се питање заштите личних података база уреди на темељан и свеобухватан начин подзаконским актима који ће пружати заштиту различитим врстама личних података на државном и међународном нивоу. Правци развоја електронске јавне управе указују да ће у догледно време и системи великих база података имати значајну улогу у функционисању органа управе, па је стога потребно регулисати и безбедност информационих система органа управе. Дакле, основна полуга која гарантује правилно и неометано функционисање *big data*, али и других информационих система који ће наћи своју примену у електронској јавној управи, јесте потпуно уређен систем правне заштите личних података.[216]

[215] Упор. A. Diligenski, D. Prlja, D. Cerović (2018), 63-64.
[216] Упор. C. Döpke (2018), 14

***

Овим закључујемо део о личним подацима и њиховој улози у друштвеном и правном животу. Будући да смо претходно одредили два основна појма овог истраживања, електронску јавну управу и личне податке, пажњу ћемо усмерити на основне механизме правне заштите личних података у Србији. Пре упуштања у анализу основних механизама заштите, испитаћемо појам, историјат и значај правне заштите личних података.

IV ПОЈАМ, ИСТОРИЈАТ И ЗНАЧАЈ ЗАШТИТЕ ПОДАТАКА О ЛИЧНОСТИ

1. О ПОЈМУ ПРАВНЕ ЗАШТИТЕ ЛИЧНИХ ПОДАТАКА

Појам правне заштите личних података тешко је дефинисати и прецизно одредити због великог броја елемената који чине такав систем. Бројни елементи утичу на то да област заштите личних података буде претежно мултидисциплинарна. Стога, правне норме представљају један, али најважнији и основни, део система правне заштите. У циљу разумевања правног појма заштите личних података, можемо рећи да се правни аспекти неминовно надовезују на техничке и организационе елементе заштите личних података. Поменути елементи су у пракси уско повезани и постижу одговарајуће резултате једино узајамним деловањем. Због тога се систем заштите личних података мора састојати од својеврсног троугла заштите који обухвата правне, техничке и организационе норме. Једино подаци који се налазе у оквиру троугла наведених подсистема могу бити у потпуности заштићени од негативних појава.

Као што смо поменули, основу система правне заштите представљају правне норме. Правне норме имају задатак да обликују, уреде и ускладе питања правног, организационог и техничког карактера. Оне омогућавају поштовање правила понашања које важе једнако за сва лица. У том контексту, правне норме представљају средство заштите и основу на коју се надограђују остали сегменти заштите. Специфичност правне заштите огледа се у томе што једино правне норме, за разлику од техничких и организационих норми, производе правна дејства, односно правно релевантне последице. Правно релевантне последице огледају се у пракси кроз остваривање људских права и интереса или примени санкција за непоштовање правних норми.

1.1. Материјални и функционални појам правне заштите личних података

Правне норме које уређују систем заштите личних података морају бити усклађене са другим нормама (техничким, технолошким и организационим), по којима поступају лица која прикупљају и обрађују личне податке грађана. Основни циљ тако конструисаног правног система заштите података усмерен је на

поштовање људских права и слобода и обезбеђење интегритета личних података. Посредни циљ тиче се очувања сигурности правног поретка и основних принципа демократског друштва. На тај начин долазимо до правног појма заштите података у материјалном смислу, као појма који обухвата непосредни и поседни објекат заштите, а суштински је усмерен на очување основних људских права, слобода и интереса у вези са личним подацима. Материјални појам усмерен је на материју која се штити правним нормама у области заштите података, а то су приватност и права грађана. Са друге стране можемо одредити и функционални појам правне заштите података о личности. Овај појам обухвата начине остваривања предвиђених циљева заштите. Прецизније речено, овај појам говори која су средства неопходна да би се пружила заштита основним заштитним објектима, које обухвата материјални појам заштите.

У теорији се наводи да је функционални (формални) појам заштите података одређен обављањем активности:

1. ограничења располагања одређеним врстама података,
2. обавезе (не) давања информација недржавним субјектима, државним органима и организацијама,
3. обавештавања грађана о подацима који се о њима прикупљају и у коју сврху.[217]

Сматрамо да би уз поменуте активности требало додати још неке елементе заштите како би дошли до јединственог свеобухватног појма. Додатни елементи се односе на правила поступка пред надлежним органима у вези са заштитом личних података и активностима санкционисања насталих повреда. У оквире тако постављеног функционалног појма заштите података треба уврстити и средства којима се остварује заштита података. Под средствима подразумевамо правно уређене механизме заштите који омогућавају остваривање права и интереса грађана у овој области.

[217] Dragan Prlja, Mario Reljanović, *Pravna informatika*, Službeni glasnik, Beograd 2010, 87.

1.2. Теоријско одређење појма правне заштите личних података

Можемо закључити да правна заштита личних података представља појам који обухвата процес доношења и примене општих и посебних правних норми које подразумевају техничка и организациона правила и успостављање правних механизама и средстава у циљу заштите личних података.

Поменуто одређење аутора обухвата елементе материјалног и функционалног појма заштите. На тај начин долази се до свеобухватног теоријског појма који уважава практична питања у вези са заштитом личних података. Такође, поменуто одређење омогућава независност појма правне заштите личних података од променљивих елемената правног система и друштвеног развоја.

2. ИСТОРИЈАТ ПРАВНЕ ЗАШТИТЕ ЛИЧНИХ ПОДАТАКА

2.1. Друштвени фактори који су подстакли развој система правне заштите личних података

Историјски посматрано, заштита личних података представља релативно нову област правног регулисања. Пре коришћења информационо-комуникационих технологија у свакодневном животу људи, првобитни облици правне заштите односили су се на папирне документе, који су садржали личне податке грађана. Једини начин чувања личних података био је физички, будући да лични подаци нису имали толику улогу у друштву и могли су бити размењени једино физичким путем. Документи са личним подацима чували су се физички одвојено од осталих докумената, на „сигурним местима“, па није ни постојала потреба за детаљнијом правном регулативом у овој области. Такође, мала улога личних података у друштву није указивала на потребу за правним уређењем.

Значајније интересовање за уређење правне заштите у вези са личним подацима развијало се упоредо са појавом и развојем информационо-комуникационих технологија. Процеси дигитализације повезивали су људе и омогућавали дигиталну комуникацију која се одвија независно од тога где се они физички налазе. Скоро неприметно, развој технологије учинио је људе све више зависним од информационо-комуникационих уређаја и дигиталних услуга.

Основна улога нових технологија односила се управо на размену информација, које су неретко садржале и личне податке.

Дигитализација је брзо ушла у све елементе друштвеног живота, од којих су можда најважније трговина и размена добара. Трговина и размена добара подразумевале су размену робних и новчаних средстава, али и личних података, као средства идентификације. Привреда, као један од основних мотора друштвеног развоја, даље је развијала и пласирала бројне електронске услуге које су омогућавале до тада неслућене могућности, као што су дигитализација новца и трансфер различитих имовинских вредности и материјалних добара у дигитализованом и нематеријалном облику (такав је случај са акцијама, вредносним папирима, уделима у компанијама, итд.). Дигитализацију привреде пратили су и органи управе како би могли нормално да функционишу и обављају улогу у модерном друштву. Држава дигитализује услуге својих органа, премешта обављање различитих делатности у дигиталну сферу и претвара традиционалну управу у електронску управу. Како информације постају све важније средство размене, њихова безбедност постаје питање од примарног значаја. У таквом стању ствари, све важнији објекат правне заштите постају лични подаци грађана.

Можемо закључити да је борба за право на приватност интензивирана тек у 21. веку. Прецизније речено, поменути век представља раздобље људске историје у коме су као кључна постављена питања безбедности личних података и надзора над свакодневним активностима људи. Информационо-комуникациони системи и невероватан напредак технологија омогућили су економски јаким субјектима да обављају свеобухватну контролу над грађанима, чиме су додатно ојачали своју надмоћ. У том смислу, информације су постале „нова нафта“, која се лако „извлачи“ и оставља простора за разне злоупотребе. Коришћењем информација и предвиђањем будућности, субјекти постају доминантни у пољима у којима обављају делатности, усклађују и побољшавају профит од свог пословања, прикупљају материјал за политичке поене и припремају терен за могуће малверзације.

Међутим, свесни грађани брзо су узвратили ударац. Разумевањем нових технологија и опасности које од њих вребају, почеле су појединачне и групне акције против поступања моћних субјеката друштвених система. Својеврсна

побуна започела је указивањем на опасности, а наставила се обелодањивањем информација које говоре да поједини субјекти заиста злоупотребљавају личне податке и надзиру различите приватне активности грађана.

2.2. Случај „Сноуден“ и заштита личних података

Један од најзначајнијих случајева у светској историји, који је подстакао јавност да више говорио о неопходности заштите личних података, односи се на пионира узбуњивача у материји података о личности - Едварда Сноудена (*Edward Snowden*). Сноуден је био амерички информатичар у фирми *Booz Allen Hamilton*, која је била у уговорном односу са Националном агенцијом за безбедност САД. Његово радно место омогућавало му је приступ „поверљивим“ информацијама будући да је као технички службеник имао приступ системима који се користе у оквиру пројекта „*Пет очију*“ (Five eyes).[218] Априла 2012. године, схвативши шта се заиста ради са личним подацима и који се све лични подаци прикупљају, Сноуден почиње са тајним преузимањем информација о прикупљеним подацима. Ступивши у контакт са значајним медијским кућама, као што је *The Guardian* и *The Wall Street Journal,* Сноуден је информације до којих је дошао у обављању своје делатности поделио са јавношћу, без икакве новчане накнаде, будући да му је главни циљ било разоткривање масовног кршења људских права преко надзирања друштвених активности.

Даље активности водиле су до једног од највећих скандала у савременој историји. У јуну 2013. године у афери „ПРИЗМА“, откривено је да су највеће светске компаније које послују са бројним личним подацима користиле те податке и достављале их Влади САД, која их је прикривено користила и флагрантно злоупотребљавала. Програм Призма је само шифровано име за пројекат у оквиру кога је Национална агенција за безбедност САД прикупљала читаву електронску комуникацију грађана и то помоћу највећих светских компанија које се у свом

[218] Пројекат „Five eyes“ представља обавештајни савез пет држава (САД, Уједињено Краљевство, Канада, Аустралија и Нови Зеланд), који се зансива на споразуму САД и Уједињеног Краљевства о обавештајним сигналима. James Cox, *Canada and the Five Eyes Intelligence Community,* Strategic Studies Working Group Papers, 2012, *https://www.opencanada.org/features/canada-and-the-five-eyes-intelligence-community/,* 20. фебруар 2019.

пословању користе личним подацима. Као највеће, можемо навести *Microsoft, Google, Facebook, Yahoo, Apple*, али и многе друге.

Ове компаније омогућиле су Националној служби за безбедност приступ својим серверима и подацима који се користе у пословању.[219] Користећи личне поруке, електронску преписку, фотографије, документе и шифре за коришћење друштвених мрежа, САД су постале тајни господар свих информација. По каснијем признању, све трансакције које су остварене путем платних картица, биле су под надзором обавештајне службе. То је коришћено за надгледање савезника, па је тако обелодањено да су надзирани и највиши званичници ЕУ (међу њима и немачки канцелар), али и званичнике Уједињених нација. Пројекат Призма је одобрио амерички федерални суд, а о њему су били информисани и поједини званичници Конгреса који се баве обавештајним пословима. Овакво чињенично стање потврдио је и тадашњи директор Џејмс Клапер (*James Clapper*).[220] Ова афера умногоме је допринела развоју свести о значају личних података и потреби за њиховом заштитом.[221]

2.3. Историјат правне заштите личних података у упоредном законодавству

Првобитни облици правне заштите односе се на заштиту личних података у дигиталном облику. Први прописи који уређују ову материју јављају се 1970. године у Немачкој савезној држави Хесе. У овој држави донет је пропис чији је непосредни циљ регулисања усмерен на заштиту података у електронским системима.[222] Назив овог закона био је Закон о заштити података државе Хесе - *Hessisches Datenschutzgesetz*. Иако скроман по обиму, овај закон умногоме је утицао на каснију упоредно-правно регулативу у вези са заштитом података. То се

[219] Barton Gellman, Laura Poitras, „U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program“, *The Washington Post*, online 2013, *https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html?noredirect=on&utm_term=.712646f40b06*, 11. фебруар 2019.

[220] Dragan Prlja, Andrej Diligenski, *Fejsbuk i pravo*, Institut za uporedno pravo, Beograd 2014, 102.

[221] За више о Едварду Сноудену и његовом случају разоткривања кршења личних података и личних права, вид. Luk Harding, *Dosije Snouden*, Evrogiunti, Beograd 2014.

[222] Mina Zirojević, Zvonimir Ivanović, *Zaštita prava intelektualne svojine u sektoru informaciono-komunikacionih tehnologija*, Institut za uporedno pravo, Beograd 2016, 76

примећује већ по самом називу овог акта (Закон о заштити података), кога ће већина европских земаља прихватити у својим законодавствима.

Највећа вредност овог закона представља увођење независног тела које је контролисало законитост обраде и друга питања у вези са заштитом личних података. То је институција Омбудсмана за заштиту података (*Datenschutzbeauftragter*). Грађани ове државе могли су да се обрате омбудсману, који ипак није имао могућност доношења обавезујућих одлука, али је имао саветодавну улогу и усмеравао грађане ком надлежном органу јавне власти могу да се обрате у случају злоупотребе и неправилног коришћења личних података.[223] Закон се односио искључиво на органе управе савезне државе Хесе, будући да због специфичног административног положаја држава није могла да уређује сва питања у вези са заштитом података. Закон је садржао и институт који је и данас актуелан у модерном законодавству - права лица чији се подаци обрађују. Можемо рећи да је овај пропис оставио пионирски траг у изградњи правне заштите података о личности, као и то да је утицао на изградњу правног система заштите података у Немачкој.

Када говоримо о државним законима који уређују област заштите података, неопходно је поменути Шведску. Шведска представља прву европску државу која је законом на свеобухватан и систематски начин пружила заштиту личним подацима грађана. Закон о заштити података Шведске донет је 1973. године, након темељне анализе потреба грађана и тенденција развоја друштвених односа. Разлог за доношење оваквог закона налазио се у чињеници да је Шведска била држава са највише рачунара по глави становника, а припадала је безбедносно неутралним државама.[224] Развој информационо-комуникационих технологија захтевао је стварање централних регистара података који су се чували у поседу органа управе. Због тога се јавила и бојазан по неутралност Шведске, будући да су домаћи и страни елементи могли да дођу до база података, чиме би и неутралност Шведске била доведена у питање.

[223] Herbert Burkert, „Privacy - Data Protection a German/European Perspective“, *in Governance of Global Networks in the Light of Differing Local Values,* (eds. E. Christoph, K. Keeneth), Nomos: Baden-Baden 2000, 46.
[224] *Ibid.*, 48.

Шведски закон о заштити података увео је принципе на којима ће касније почивати и европско законодавство, а један од најзначајнијих принципа је тај да се јавни регистри личних података у поседу органа управе, као и обрада података коју врше ови органи налазе под надзором јавности, заинтересованих лица и посебних тела која се баве заштитом података. Дакле, принцип транспарентности промовисан је као један од стубова заштите личних података.

Законодавну праксу Шведске убрзо су прихватиле и остале скандинавске државе. Пет година касније, 1978. године, Данска, Норвешка и Аустрија усвојиле су своје законе којима су уредиле систем заштите личних података.[225] Исте године је и Француска усвојила Закон о информатици, евиденцијама и слободама,[226] који је уређивао област заштите личних података. Француски закон је установио специфично тело под називом Национална комисија за информатику и слободе (*Commission Nationale de L'informatique et des Libertes*),[227] које је имало регулаторна и контролна овлашћења. Национална комисија, у измењеном облику, и данас обавља важну улогу у француском систему заштите личних података. У годинама које следе и остале европске државе ће почети да регулишу област личних података.

На нивоу целе ЕУ, први важнији корак у циљу заштите личних података грађана ЕУ представљао је усвајање Директиве о заштити појединаца у вези са обрадом личних података и слободном кретању таквих података 24.10.1995. године. [228] Овај пропис представљао је први покушај да се уреди систем заштите личних података на нивоу ЕУ, при чему је Директива обухватала обраду свих личних података, независно од тога да ли се обрађују аутоматски или не. Систем заштите базиран је на три основна приниципа: принцип транспарентности,

---

[225] Изван европског континента Сједињене Америчке држава усвојиле су пропис у вези са заштитом личних података 1974. год. Вид. D. Milenković, *Pristup informacijama, zaštita podataka o ličnosti i tajnost informacija – Aktuelna pitanja zakonodavstva u Srbiji*, Komitet pravnika za ljudska prava, Beograd 2009, 64.

[226] Закон о информатици, евиденцијама и слободама - *Loi n° 78-17, relative à l'informatique, aux fichiers et aux libertés*, 6 janvier 1978.

[227] С. Лилић, „Право, информатичка технологија и заштита података", *Анали Правног факултета у Београду*, бр. 2-3/1989, Београд 1989, 220.

[228] Директива о заштити појединаца у вези са обрадом личних података и слободном кретању таквих података-Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23/11/1995 P. 0031 – 0050**.**

принцип легитимне сврхе обраде и принцип пропорционалности. Као важан механизам заштите предвиђено је независно надзорно јавно тело на нивоу држава чланица које обавља послове у циљу заштите личних података грађана.

Ипак, због правне природе Директиве, државе нису имале обавезу директне примене, већ су прихватале њена решења кроз национална законодавства. Такође, многи принципи, права и механизми нису уређени, па је остало отворено питање примене бројних института у области заштите података. Та и многа друга питања системски су решена доношењем Опште уредбе ЕУ, која је усвојена 2016. године, а почела је да се примењује 25. маја 2018. године. Овај пропис изазвао је много полемике у пракси, али је ипак на свеобухватан начин регулисао питања од значаја за правну заштиту личних података на територији ЕУ.[229]

2.4. Историјат правне заштите личних података у Србији

Зачеци регулисања заштите личних података на територији Србије датирају у доба Социјалистичке Федеративне Републике Југославије (у даљем тексту: СФРЈ).[230] Тадашња држава, у чијем је саставу била и Србија, није уређивала област личних података посебним прописом, али су основе система података биле присутне у уставним и законским текстовима.

Устав СФРЈ из 1974. године,[231] предвиђао је одређена правила у вези са друштвеним системом информисања. Овим Уставом предвиђено је да се „друштвеним системом информисања обезбеђује усклађено евидентирање, прикупљање, обрада и исказивање података и чињеница значајних за праћење,

[229] Основне критике Опште уредбе ЕУ односе се на велики број отворених клаузула које омогућавају државама чланицама да по сопственој вољи уреде конкретна питања, као и то да недостају додатни видови правне заштите грађана у вези са личним подацима. Nicolai Culik, „Brussels Calling: Big Data and Privacy", у *Big Data in Context- Legal, Social and Technological Insights*, (eds. T. Hoeren, B. Kolany-Raiser), Springer, online 2018, 31.

[230] У литератури се наводи да најранији траг права на приватност у Републици Србији сеже до Устава Краљевине Србије из 1888. године, где се у члану 15. гарантовала неповредивост стана, а у члану 23. неповредивост тајности писама и телеграфских депеша. Krivokapić Danilo *et al*, *Moji podaci, moja prava*, SHARE fondacija, Beograd 2018, 14. Ипак, сматрамо да на овај начин није пружена заштита подацима о личности, већ само приватност одређених сегмената живота грађана.

[231] Устав СФРЈ, *Службени лист* СФРЈ, бр. 9/74.

планирање и усмеравање друштвеног развоја, као и доступност информација о тим подацима и чињеницама“.[232]

Такође, важност података за друштво и тадашњи друштвено-политички систем препознат је у Закону о основама друштвеног система информисања и информационом систему Федерације.[233] Закон је у чл. 1. предвиђао да „Радници и други радни људи и грађани осигуравају у друштвеном систему информисања податке и информације неопходне за живот, рад и самоуправљање, за праћење, усмеравање и планирање друштвеног развоја, усклађивање односа у друштвеној репродукцији, вршење функција области и управљање другим друштвеним пословима“. Ипак, овај Закон није ближе уређивао питања заштите личних података, на начин како се то чини у савременим законодавствима.

Након тога, у новој држави, Савезној Републици Југославији, осим потврђивања Конвенције Савета Европе о заштити лица у односу на аутоматску обраду личних података из 1981. године, усвојен је и Закон о заштити података о личности 1998. год.[234] Циљ овог закона био је усмерен на усклађивање са поменутом Конвенцијом Савета Европе. Закон је уређивао искључиво заштиту података, али је пропустио да уреди питања прикупљања, обраде и коришћења личних података, са тенденцијом да се ова материја уреди посебним законима, што се никада није остварило.[235]

Надаље, у државној заједници Србије и Црне Горе, Повеља о људским и мањинским правима и грађанским слободама из 2003. године,[236] јемчила је право на заштиту података о личности. У тадашњем правном систему није постојало посебно право на заштиту података о личности, већ је заштита пружана у оквиру права на поштовање приватног и породичног живота. Предвиђена је санкција за употребу личних података у сврхе за које нису прикупљени. Такође, зајамчено је и право сваког да буде обавештен о прикупљеним подацима о својој личности.

---

[232] Чл. 75, Устава СФРЈ.
[233] Закон о основама друштвеног система информисања и о информационом систему Федерације, Сл. лист СФРЈ, бр. 68/81.
[234] Закон о заштити података о личности, Сл. лист СРЈ, бр. 24/98 и 26/98.
[235] Aleksandar Resanović, „Zaštita podataka o ličnosti u Srbiji i Crnoj Gori, odnosno u SR Jugoslaviji“, у *Zaštita podataka o ličnosti i poverljivi podaci – pravni aspekti*, Fond za otvoreno društvo, Beograd 2005, 52.
[236] Повеља о људским и мањинским правима и грађанским слободама, *Службени лист* СЦГ, бр. 6/2003.

Прикупљање, држање и коришћење личних података остављено је за уређивање посебним законом.[237]

У Републици Србији, као самосталној и независној држави, област заштите личних података уређена је на системски начин 2008. године, када је донет Закон о заштити података о личности (2008). Одредбе овог закона, од значаја за систем заштите података у електронској јавној управи сразмерно су обрађене и у овом истраживању. Овај закон замењен је Законом о заштити података о личности из 2018. године, који је усвојен на таласу европских и светских промена у области заштите података.

3. ЗНАЧАЈ ЗАШТИТЕ ЛИЧНИХ ПОДАТАКА

3.1. Друштвени контекст и значај заштите личних података

Питање значаја заштите личних података захтева сагледавања ширег друштвеног контекста. Развојем информационо-комуникационих технологија и посебно стварањем интернета, пре нешто више од 30 година (у Швајцарској, у познатој научној институцији ЦЕРН је 1991. године представљена прва интернет адреса, односно веб сајт), долази до структуралне промене друштва и друштвених односа.

Најзначајнији утицај на савремено друштво извршио је свеобухватни процес дигитализације. Пребацивање материјалних докумената, предмета и садржаја у електронски облик отворило је разне могућности за напредак многих друштвених области. Људи су добили шансу да брзо и лако комуникацирају без обзира на то где се налазе. Интернет, као светски систем умрежених рачунарских мрежа широм је отворио дигитална врата за цео свет,[238] чиме је подстакао развој нових идеја, бизниса, начина комуникације и размене информација. На тај начин многе активности и услуге постале су доступне кликом на једно дугме, било да је у питању мобилни телефон, рачунар или неки други електронски уређај.

[237] Чл. 24, ст. 4 и 5, Повеље о људским и мањинским правима и грађанским слободама државне заједнице Србије и Црне Горе.

[238] Према подацима, интернет данас користи чак 4,208,571,287 људи на Свету, што представља 55% од укупне светске популације. World Internet Users and 2018 Population Stats, *https://www.internetworldstats.com/stats.htm*, 26. септембар 2018.

Захваљујући таквим трендовима јављају се нове информационо-комуникационе технологије које у потпуности омогућавају коришћење интернета, од добијања информација о радном времену, реалном месту на коме се неко лице налази у датом тренутку, заказивање термина код органа управе, електронске трговине, итд. Такође, јављају се друштвене мреже које омогућавају размену идеја, слика, аудио и видео садржаја чиме стварају нову друштвено-електронску заједницу, нове обрасце понашања и идеја о улози појединца и друштва у новом електронском свету.

Учествовање у новим облицима дигиталне комуникације одвија се на основу размене информација и података. Велики део података који се размењује је личне природе. Отуда, заједно са употребом информационо-комуникационих технологија, интернета и друштвених мрежа порастао је и значај личних података у модерном друштву. Као што је за употребу моторних возила неопходно гориво да би оно могло да се креће, тако је за учествовање на друштвеним мрежама и интернету неопходно користити личне податке. У том смислу, можемо рећи да лични подаци представљају својеврсну „валуту“ за учествовање у електронским системима комуникације и модерним друштвеним дигиталним заједницама.

Лични подаци се користе у вези са кредитним и дебитним картицама приликом обављања новчаних трансакција, јединствени матични број грађана користи се приликом склапања купопродајних уговора и приступа електронским сервисима органа управе, здравствени картони приликом посете лекару и фармацеуту, подаци о пореклу као услов остваривања посебних социјалних права, број ципела приликом куповине истих, лична фотографија као средство идентификације, историја посета на веб претраживачима као доказно средство, итд. На основу тога, можемо рећи да поменути лични подаци представљају материјализацију личности грађана у правном животу.

Да би се омогућило нормално одвијање друштвених токова неопходно је да подаци буду сигурни и заштићени од злоупотреба и штетних утицаја трећих лица која немају право да буду упознати нити да користе без основа туђе личне податке. То се посебно односи на органе управе, будући да они рукују са великим бројем личних података грађана. Тиме се не остварује искључиво заштита личних података, већ и човека, као јединственог и непоновљивог бића.

3.2. Разлози установљавања правне заштите личних података

Установљавање правне заштите у некој области у вези су са друштвеним односима и интересима које треба заштити. Разлози због којих се установљава правна заштита личних података има више и они се могу груписати у три основне категорије. То су: заштита човекове личности, заштита државног и друштвеног интереса и заштита привредног интереса.[239]

Право тежи да заштити човека и његова лична добра од нежељених утицаја других лица. Као део човекове личности и лични подаци уживају правну заштиту. Можемо рећи да је у средишту заштите личних података сама човекова личност. Пружањем правне заштите личним подацима посредно се пружа заштита и другим основним људским правима и слободама, попут права на приватност, слободу, итд. Значај заштите личних података у савременом друштву осликава се у појави нових материјалних и процесних права у вези са личним подацима. Ова права налазе своја места у важним међународним документима и општим правним актима држава. Такав је случај и у правном систему Србије.[240]

Правном заштитом личних података остварују се и шири друштвени интереси. Обезбеђивањем безбедности личних података остварује се низ начела на којима се заснива функционисање државе. Основна начела, као што су слобода, једнакост и владавина права остварују се управо кроз заштиту појединца и његов слободан развој. Појединац и његови лични подаци могу бити сигурни једино у безбедном друштву које пружа заштиту свим својим члановима и њиховим добрима на једнак начин.

Глобализација, која је праћена свеопштим економским и друштвеним повезивањем, развила је потребу за разменом личних података. Такве појаве

---

[239] У односу на органе управе може се истаћи још један разлог, а то је досадашња лоша искуства у области заштите личних података. Овде се посебно истиче случај „цурења“ личних података из Агенције за приватизацију, где је јавности на интернету био доступан линк ка базама података чак 5 милиона грађана. Осим овог случаја, јавили су се проблеми и са апликацијом „Изабрани доктор“ у оквиру које је било бројних пропуста у вези са здравственим подацима грађана. Нав. према: D. Krivokapić (2018), 28.

[240] Ипак, иако су многи сегменти система заштите података регулисани, одређене значајне области остале су ван правног оквира. Тако, Србија нема Закона о видео-надзору, правила за прикупљање и обраду биометријских података, систем заштите за пресретање електронске комуникације, правила о чувању дигиталних података, правила о наслеђивању дигиталних података, и др. Александар Арсенин, *Приватност у 21. Веку – Заштита приватности и података о личности у информатичком добу*, Београд 2012, 88.

утичу на повећану размену личних података између приватних субјеката, али и држава, што је одраз сложености тржишта. Размена личних података између привредних субјеката представља део пословања ових лица, па је неопходно да таква размена буде брза и сигурна.

Потребе привредних субјеката да се могу поуздати у тржишне услове ствара потребу за заштитом интегритета свих учесника на тржишту, како би трговина и размена добара могле неометано да функционишу. За такво слободно функционисање тржишта неопходан је систем који ће штитити информације и личне податке који представљају део таквих размена. Због тога, заштитом личних података грађана штити се тржиште и слободна тржишна утакмица.

V ОСНОВНА НАЧЕЛА ЗАШТИТЕ И ПРАВА ГРАЂАНА У ВЕЗИ СА ПОДАЦИМА О ЛИЧНОСТИ У ЕЛЕКТРОНСКОЈ ЈАВНОЈ УПРАВИ

1. НАЧЕЛА ПРАВНЕ ЗАШТИТЕ ПОДАТАКА О ЛИЧНОСТИ

1.1. О начелима уопште

Сваки правни систем и подсистем заснива се на начелима која представљају основне принципе, основне вредности и полазишне тачке у разумевању његових правила. Начела представљају идеју водиљу и основно средство помоћу кога се попуњавају правне празнине и нејасна законска решења. То значи да све правне норме одређеног прописа морају бити у складу са начелима.

Начела налазе своје место у највишим правним прописима државног права, уставима и законима. Она су присутна и у међународним документима. Можемо правити разлику између оних начела која се односе на целокупан правни систем, па се примењују у свим посебним областима права и посебних начела, која важе само у појединој области правног регулисања. Начела која су заједничка за све гране и области правних система су начело законитости, начело правичности, начело једнакости, итд. Посебна начела су карактеристична за поједине правне области и заснивају се на специфичностима подсистема и материје које регулишу, попут начела предвидљивости и начела помоћи странци у управном праву.

Установљавање правне заштите података о личности подразумева одређене принципе на којима се темељи систем и конкретни облици правне заштите. Тако настају начела правне заштите личних података.

Правни систем заштите података заснива се на општим и посебним начелима. Општа начела у систему заштите података јесу начело законитости, правичности и истине. Посебна начела представљају основне вредносне идеје које су специфичне за област заштите података о личности. Она се морају поштовати приликом обраде података, доношењем одлука и предузимањем мера у вези са заштитом личних података. Свакако, она се примењују независно од тога да ли се закон односи на лица приватног права или јавног права.

1.2. Начела заштите података у правном систему Србије и правном систему ЕУ

1.2.1. Начела заштите личних података у ранијем законодавству Србије и ЕУ

У Србији, претходни Закон о заштити података о личности (2008) није одређивао основна начела заштите података, већ је једино садржао циљ закона. Основни циљ овог закона је био да се сваком физичком лицу обезбеди остваривање и заштита права на приватност и осталих права и слобода.[241] Међутим, циљ закона не може се изједначити са основним начелима на којима се заснива систем заштите личних података. Циљ закона представља разлоге због којих је пропис донет. Изостављање начела представља пропуст законодавца, будући да она представљају вредносне основе и идеје које служе онима који примењују пропис и онима на које се пропис односи. Начела помажу да се примена материјалних и процесних одредби и њихово тумачење одвија у одређеном вредносном оквиру којем је тежио законодавац приликом прописивања норми. Уз то, начела могу служити и приликом попуњавања правних празнина које се могу указати у пракси.

Са друге стране, европско законодавство садржало је основне принципе и у ранијим документима. Тако је Директива Европске уније о заштити података (1995)[242] предвиђала посебна начела заштите података. Директива је предвиђала да лични подаци морају бити обрађивани у складу са принципом законитости и поштења. Сврха обраде морала је бити одређена, јасна и легитимна како би били прикупљени само подаци који су адекватни и релевантни за утврђену сврху. Уведен је и принцип ограничења чувања података, будући да су они могли да се чувају онолико колико захтевају потребе обраде за конкретне сврхе, при чему је руковалац водио рачуна о примени поменутих начела.[243]

[241] Чл. 2, Закона о заштити податка о личности (2008).
[242] Директива о заштити појединаца у односу на обраду личних података и слободном промету таквих података- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data , Official Journal L 281 , 23/11/1995 P. 0031 – 0050.
[243] Вид. чл. 6, Директиве о заштити података ЕУ (1995).

1.2.2. Начела заштите личних података у актуелном законодавству Србије и ЕУ

Након неколико година важења поменутих прописа дошло се до закључка да је неопходно иновирати материјалне одредбе које уређују систем заштите личних података. Развој информационо-комуникационих технологија, структуралне промене у друштву и потреба за квалитетнијом заштитом личних података искристалисале су потребу за новим начелима, односно принципима на којима ће почивати систем заштите личних података. Та „нова“ начела прихваћена су у Закону о заштити података о личности (2018), као и у Општој уредби ЕУ. Оба прописа садрже идентичне принципе, што говори о усклађивању правног система Србије са правним тековинама ЕУ, као и потреби стандардног и истоветног приступа у уређењу поменутих питања у оквиру ЕУ.

Поменути прописи познају општа и посебна начела. Општа начела, она која се примењују у различитим гранама права, представљају основе читавог правног система, па тако налазе место и у области заштите података. Она општа начела која налазе примену у области заштите података јесу начело законитости, правичности и транспарентности.

Са друге стране, постоје посебна начела која важе искључиво у области заштите личних података. Она представљају посебне стубове на којима почива правна заштита личних података. Посебна начела система заштите података јесу начело коришћења најмањег обима података, начело ограничене сврхе обраде, начело тачности обраде, начело интегритета и поверљивости обраде и начело ограниченог броја разлога због којих се чувају подаци.

Ова начела уско су повезана са поменутим општим начелима, те се кроз њихову примену остварује сврха општих начела и обрнуто. Иако апстрактна по природи, посебна начела имају практичну примену и велики значај у примени норми које су усмерене на заштиту личних података.

2. ОПШТА НАЧЕЛА ЗАШТИТЕ ЛИЧНИХ ПОДАТАКА

2.1. Начело законитости

Начело законитости представља једно од основних принципа на којима се темеље правни системи, како у упоредном законодавству, тако и у Србији. Можемо рећи да право не би могло да остварује своју друштвену улогу без начела законитости, будући да се његова улога остварује помоћу општих и појединачних правних норми који се примењују у конкретним животним ситуацијама. Као основно начело, законитост је усмерена ка правилној примени правних норми и обезбеђивању функционалности правног система.

Принцип законитости може бити схваћен на неколико начина, у зависности од тога да ли се посматра шире или уже у односу на своју функцију. За законитост се наводи да „..у најширем смислу означава сагласност свих односних аката са законом као вишим актом. У нешто ужем смислу законитост означава да сви правни акти и све материјалне радње које предузимају државни органи и грађани јесу односно морају бити у складу са законом, морају се донети, односно вршити у складу и на основу закона као највишег правног акта. У најужем смислу, законитост значи да сви правни акти са мањом правном снагом јесу, односно морају бити, у складу и донети на основу правних аката с већом правном снагом“.[244] Независно од начина посматрања, основна сврха начела законитости јесте да усклади опште и посебне правне норме, да створи хијерархију правила више правне снаге и да то оствари у конкретним животним ситуацијама, путем појединачне правне норме.

Због своје правне природе начело законитости је од прворазредног значаја за функционисање и рад органа електронске управе. Основна сврха начела законитости у управном праву јесте да спречи самовољу органа управе и да њихове делатности и одлуке „стави“ под право. Законитост ствара двоструке везе између управе и грађана. Она иде за тим да органи управе поступају у свему

[244] Драган Митровић, *Увод у право*, Правни факултет Универзитета у Београду, Београд 2010, 360-361.

према правним нормама, али и да грађани поштују правне норме које их обавезују у односу према држави.[245]

Ипак, има и аутора који сматрају да начела нису *conditio sine qua non* управног права, а тиме и управних прописа. У том смислу се наводи да не постоји права потреба за основним начелима у законским текстовима, већ да њихова садржина треба да буде имплементирана у сваку норму тог прописа. Такође, повреда начела не води никаквој санкцији, тако да она више представљају „жеље“ и тежње законодавца које непотребно оптерећују прописе.[246]

У односу на управно право, начело законитости обично стоји заједно са начелом предвидљивости, које је усмерено ка остваривању извесности и сигурности управног поступања. Оно подразумева да се органи придржавају својих ранијих одлука у истоветним ситуацијама чиме се обезбеђује испуњење легитимних очекивања грађана и правних лица. Са друге стране, органи могу одступити од своје раније праксе, али то морају посебно да образложе у конкретној одлуци.

Такође, у управном праву, један од посебних циљева начела законитости јесте да дискрециono одлучивање стави под оквире права, на тај начин што ће свака управна одлука бити заснована на одговарајућем пропису, у граници овлашћења које пропис дозвољава, као и у складу са циљем због кога је овлашћење додељено. Ово је од значаја за обраде личних података које управни органи врше на основу дискрециone оцене.

У односу на систем заштите података, законитост значи да свака обрада мора да буде заснована на одговарајућим законским и подзаконским нормама. Оно штити од самовоље органа управе у односу на личне податке грађана.

Помоћу овог начела, правне норме се постављају изнад личне воље руковаоца и обрађивача података, односно управног органа. Такође, оно иде за тим да свака одлука буде заснована на пропису, да буде донета од надлежног органа и у складу са предвиђеним правилима поступка уз могућност улагања

[245] Д. Васиљевић (2012), 26.
[246] За више вид. Д. Милков (2017), 84-85. Чинећи осврт на начела управног права, аутор наводи и то да у аустријском и немачком Закону о општем управном поступку, као модерним прописима управног права не постоје начела.

правног средства или жалбе ради преиспитивања правилности и законитости одлуке или радње надлежног органа.

2.2. Начело правичности

У филозофији права, правичност је уско повезана са правдом, која се остварује правилном применом правних норми. Правда се може одредити као концепт моралног и исправног поступања доносиоца одлуке. Она тежи остваривању вредности истине и једнакости. У односу на тај појам, правичност се одређује као „правда појединачног случаја".[247] Наводи се да „без правичности, праведност не би у свим случајевима била задовољена, била би непотпуна, јер је правичност коректив позитивног прописа".[248]

У систему заштите личних података, начело правичности има истоветно значење. Она је усмерено на то да се опште правне норме примењују у складу са посебностима конкретног случаја. То је од посебног значаја у области личних података код којих се јављају многе посебности које се тичу лица, података, разлога обраде, итд. Сваки случај има своје посебности које се морају узети у обзир приликом одлучивања о правима, обавезама или правним интересима, што имплицитно утиче и на законитост обраде. Ово начело остварује се кроз дужност органа управе да оцењују све релевантне чињенице конкретног случаја и да их подведу под одговарајућу правну норму. Правни стандарди који се користе у систему заштите података захтевају процену и вагање различитих интереса и у конкретном случају, где треба имати на уму начело правичности.

Многа начела управног права, попут начела сразмерности, начела заштите права странака и остваривања јавног интереса, начела истине и других, остварују одређени однос са начелом правичности. Због тога, приликом обраде личних података, органи управе морају имати на уму поменута начела управног поступања, како би се остварио принцип правичности. Поменута начела једино у садејству остварују пуну практичну примену која се конкретизује кроз

[247] Gustav Radbruh, *Filozofija prava*, Nolit, Beograd 1980, 43.
[248] Laurenz Vuchetich, „Pravednost i pravičnost u filozofiji prava", *Pravnik: časopis za pravna i društvena pitanja*, 41 br. 2 (85), Pravni fakultet u Zagrebu (ur. Jerko Bulić), Zagreb 2007, 73.

појединачну обраду и одлуку која је утемељена на закону, а у складу је са чињеницама конкретног случаја.

2.3. Начело транспарентности

Начело транспарентности представља можда и најзначајније начело у вези са заштитом личних података у електронској управи. Обавештеност грађана и отвореност рада органа управе кључни су елементи за остваривање законитости обраде и безбедности личних података. Применом начела транспарентности остварују се принципи демократије, оснажује се учешће грађана у државном и друштвеном животу и повећава се одговорност носиоца јавне власти. Транспарентност подразумева јавност резултата рада свих лица која обрађују или врше друге активности у вези са личним подацима. Грађани добијају могућност да буду упознати са свим оним активностима које се односе на њихове личне податке, што подразумева одговоре на питања ко, на који начин, када и како употребљава личне њихове податке.[249]

Иако се транспарентност понекад изједначава са појмом отворености, ова два појма се разликују. „Отвореност и транспарентност омогућавају да сви заинтересовани грађани буду упознати са разлозима одређене управне одлуке или радње, а са друге стране, ови принципи омогућавају лакшу контролу управних делатности од другостепених органа".[250] Отвореност рада органа управе означава то да грађани имају увид у то како се одвија управни рад.[251] Последично, остварује се могућност грађана да реагују правним средствима на уочене грешке и недостатке у функционисању органа управе у вези са обрадама личних података. Зато се отвореност може посматрати као део начела транспарентности.

---

[249] Нове технологије омогућавају брзо ширење информација, па се тако грађани данас могу упознати са стварним стањем ствари у пракси и путем мобилних апликација, у оквиру којих грађани пријављују одређене грешке и кварове који спадају у надлежност органа управе. Тако се транспарентност, између осталог, остварује и кроз апликације за мобилне телефоне. Вид. S. Goldsmith, S. Cawford (2014), 27-29.

[250] Organization for Economic Co-operation and Development, *European Principles for Public Administration*, Sigma Papers, No. 27, online 1999, 11, *http://unpan1.un.org/intradoc/groups/public/documents/nispacee/unpan006804.pdf*, 11. јануар 2019.

[251] „Начело отворености подразумијева надзор јавне управе споља, док начело транспарентности да је управа сама по себи „прозирна", управо за потребе контроле споља". За више о начелу отворености вид. Јелена Старчевић, „Начело транспарентности у управном поступку", *Годишњак факултета у Источном Сарајеву*, год. VI, бр. 1/2015, Источно Сарајево 2015, 35.

Улога начела транспарентности у заштити личних података односи се на свако поступање органа управе у вези са личним подацима грађана. Такође, начело транспарентности остварује се и кроз навођење разлога због којих се доноси одређени акт или предузима појединa управна радња, односно зашто се предузима управни рад.

Уколико посматрамо уже, искључиво у односу на личне податке у поседу органа управе, можемо говорити о два облика начела транспарентности.[252] Први облик се односи на јавност рада органа у односу на личне податке грађана, на начин који је претходно изложен. Други облик односи се на обраде оних података који су од значаја за ширу друштвену заједницу, па се заштита заправо односи на могућност приступа заинтересованих лица тим подацима. У ову категорију можемо сврстати отворене податке и информације од јавног значаја. Они се обично налазе у поседу органа јавне власти, па се транспарентност остварује тако што органи имају дужност да обезбеде приступ заинтересованим лицима. У случају отворених података, то значи константан приступ базама података у поседу органа управе које су отворене и свима доступне, док у случају информација од јавног значаја морају да се испуне законски услови, при чему је неопходан захтев лица за приступ таквим информацијама. Остваривањем законских услова, заинтересованом лицу мора бити дозвољено да се упозна са садржином информације која је од јавног интереса.

Поменута подела је теоријске природе и има за циљ да класификује облик остваривања начела транспарентности у зависности од врсте података којима се приступа (лични подаци, отворени подаци и информације од јавног значаја). Остваривање увида у личне податке представља један, али јако важан сегмент начела транспарентности. Суштински посматрано, начело транспарентности у области личних података, односи се искључиво на обраду и заштиту личних података, где се остварује кроз посебна права грађана у вези са заштитом личних података.

[252] Упор. Ј. Старчевић (2015), 36.

3. ПОСЕБНА НАЧЕЛА ЗАШТИТЕ ЛИЧНИХ ПОДАТАКА

Посебна начела заштите података представљају посебне принципе заштите личних података којима органи управе треба да се руководе приликом обраде података грађана.[253] Она су усмерена на обраду најмањег могућег обима података, ограничење сврхе обраде, тачност обраде, интегритет и поверљивост обраде и ограничење разлога због којих се подаци чувају.

Посебна начела уско су повезана са поменутим општим начелима транспарентности, законитости и правичности. Због тога, можемо рећи да примена посебних начела осигурава поштовање општих начела и обрнуто, чиме правни систем заштите података добија стабилне темеље који гарантују грађанима адекватну правну заштиту.

3.1. Начело употребе најмањег могућег обима података

Начело употребе најмањег могућег обима података значи да орган управе (као руковалац или обрађивач) не сме постављати непримерене захтеве грађанима у вези са прикупљањем и обрадом личних података, тако да они превазилазе сврху обраде. Када постоји потреба за обрадом личних података у управном поступку, орган може захтевати и приступити само оним подацима који су од суштинске важности за циљ обраде. Такође, неопходност се односи и на обим података који се обрађују, тако да се у неким ситуацијама могу обрађивати само одређени сегменти личних података.

Начело употребе најмањег могућег обима података у праву Србије и упоредном законодавству познато је под термином „минимизација података“. Минимизација података означава да подаци о личности који се обрађују морају бити примерени, значајни и ограничени на оно што је неопходно утврдити у односу на сврху обраде.[254] Можемо рећи да се ово начело састоји од три кључна

[253] Посебна начела одређују се и као „принципи квалитетних података“. Према: P. Lambert (2017), 136.
[254] Чл. 5, ст. 1, тач. 3, Закона о заштити података о личности (2018), и чл. 5, ст. 1, тач. 3, Опште уредбе ЕУ.

елемента. То су примереност, значај и ограниченост обима обраде.[255] Ове елементе орган управе мора образложити на захтев лица чији се подаци обрађују, иначе обрада није у складу са принципом законитости.

Појам примерености односи се на границу довољне количине личних података која омогућава остваривање предвиђене сврхе обраде. Значај, односно релевантност података подразумева неопходну везу између личних података који се обрађују и сврхе обраде. Ограниченост се односи на обраду и значи да се подаци могу користити само у прикупљене сврхе обраде, док би обрада у друге сврхе била противправна. Изостављање неког од наведених елемената значило би повреду начела коришћења најмањег могућег обима података.

Примена овог начела од великог је значаја за обављање послова органа управе. Примера ради, орган пореске управе може прикупити податке о имовини више лица са истим личним именом у циљу утврђивања одређене фискалне обавезе. У процесу обраде података орган ће установити лице коме треба утврдити обавезу, док податке о имовини осталих лица нема право да обрађује. Ипак, орган може задржати основне податке о осталим лицима како би се спречила забуна између лица којем се утврђује обавеза и њих. Међутим подаци морају бити примерени и довољни само да би се спречила конфузија у сличним ситуацијама.

Такође, може се јавити обавеза послодавца да чува податке о крвним групама појединих запослених на ризичним пословима који могу угрозити здравље и безбедност запослених. Ови подаци су неопходни за спречавање настанка штетних последица у ванредним ситуацијама које се могу десити обављањем тих послова, што чини одговарајући и адекватан правни основ за чување осетљивих података. Ипак, подаци могу се користити, односно обрађивати искључиво у ванредним ситуацијама када је неопходно заштитити живот и здравље запослених на високо ризичним радним местима.[256]

---

[255] Поједини аутори другачије одређују поменута три елемента, па наводе да се начело минимизације података састоји од елемената пропорционалности обраде, неопходности обраде и нужности обраде података. A. Diligenski, D. Prlja, D. Cerović (2018), 82.

[256] Упор. UK Information Commissioner's Office, Principle (c): Data minimisation, *https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/*, 22. септембар 2018.

3.2. Начело ограничене сврхе обраде

У директној вези са начелом коришћења најмањег могућег обима података стоји начело ограничене сврхе обраде. Свака обрада личних података мора се заснивати законитој и легитимној сврси због које се подаци обрађују. Сврха обраде говори због чега, односно из ког разлога се предузима обрада. Разумно је очекивати да се обрада података не може вршити самовољно, већ једино због циља који је законит, односно оног циља који оправдава увид органа управе у личне податке грађана. Због тога, модерни правни системи, међу којима су и правни системи Србије и ЕУ, предвиђају принцип којим ограничавају и оправдавају разлоге обраде личних података.[257]

Начело ограничене сврхе обраде значи то да се прикупљање личних података може вршити само на основу законских разлога. Орган може вршити обраду само у односу на одређене, изричите и оправдане сврхе. Одређеност сврхе значи да орган мора вршити делатности у вези са којима су му потребни лични подаци грађана. Лични подаци не могу се прикупљати пре него што се јави потреба за њиховом обрадом. Прикупљање података без одређене сврхе је противправно. Када се укаже потреба, орган мора тачно одредити због чега се подаци прикупљају и обрађују. Изричитост, као елемент обраде, означава то да орган мора на јасан и разумљив начин упознати лице чији се подаци обрађују са сврхом обраде. Органи управе не могу сакрити разлоге због којих обрађују личне податке, што значи да не могу давати апстрактне и неодређене разлоге за прикупљање и обраду података. Оправданост значи да објективно постоји законска потреба за прикупљањем и обрадом личних података грађана.

Ограничење сврхе обраде значи и то да се подаци не могу користити и обрађивати у другачије сврхе од оних због које су првобитно прикупљени. Ипак, лични подаци могу се обрађивати у нове сврхе уколико су оне у складу са сврхом ради које су првобитно прикупљени (што мора бити посебно образложено), уколико постоји пристанак на нову обраду лица чији се подаци обрађују или ако

[257] Чл. 5, ст. 1, тач. 2, Закона о заштити података о личности (2018), и чл. 5, ст. 1, тач. 2, Опште уредбе ЕУ. За више о настанку принципа ограничене сврхе обраде вид. Nikolaus Forgó, Stefanie Hänold, Benjamin Schütze, „The Principle of Purpose Limitation and Big Data“, у: *New techonolgy, Big Data and the Law* (ed. Marcelo Corrales, Mark Fenwick, Nikolaus Forgó), Springer, Singapore 2017, 22-25.

је могућност нове обраде предвиђена посебним законом. Уз то, обрада се може накнадно предузети ради задовољења одређеног појавног облика јавног интереса. То је случај са обрадом података која се врши у интересу историјских истраживања, истраживања научних или статистичких делатности, што предвиђају Општа уредба ЕУ, као и Закон о заштити личних података (2018). Ради остваривања законитости и правне сигурности, грађани морају бити обавештени о измењеној сврси обраде, што орган мора посебно и јасно образложити.

3.3. Начело тачности

Свака истина заснива се на чињеницама. У том маниру, можемо рећи да се свака правилна обрада мора базирати на тачним личним подацима. Овај став посебно је значајан код обраде коју врше органи управе, јер од тачности обраде зависи одлука у конкретном случају, што има директног утицаја на правни статус и права грађана.

Начело истине је нашло своје место и у правилима општег управног поступка.[258] Тако, Закон о општем управном поступку предвиђа да је орган дужан да правилно, истинито и потпуно утврди све чињенице и околности од значаја за законито и правилно поступање у управној ствари.[259] Од великог значаја за сваки управни поступак и правни систем је да се обрада личних података врши на основу истинитих и тачних података, будући да се једино тако могу остваривати основни принципи управног права. У складу са тим, прописи који уређују систем заштите података у његове темеље постављају начело тачности.[260]

Начело тачности односи се на саму обраду података, али и на орган који обрађује податке. Подаци који се складиште у базама података морају бити ажурирани и усклађивани у односу на промене чињеничног стања.[261] У пракси,

[258] „У (управном) поступку се морају правилно и потпуно утврдити све чињенице и околности које су од значаја за доношење законитог и правилног решења (одлучне чињенице)“. С. Лилић (2013), 448.
[259] Чл. 10, ст. 1, Закона о општем управном поступку.
[260] Чл. 5, ст. 1, тач. 4, Закона о заштити податак о личности (2018), и чл. 5, ст. 1, тач. 4, Опште уредбе ЕУ.
[261] Paul Voigt, Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR)- A Practical Guide*, Springer, eBook, online 2017, 91.

ово начело треба да буде примењено тако да орган предузме све одговарајуће мере које омогућавају константну тачност и истинитост података који се обрађују.

Појам тачности значи да орган управе мора прецизно водити податке о личним подацима грађанима у свом поседу. Примера ради, уколико неко лице промени место пребивалишта из једног града у други, у оквиру исте државе, податак који говори да лице има пребивалиште у граду из којег се преселио није тачан, па га треба ажурирати и изменити. Са друге стране, тачан је податак да је лице имало претходно пребивалиште у првобитном месту становања, па тај податак не треба мењати.[262]

Начело тачности своју примену налази и у случајевима када се чува податак за који је утврђено да није тачан. Чување нетачног података може бити легитимно и потребно ради заштите интереса лица на кога се подаци односе. Примера ради, медицински картон одређеног лица може да садржи податак о дијагнози која је дата, али за коју се касније испоставило да није тачна. Тај податак ће се чувати иако је нетачан, будући да је од значаја за даље лечење тог лица и успостављање правилног поступка лечења. Ипак, неопходно је направити напомену о нетачности таквог податка и разлоге због којих је утврђено да је он нетачан.[263]

Ради остваривања овог начела, органи управе имају дужност да повремено проверавају тачност похрањених личних података до чије промене може доћи протеком времена. Будући да је то од значаја за лица чији се подаци чувају, и сами грађани морају показати заинтересованост за измену њихових нетачних података.[264]

---

[262] Упор. UK Information Commissioner's Office, Principle (d): Accuracy, *https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/*, 22. септембар 2018.

[263] *Ibid*.

[264] Таква иницијатива је неретко постављена као правило, будући да органи управе не могу водити рачуна о промени података свих грађана, будући да се ради о великом броју информација. То је случај са променом пребивалишта или боравишта грађана, чију измену они сами морају да пријаве надлежном органу. Иста је ситуација и са променама породичног статуса грађана (промена презимена и слично).

3.4. Начело интегритета и поверљивости података

Начело интегритета и поверљивости података односи се на органе управе који морају осигурати низ неопходних мера како би обрада била сигурна и како подаци не би били злоупотребљени или незаконито јавно објављени. Управни органи морају вршити обраду личних података на законит начин који подразумева примену техничких и организационих мера у циљу спречавања губитка, оштећења или других грешака које могу настати обрадом података.[265] Обрада мора бити затвореног типа, а резултати обраде и сами подаци морају се осигурати посебним мерама које штите од приступа и злоупотребе других лица (чак и од неовлашћених лица у оквиру истог органа), чиме се остварују поверљивост и интегритет обраде, као вредностима сваког система заштите личних података.[266]

Приликом обраде личних података управни органи долазе до значајних информација о животу лица чији се подаци обрађују. Уколико би ти подаци били изгубљени, уништени или злоупотребљени од стране трећих лица, могле би настати значајне негативне последице по права и интересе грађана. У модерном информационом друштву, лични подаци могу се злоупотребити на различите начине. Тако је могућа замена идентитета, недозвољене електронске новчане трансакције, објављивање строго поверљивих личних података, лажно пријављивање, итд. Како би се спречиле негативне последице по појединце и друштво, прописи установљавају системе заштите података који се заснивају на правним, организационим, техничким и информатичким мерама које треба да пруже заштиту од сваког вида злоупотребе.

Можемо закључити да се принцип интегритета и поверљивости највише остварује кроз механизам информационе безбедности чији је циљ да „осигура континуитет пословања (обраде) и потпуно смањи штету по пословање спречавајући и смањујући могућност безбедносних инцидената“.[267]

---

[265] Чл. 5, ст. 1, тач. 6, Закона о заштити података о личности (2018), и чл. 5, ст. 1, тач. 6, Опште уредбе ЕУ.
[266] P. Voigt, A. Bussche (2017), 92.
267 Rossouw von Solms, „Information security management: why standards are important“, *Information Management & Computer Security*, 7/1, MCB UP Ltd., UK 1999, 56.

3.5. Начело временског ограничења чувања података

Начело временског ограничења чувања података усмерено је на то да се поставе временске границе чувања личних података, искључиво на време које је заиста потребно да се изврши обрада. Када је испуњена сврха ради које су подаци прикупљени и обрађени, нестаје и потреба за чувањем података, па даље чување и губи законитост. Увођењем овог начела у систем заштите података тежи се ограничавању могућности чувања и коришћења туђих личних података.

У систему заштите личних података Србије и ЕУ, ово начело упућује на то да се подаци о личности морају чувати у облику који омогућава идентификацију лица и то само у временском периоду који је неопходан да се оствари сврха обраде.[268]

То значи да орган управе нема право да чува личне податке колико он жели, већ само онолико колико су му потребни за остварење сврхе обраде. Даље, ово начело имплицира да мора постојати сврха због које се подаци чувају одређено време, што установљава обавезу органа да повремено врши преглед података како би обрисао оне податке који му више нису неопходни. Примера ради, орган управе као послодавац треба да изврши проверу личних података запослених који су напустили органе управе ради вршења нове систематизације радних места. Орган не сме да чува све податке о бившем запосленом зато што је сврха ради које су се подаци чували отпала. Међутим, орган управе ће моћи да задржи поједине личне податке у вези са запослењем који ће му бити потребни за регулисање, примера ради, пензионог стажа. Сви остали подаци који се неће користити, морају се обрисати.[269]

Поступање у складу са овим начелом налаже потребу да се бришу подаци у поседу органа који више нису неопходни, што смањује могућност злоупотребе, застарелости и нетачности података који се чувају. Такође, ово начело доприноси и лакшем раду управних органа, који брисањем података за којима више не постоји потреба, смањује трошкове и ангажоване ресурсе свог пословања. Када

268 Чл. 5, ст. 1, тач. 5, Закона о заштити података о личности (2018), и чл. 5, ст. 1, тач. 5, Опште уредбе ЕУ.

269 Упор. UK Information Commissioner's Office, Principle (e): Storage limitation, *https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/*, 22. септембар 2018.

нестане потреба за чувањем личних података орган може обрисати податке или их учинити анонимним и као такве користити у статистичке или друге сврхе. Брисање података подразумева и брисање свих трагова у вези са подацима, као што је случај са метаподацима, како би се максимално смањила могућност злоупотребе.

Начело временског ограничења чувања података сусреће се са одређеним питањима у вези са пословима и дужностима органа управе. Због великог броја правних односа између државе и појединца, као и права и обавеза који проистичу из тих односа, није реално очекивати да се сви подаци у поседу органа управе могу брисати.

Многе личне податке грађани добијају од државе, односно управних органа, због правно релевантне везе појединца са државом (подаци о држављанству, здравствени картон, подаци из социјалне сфере, итд). У таквим ситуацијама, органи управе „установљавају“ личне податке које не могу брисати на захтев грађана, све док конкретно лице има правно релевантне везе са државом због којих су подаци и установљени, иако они суштински припадају грађанима. Због тога, ово начело има своја ограничења у односу на податке у поседу органа управе, јер посебни управни закони обавезују на чување појединих врста података по службеној дужности.

У случају чувања и обраде личних података коју врше органи управе, неопходно је дозволити приступ само појединим запосленима, који имају стварну, легалну и конкретну потребу за одређеним подацима и то у одређеном временском периоду. Неовлашћеним лицима мора се ускратити приступ подацима који им не требају у вршењу делатности како би се избегле злоупотребе службеног положаја и кршење приватности грађана. Према томе, ово начело је од великог значаја за заштиту личних података који се налазе у поседу органа управе.

3.6. Начело одговорности руковаоца

Како би систем могао да остварује заштитну функцију, неопходно је установити права и обавезе свих лица која учествују у процесу обраде. У том правном односу учествују лице чији се подаци обрађују (физичка лица) и лице које обрађује податке (нпр. органи управе). У области заштите података ово лице се назива руковаоцем. Руковалац је физичко или правно лице, орган јавне власти, агенција или друго тело које само или заједно са другима одлучује о сврхама и средствима обраде података о личности.[270] Уколико неко тело обрађује податке у име руковаоца, оно се назива обрађивачем података. То значи да се орган управе може наћи како у позицији руковаоца, тако и у позицији обрађивача.[271]

Будући да руковалац управља туђим личним добрима (личним подацима), он је одговоран за правилност и законитост обраде, као за и евентуалне последице настале у вези са обрадом. Због тога, правни системи заштите личних података Србије[272] и ЕУ[273], као једно од основних начела предвиђају одговорност руковаоца за правилност обраде личних података. Ово начело је новијег датума будући да ни Закон о заштити података о личности (2008), као ни Директива о заштити података (1995) нису садржали експлицитно овај принцип.

Појам одговорности у општем смислу односи се „на поступање према правилима које прописује нека друштвена норма…При коришћењу појма одговорност, прва асоцијација је да нешто није извршено од стране некога, а постојала је обавеза да се то уради“.[274] У односу на општи појам, можемо закључити да у правном смислу одговорност значи поступање према предвиђеним правним нормама и сношење последица због њиховог непоштовања.

---

[270] A. Diligenski, D. Prlja, D. Cerović, (2018), 65.

[271] „Пример: Јавно предузеће „Београд воде“ из разлога недостатка пословног простора закључи уговор са градском управном Града Београда ради чувања документације у архиви Града Београда. У односу на документацију која садржи одређене податке о личности „Београд воде“ ће бити руковалац, а градска управа Града Београда ће бити обрађивач, с обзиром да је уговором предвиђен да ће за „Београд воде“ чувати документацију у својој архиви. Нав. према: Д. Кривокапић *et al*. (2016), 17.

[272] Чл. 5, ст. 2, Закона о заштити података о личности (2018).

[273] Чл. 5, ст. 2, Опште уредбе ЕУ.

[274] Александра Илић Петковић, Миле Илић, „Одговорност државних службеника и заштита њихових права“, *Годишњак Педагошког факултета у Врању*, 1/2017, (ур. Сунчица Денић), Педагошки факултет у Врању, Врање 2017, 94.

Према томе, начело одговорности у вези са заштитом података установљава општу обавезу органа које обрађује податке да поштује предвиђене норме и правилност обраде. У односу на органе управе, то значи да надлежни орган (руковалац) мора у потпуности да усклади своје пословање са општим прописима који уређују заштиту података и прописима управног поступања, као и да буде у могућности да докаже усклађеност обраде са тим правилима. Усклађеност подразумева примену правних, техничких и организационих мера које су неопходне ради заштите личних права грађана и њихових личних података. Принцип одговорности подразумева дужност органа управе да континуирано води рачуна о личним подацима грађана у њиховом поседу, али и да води рачуна о развоју технологије и безбедносних мера електронске заштите.

Ова начело превасходно је усмерено ка побољшању позиције грађана и њихових личних података који сада знају коме могу да се обрате уколико се појави неки проблем са њиховим личним подацима. На овај начин, у посебној управној области заштите података, имплементира се начело предвидљивости управног рада и начело заштите права странака и остваривања јавног интереса. Органи управе не могу избећи одговорност за личне податке грађана који се налазе у њиховом поседу. Због тога је од посебне важности да се подзаконским општим правним актима уреде сва питања од значаја за заштиту личних података. Једино на тај начин органи управе могу ускладити свој рад са правилима прописа који уређују заштиту података.

Усклађеност пословања подразумева примену адекватних мера заштите личних података. То је фактичко питање које зависи од могућности органа и осетљивости личних података које треба заштити. Усклађеност подразумева и транспарентан рад органа јавне управе. Вођење евиденција о личним подацима, обрадама и потенцијалним изазовима побољшава усклађеност са прописима. У одређеним случајевима, усклађеност ће захтевати и именовање лица за заштиту података у оквиру органа чија ће основна дужност бити праћење предвиђеног и практичног односа заштите личних података.

***

На основу изложеног можемо закључити да су начела система заштите података основне полазишне тачке које гарантују закониту и правилну обраду личних података. Она делују према свим учесницима у поступку чувања и обраде личних података, тако што усмеравају руковаоце и побољшавају позицију оних чији се подаци обрађују.

Истоветност начела у праву Србије и ЕУ говоре о значају личних података, али и потреби грађана, без обзира где се налазили, да уживају правну заштиту своје личности, односно података. Приметна је и повезаност општих правних начела и посебних начела у материји личних података, које најбоље резултате остварују у заједничком деловању и примени. То се посебно односи на органе управе, који морају да воде рачуна о начелима управног права и начелима заштите података. Ипак, начела представљају норме апстрактног карактера која своју примену у пракси остварују кроз конкретна права грађана у вези са заштитом личних података у односу на органе управе.

4. ПРАВА ГРАЂАНА У ВЕЗИ СА ЛИЧНИМ ПОДАЦИМА

Модерне државе гарантују грађанима бројна лична права чиме остварују демократске вредности, принципе правне државе и владавине права. Људска права представљају основни елемент заштите грађана од недозвољеног мешања других у њихов приватни живот. У области заштите личних података проналазимо посебна људска права.

Обезбеђивањем безбедности личних података штите се и основна људска права. Повредом личних података не долази само до повреде података, већ долази до повреде права личности и низа посебних права које правни системи теже да заштите. Зато, људска права представљају окосницу система заштите података, а своје постојање заснивају на општим и посебним начелима.

Лична права су део породице грађанских права којима се штити јединственост и непоновљивост човекове личности. Њихов циљ јесте да омогуће слободан развој појединца у друштву, омогућавајући му испољавање свих посебности које га одликују као човека. Због тога, она представљају један од основних постулата демократских друштава. Лична права су „субјективна права

на личним добрима, као што су: право на живот, физички интегритет, здравље, психички интегритет, пијетет, достојанство, част, углед, приватни живот, лик, глас, лични запис, тајну сферу, личне податке, идентитет, име и др. Она омогућавају имаоцу да своје лично добро оствари, уживајући га и располажући њиме.“[275] Њихов основни циљ је да заштите појединца и његова лична добра од неовлашћеног утицаја свих трећих лица. На тај начин се остварује слободно уживање и располагање личним добрима у правном систему.

Непосредан објекат заштите личних права јесу лична добра. Како човек представља комплексно биће, тако је и круг личних добара човека којима се пружа заштита широк. За лична добра можемо речи да представљају оне вредности које су тесно повезане са човеком и његовом личношћу. При томе је важно имати на уму да свако лично добро припада одређеном лицу.

У теоријском смислу, могуће је класификовати две групе личних добара, у зависности од начина манифестовања у спољном свету. У прву групу спадају она лична добра која су саставни делови (елементи) личности, док у другу групу спадају добра која су опредмећени изрази лица.[276] Лична добра као што су живот, глас, достојанство, емоције припадају првој групи личних добара. Другу групу чине добра попут слика, аудио и видео записа на којима се налази одређено лице, итд.

Лични подаци представљају лично добро човека које представља саставни део његове личности. Њега треба разликовати од облика на коме или у коме је манифестован, као што је то случај са личним документима (лична карта, возачка дозвола) будући да документи представљају писмена које садрже информацију о одређеним личним подацима грађана (националност, годину рођења, и томе слично.).

Прописи обично наводе лична права грађана, али не затварају њихов круг, будући да се њихов број у данашњим околностима непрестано повећава. Понекад, лични подаци заштићени су заједно са другим личним добрима, па представљају предмет заштите права које штити посебан скуп личних добара. Такав је случај са

[275] Обрен Станковић, Владимир Водинелић, *Увод у грађанско право*, Номос, Београд 2007, 120.
[276] *Ibid*., 121.

правом на приватност, које је предвиђено у Универзалној декларацији о људским правима и Европској конвенцији за заштиту људских права и основних слобода.

Са друге стране, поједини прописи предвиђају право на заштиту личних података као посебно људско право, које је сложено и које се састоји из низа овлашћења гарантованих његовом имаоцу.[277] Такав је случај са правним системом Србије који гарантује право на заштиту личних података. Исто је учињено и у Општој уредби ЕУ.

Ипак, право на заштиту личних података није одувек представљало посебно лично право. Потреба за установљењем овог права расла је заједно са повећањем улоге личних података. Због тога, можемо рећи да је право на заштиту личних података изведено из права на приватност. Ради разумевања права на заштиту личних података аутор ће анализирати и право на приватност, као темељ права на заштиту личних података.

4.1. Право на приватност

Право на приватност представља врсту личних права. Оно је повезано са многим другим личним правима, али је можда у најближој вези са правом на живот.[278] Право на приватност присутно је у упоредно-правним системима, па се у англосаксонским правним системима користи термин „*Right to privacy*“, у француском праву „*droit au respect de la vie*“, у немачком праву„*Recht auf Privatheit*“ ili „*Recht auf Privatsphäre*“, итд.[279]

Основу овог права представља лична сфера појединца која се представља појмом приватности. Под приватношћу подразумевамо личну, ограничену и затворену сферу појединца у оквиру које он суверено одлучује и коју својевољно испуњава животним садржајем. У том смислу, можемо рећи да појам приватности искључује било какво присуство других лица у уређивању личне сфере.[280]

---

[277] Vladimir Vodinelić, „Sloboda medija kao granica zaštite podataka (medijska privilegija)“, *Zaštita podataka o ličnosti i poverljivi podaci – pravni standardi*, Fond za otvoreno društvo, Beograd 2005, 70.

[278] Право на живот, као лично право, гарантује сваком појединцу да живи и свој живот уређује онако како он то жели, слободно и самовољно, све док тиме не угрожава права и слободе других.

[279] Marija Boban, „Pravo na privatnost i pristup informacijama u suvremenom informacijskom društvu“, *Zbornik radova Pravnog fakulteta u Splitu* 3/2012, Split 2012, 582.

[280] У свету електронских информационих технологија и све присутније улоге државе у различитим сегментима друштвеног живота, појам приватности се мења. Јављају се изузеци од општег искључења јавности из сфере приватног. У зависности од области друштвеног живота, укључење

Супротно од појма приватности налази се појам јавности. Јавност можемо разумети као сферу друштвеног живота у којој долази до појављивања и умрежавања различитих приватних и друштвених интереса, активности и потреба које су познате или су доступне свима лицима или већини.

Право на приватност је строго лично право, будући да се његово уживање и коришћење не може пренети на другога. Оно је широко и обухвата различите аспекте човекове личности и личних добара, па се неретко у прописима и теорији врши његово разграничење на ужа права.

Као теоријски концепт, право на приватност потиче од „права да се буде остављен на миру“ (*right to be left alone*), које су конципирали америчке судије *Samuel Warren*-а і *Louis Brandais*-а, крајем 19. века.[281] Од тада, приватност постаје све важније лично добро и предмет интересовања правне теорије и праксе. „Приватност грађана у савременом свету постаје питање слободе живљења. Навика да свој дигитални траг немарно остављамо за собом није ништа ново... Личне податке нам узимају свакодневно, фотокопирају нам личне карте, а често нас пописују и класификују уз нашу сагласност. Свест грађана о личној приватности је на ниском нивоу, а одговорност институција које прикупљају и обрађују податке постоји у ретким случајевима, на шта званичници упозоравају. Када генерално сагледамо проблем, можемо закључити следеће: мотивисати човека да се бори за приватност је изазов модерног друштва, и уједно, решење проблема“.[282]

трећег лица или јавности у одређену приватну сферу правда се различитим интересима као што су јавно здравље, национална безбедност, друштвени ред, итд.

[281] П. Димитријевић, „Правна регулација електронске комуникације и право на приватност, *Зборник радова Правног факултета Универзитета у Источном Сарајеву* (ур. Горан Марковић), Правни факултет у Источном Сарајеву, Источно Сарајево 2011, 202.

[282] Александар Арсенин, *Приватност у 21. веку – Заштита приватности и података о личности у информатичком добу*, Београд 2012, 96.

4.2. Право на приватност у међународним документима

4.2.1. Право на приватност у Универзалној декларацији о људским правима

Један од најважнијих међународних докумената у вези са људским правима јесте Универзална декларација о људским правима из 1948. године.[283] Овај документ усвојила је Генерална скупштина Уједињених нација са циљем да људска права учини универзалним и доступним свима. Значај права на приватност препознато је већ у преамбули која наводи разлоге доношења Декларације. У преамбули се наводи: „пошто је признавање урођеног достојанства и једнаких и неотуђивих права свих чланова породице темељ слободе, правде и мира у свету,… пошто је стварање света у којем ће људска бића уживати слободу говора и убеђења и бити слободна од страха и несташице проглашено као највиша тежња сваког човека... пошто су одлучили (народи Уједињених нација) да подстичу друштвених напредак и побољшају услове живота у већој слободи...“.[284]

У члану 12. Декларације зајамчено је право на приватност. Прописано је да нико не сме бити изложен произвољном мешању у приватни живот, породицу, стан или преписку, нити нападима на част и углед, при чему свако има право на законску заштиту од таквог мешања или напада.[285] Према овој одредби приватност се схвата као једна од основних вредности појединца и стоји у рангу са породичним животом и приватном својином. Обавеза је држава Уједињених нација да пруже законску заштиту приватности свих лица. Ипак, Декларација не гарантује потпуну слободу од мешања у приватни живот, већ само слободу од „произвољног мешања“. Овај правни стандард дозвољава различита тумачења. Ипак, треба имати на уму да је овај документ декларативног карактера и да је његова основна тежња да промовише најважнија људска права и слободе на универзалан начин.

[283] Универзална декларација Уједињених нација о људским правима, Организација Уједињених Нација, 217 (III) , од 10. децембра 1948 год., Париз.
[284] Вид. Увод (преамбулу) Универзалне декларације о људским правима.
[285] Вид. чл. 12, Универзалне декларације о људским правима.

4.2.2. Право на приватност у Међународном пакту о грађанским и политичким правима

Право на приватност нашло је своје место и у Међународном пакту о грађанским и политичким правима из 1976. год.[286] Овај међународни уговор усвојен је 16. децембра 1966. године, од стране Генералне скупштине Уједињених нација. Пакт је усмерен на заштиту основних грађанских и политичких права појединаца. Одредба у вези са правом на приватност истоветна је са оном предвиђеном у Универзалној декларацији о људским правима. Пакт превиђа да нико не може бити изложен произвољном или незаконитом мешању у приватни живот, породицу, стан или преписку, нити противзаконитим нападима на част и углед.[287]

Државе потписнице овог пакта дужне су да законом осигурају заштиту од незаконитог или произвољног мешања или нападања приватности појединца. Све што је претходно изложено за Универзалну декларацију у вези са правом на приватност, важи и за Међународни пакт.

4.2.3. Право на приватност у оквиру Савета Европе

Право на приватност препознато је и на нивоу Савета Европе. У Декларацији скупштине Савета Европе која се тиче масовних медија, људских права и приватног живота појединца,[288] предвиђа се и право на приватност. Право на приватност суштински састоји се из права појединца да живи са минимум утицаја са стране. Ово право тиче се приватног, породичног живота у дому, физичког и моралног интегритета, части и угледа, недопуштености клеветања, недопуштености изношења ирелевантних и изненађујућих чињеница, неовлашћеног објављивања приватних фотографија, заштите од објављивања информација које су као тајне саопштене другима.[289]

---

[286] Међународни пакт о грађанским и политичким правима, *Службени лист* СФРЈ, (Међународни уговори), бр. 7/1971.
[287] Чл. 17, Међународног пакта о грађанским и политичким правима.
[288] Текст Декларације је доступан на: *https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=15842&lang=en*, 20. април 2019.
[289] Council of Europe, *Twenty – First Ordinary Session*, collected texts, Strasbourg, 1979, 908. Нав. према: Александар Јакшић, *Европска конвенција о људским правима – коментар*, Правни факултет Универзитета у Београду, Београд 2006, 251.

4.2.4. Право на приватност у Европској конвенцији о заштити људских права и основних слобода

Европска конвенција о заштити људских права и основних слобода,[290] као један од најважнијих европских прописа из области заштите људских права, предвиђа право на поштовање приватног и породичног живота. Члан 8. Конвенције наводи да „Свако има право на поштовање свог приватног и породичног живота, дома и преписке. Јавна власт не сме да се меша у вршење овог права, осим ако је такво мешање предвиђено законом и ако је то неопходна мера у демократском друштву, ради заштите интереса националне безбедности, јавне сигурности, економске добробити, спречавања нереда или спречавања злочина, заштите здравља и морала или заштите права и слобода других“.[291] Конвенција штити приватни живот појединца, али не помиње податке о личности као део права на приватни живот. Међутим, у пракси, право на заштиту личних података подводи се под окриље права на приватност.

Право на приватност штити три области који се тичу човекових личних добара. Прва област се односи на заштиту физичког и моралног интегритета појединца, друга се тиче приватне сфере појединца у најширем смислу речи, док се трећа област односи на слободу човекове личности.[292] За тему овог истраживања кључна је друга област која под приватном сфером појединца подразумева и заштиту података о личности.

- *Пракса Европског суда за људска права у вези са правом на приватност и личним подацима*

Пракса Европског суда за људска права говори више о повезаности права на приватност, јавне управе и личних података грађана. У том смислу, Европски суд за људска права стао је на становиште да држава има дужност да се уздржи од прикупљања, чувања и објављивања података који се тичу личног живота појединца.[293]

[290] Европска конвенција о заштити људских права и основних слобода, Савет Европе, Рим, 1950.
[291] Чл. 8. Европске конвенција о заштити људских права и основних слобода.
[292] А. Јакшић (2006), 251.
[293] ECHR, Rotary, пресуда од 04.05.2000. год., бр. 46., ECHR, Amman, пресуда од 16.02.2000. год., бр. 69. Нав. према: А. Јакшић (2006), 254.

Такође, судска пракса под личним животом појединца подразумева пословне и политичке аспекте живота приватног живота, што се може довести у везу са личним подацима грађана у овим областима.[294] У вези са заштитом података који се размењују у електронском облику, наводимо и став суда да се под преписком подразумева свака врста преписке и комуникације, независно од начина и средства комуникације. Овај став је од изузетног значаја за различите области друштвеног живота и указује да и правна пракса мора да буде упозната са друштвеним трендовима. Надаље, Европски суд је закључио да држава не сме да контролише или на други начин надзире комуникацију.[295] Овај став је изузетно важан будући да органи електронске јавне управе, данас, више него икада, имају могућност да приступе преписками грађана у електронском облику.

Дакле, закључујемо да је Европски суд за људска права препознао право на заштиту личних података као важан сегмент права на поштовање приватног и породичног живота (права на приватност), иако Конвенција не предвиђа посебно право на заштиту личних података.

Сматрамо да је у данашњим околностима, неопходно извршити ревизију Конвенције и ускладити је са реалним потребама човека, у чему велику помоћ може да понуди пракса Суда. У том смислу, важно је препознати право на заштиту података о личности као посебно људско право, а не као део права на приватност.

4.3. Право на заштиту личних података

Прописи упоредних законодавстава у материји личних података углавном предвиђају посебно људско право које носи назив „право на заштиту личних података“. У средишту овог права, као што и сам назив говори, налазе се лични подаци, који представљају његов основни заштитни објект. Приватност се може схватити као посредан објекат заштите права на заштиту личних података.

Можемо рећи да се право на заштиту личних података развило у посебно право из права на приватност, као ширег права. Важност личних података и потреба за конкретизацијом бројних овлашћења у вези са њима, утицали су на

[294] ECHR, Halford, пресуда од 25.06.1997. год., RJD, 1997 – III, бр. 44. *Ibid*.
[295] ECHR, Silver, пресуда од 25.03.1983. год., Series A, no. 61, бр.83. *Ibid*., 257.

формирање посебног права. Такође, на појаву овог права утицала је и све већа улога личних података у савременом информационом друштву.

Право на заштиту личних података састоји се из већег броја овлашћења, па је у том смислу комплексно право. Како Водинелић наводи: „Право на личне податке представља у основи овлашћење да човек одлучује о давању и обради података о себи, независно од степена поверљивости тих података. Право на личне податке сложено је право, састављено из низа овлашћења. Право је човека да се подаци о њему не прикупљају од других него од њега самог, да се неки подаци не прикупљају и не обрађују уопште, да они који се обрађују не буду доступни другима, да зна ко обрађује податке о њему, да тражи обавештење о томе да ли неко обрађује податке о њему, да изврши увид, да тражи исправљање података, да тражи ажурирање, да тражи употпуњавање, да тражи обуставу, да тражи брисање, да зна коме се подаци преносе и у које сврхе“.[296] Дакле, разумевање правне природе права на заштиту личних података захтева разумевање права на приватност, али и овлашћења њиховог имаоца у вези са обрадом и коришћењем личних података, које му гарантује заштиту од недозвољеног мешања у његову личну сферу.

4.3.1. Право на заштиту личних података у правном систему Србије

У правном систему Србије приватни живот појединца заштићен је кроз право на заштиту података о личности. Уставом Србије зајамчена је заштита података о личности, а питања прикупљања, држања, обраде и коришћење података остављени су законској регулативи.[297] Забрањена је и кажњива свака употреба података о личности изван сврхе за коју су прикупљени, у складу са законом, осим за потреба вођења кривичног поступка или заштите безбедности Србије. Важно је напоменути и то да свако има право да буде обавештен о прикупљеним подацима о својој личности, у складу са законом, и право на судску заштиту због њихове злоупотребе.[298]

[296] V. Vodinelić, (2005), 69-70.
[297] Чл. 42, став 1. и 2. Устава РС.
[298] Чл. 42, став 4. Устава РС.

Према Уставу, подаци о личности представљају значајан елемент приватности и живота појединца. Сви морају поштовати податке о личностима и не смеју их злоупотребљавати, односно користити у сврхе другачије од оних предвиђених законом. Сва питања од значаја за личне податке појединаца морају бити уређена посебним законом, чиме се додатно даје на значају институцији личних података.

Посебан закон који уређује питања од значаја за заштиту личних података у Србији јесте Закон о заштити података о личности (2018). Овим законом уређено је право на заштиту физичких лица у вези са обрадама података и слободним протоком таквих података, начела обраде, права лица на које се подаци односе, обавезе руковалаца и обрађивача, правна средства, одговорност и казне у случају повреде права физичких лица у вези са обрадом њихових личних података и посебне ситуације обраде.[299]

4.3.2. Право на заштиту личних података као посебно право у правном систему ЕУ

Правни систем ЕУ препознаје право на заштиту личних података као једно од основних људских права. То је потврђено кроз неколико прописа, међу којима су најзначајнији оснивачки уговор - Уговор о функционисању Европске уније[300] и Повеља Европске уније о основним правима.[301] Ови документи гарантују посебно право сваког лица на заштиту својих личних података. Лични подаци могу бити предмет обраде једино уколико је она законита, заснована на одређеној сврси и уколико се врши на основу пристанка лица чији се подаци обрађују. Гарантовано је и право сваког лица на приступ његовим личним подацима, када се они налазе код другог лица.[302]

Да је право на заштиту личних података основно лично право утврђено је и у Општој уредби ЕУ као најзначајнијем пропису ЕУ у области заштите личних

[299] Чл. 1, ст. 1, Закона о заштити података о личности (2018).
[300] Чл. 16, ст. 1, Уговора о функционисању ЕУ.
[301] Paul Lambert, *Understanding the New European Protection Rules*, CRC Press- Taylor and Francis Group, New York 2017, 24.
[302] Вид. чл. 8, Повеље ЕУ о основним правима.

података. Она предвиђа да је заштита лица у односу на обраду података и личности основно људско право.[303]

Право на заштиту личних података није апсолутно право, већ је његово уживање ограничено јавним (друштвеним) интересима. Имајући у виду значај личних података за функционисање друштва, право на заштиту личних података мора да остварује у складу са осталим основним људским правима. Једино на тај начин, право на заштиту личних података може остварити своју друштвену улогу.

5. ПОСЕБНА ПРАВА У ВЕЗИ СА ЗАШТИТОМ ЛИЧНИХ ПОДАТАКА

Гарантовањем људског права остварује се само први корак у пружању правне заштите личним добрима. Следећи корак јесте установљавање механизама који ће остварити практичну примену људских права. Такав је случај и са правом на заштиту личних података. Оно представља теоријски концепт који се остварује кроз низ посебних овлашћења која су усмерена на заштиту приватности лица. Када томе додамо и права која се гарантују грађанима у односу са органима управе, добијамо систем посебних права која су усмерена на заштиту личних података у електронској управи.

Циљ таквог система је успостављање квалитетнијег положаја грађана који обезбеђује да сва лица подједнако уживају правну заштиту, како би слободно управљала својим животом и развијала своју личност, без страха и утицаја других. Основни разлог постојања посебних права, која су обично процесног карактера, јесте да омогуће ефикасну заштиту основном праву у вези са чијим постојањем су и зајамчена. Такав је случај са правом на заштиту личних података.

У систем права на заштиту личних података убраја се низ права којима ће бити посвећена посебна пажња у овом истраживању. У праву Србије и праву ЕУ, као права у вези са заштитом података издвајају се: право на обавештеност, право на приступ, право на исправку, право на заборав, право на ограничену обраду, право на пренос, право на приговор, права у вези са аутоматском обрадом података.

[303] Тачка 1, Преамбуле Опште уредбе ЕУ.

5.1. Право на обавештеност

Један од основних права у вези са остваривањем права на заштиту личних података односи се на могућност грађана да буду упознати са свим питањима обраде њихових личних података.[304] Једино када су грађани упознати са обрадом, када знају шта се дешава са њиховим личним подацима који се налазе у поседу органа управе, они могу предузети одређене кораке у циљу њихове заштите. Добијањем информација о поступању са личним подацима грађана остварује се и начело транспарентности, принцип од кључног значаја за систем заштите података и функционисање јавне управе.

Уколико грађани не би били обавештени о поступцима службених лица у вези са њиховим личним подацима, стварала би се атмосфера тајности која не доприноси демократији и квалитетном раду јавне управе. Због тога, један од основних начина остваривања видљивости деловања органа управе и поступања са личним подацима грађана јесте гарантовање права на обавештеност.

Право на обавештеност може се посматрати шире и уже. Шире посматрано, право на обавештеност значи да сва лица имају право да на адекватан начин буду информисана о различитим питањима у вези са обрадом њихових личних података. Реч је о подацима која се тичу појединаца, али и подацима од ширег друштвеног значаја. У том смислу илустративна је одредба Устава Србије која предвиђа да свако има право да истинито, потпуно и благовремено буде обавештен о питањима од јавног значаја и средства јавног информисања су дужна да то право поштују.[305] Дакле, право на обавештеност у ширем смислу односи се на право грађана да добију све информације из различитих области друштвеног живота, које се посредно и непосредно тичу грађана. У овом контексту може се повезати право на заштиту личних података са правом на јавно информисање, као сегментом права на обавештеност.[306]

---

[304] М. Давинић, *Независна контролна тела у Републици Србији*, Досије студио, Београд 2018, 51-52.

[305] Чл. 51, ст. 1, Устава РС.

[306] За више о праву на јавно информисање вид. Јелена Јовичић, „Уставно регулисање права на јавно информисање“, *Зборник радова правног факултета у Нишу* (ур. Предраг Димитријевић), Правни факултет Универзитета у Нишу, Ниш 2012, 543-552.

Са друге стране, право на обавештеност у ужем смислу означава право грађана да буду обавештени о свим обрадама и поступцима органа управе у вези са подацима који се односе на то лице. Оквири ужег схватања не обухватају информације од јавног значаја, већ искључиво личне податке грађана који се налазе у поседу другог лица.

Право на обавештеност у ужем смислу припада корпусу посебних права у вези са заштитом личних података у електронској јавној управи. Свако има право да буде обавештен о обради његових личних података. Ово право је материјално-процесне природе. Састоји од обавезе органа управе да информишу лице чије податке обрађују. Такође, оно се састоји и од овлашћена лица чији се подаци обрађују, да оствари увид у све елементе обраде које се тичу његових података. Због тога, право на обавештеност у ужем смислу представља важан елемент права на заштиту личних података.

- Право на обавештеност у правном систему Србије и правном систему ЕУ

Правни системи Србије и ЕУ познају право на обавештеност. У Закону о заштити података о личности (2018), по први пут у правном систему Србије, предвиђено је право на обавештеност. У Закону се не користи термин право на обавештеност, већ се одређује круг информација које се пружају лицу када се подаци о личности прикупљају од њега.[307] Предвиђањем обавезе органа управе да информишу лице чији се подаци обрађују, остварује се право на обавештеност у ужем смислу, као посебно право које чини важан део права на заштиту личних података. Када се ово право посматра у односу на функционисање органа управе, можемо рећи да се њиме конкретизује принцип управног поступка - начело приступа информацијама и заштите података.[308]

У управном поступку предвиђена је дужност органа да сваком лицу омогући приступ информацијама од јавног значаја, али и дужност да пружи заштиту личним подацима грађана у складу са законом који уређује заштиту података. Тако се остварује веза управног поступања и заштите личних података. На истоветан начин, право на обавештеност уређено је и у Општој уредби ЕУ.

[307] Чл. 23. Закона о заштити података о личности (2018).
[308] Ово начело регулисано је у члану 15, Закона о општем управном поступку.

Право на обавештеност остварује се кроз обавезу органа управе да пруже релевантне информације грађанима о обради личних података у сваком поједином случају. То значи да се право на обавештеност не остварује само захтевом лица, већ и пружањем информација по службеној дужности. Таква дужност је од великог значаја, будући је тешко очекивати од грађана да имају у виду све податке који се налазе у поседу органа управе и обраде који они врше. Зато је адекватније самој природи права на обавештеност да у сваком поједином случају обраде орган пружи одговарајуће информације о обради, јер се на тај начин остварује ваљано управно поступање.

У систему заштите података о личности Србије и ЕУ разликују се две ситуације када орган пружа информације о обради података. Разлика између ове две ситуације учињена је у односу на начин прикупљања личних података. Први случај односи се на ситуације у којима се подаци прикупљају од лица на које се односе, док се други случај односи на ситуације у којима се подаци не прикупљају од лица на које се односе.

- *Давање обавештења о обради када се подаци прикупљају од лица на које се односе*

Уколико се подаци о личности прикупљају од лица на које се односе, поступајуће лице управног органа дужно је да обавести странку о појединим елементима од значаја за транспарентну обраду. Приликом прибављања података о личности, орган управе ће лицу пружити информације које се односе на:

1. Идентитет и начин остваривања контакта са руковаоцем података (органом), односно његовим представником или лицем које је дужно да се стара о заштити података,
2. Правни основ и сврху ради које се прикупљају лични подаци,
3. Намеру органа да изврши трансфер личних података у другу државу или међународну организацију,
4. Рок у коме се чувају лични подаци, односно о критеријумима њиховог одређивања,
5. Процесна права која лице има у поступку (право на приступ, исправку, брисање, право на преносивост, право на правна средства),
6. Евентуалне последице непружања личних података,

7. Могућност аутоматизованог доношења одлуке.[309]

Лице чији се подаци прикупљају мора бити обавештено о поменутим чињеницама већ приликом прибављања података. То значи да је за остваривање овог права неопходно да лице чији се подаци обрађују и прикупљају од самог почетка управног поступка буде упознато са основним елементима обраде.

Елементи обавештења односе се на субјекта који прикупља податке и врши обраду, разлоге због којих се врши прикупљање, процесна права и друге чињенице које могу бити од значаја за правни статус странке (пренос у иностранство и аутоматизовано доношење одлуке). Њима се гарантује транспарентна обрада будући да грађани добијају информацију о томе ко, на основу чега и због чега прикупља и обрађује њихове личне податке. Иако су права гарантована законом, постоји обавеза обавештавања и о процесним правима, како би грађани били упућени у могућности које им правни систем пружа.

- *Давање обавештења о обради када подаци нису прикупљени од лица на које се односе*

Други случај односи се на пружање информација о обради када подаци о личности нису прикупљени од лица чији су подаци, већ од неког другог лица.[310] Осим елемената обраде који се пружају у случају када су подаци прикупљени од лица чији су подаци, неопходно је и обавештење о додатним чињеницама, због тога што се разликује ималац података и извор од кога су подаци добијени. Због тога, орган је дужан да пружи додатне информације о извору од кога су прикупљени подаци. Органи управе су дужни да пруже оправдање уколико прикупљање и обрада извршени ради задовољења јавног интереса или потреба поступка.[311]

Информације у вези са личним подацима морају се пружити у концизном, разумљивом и лако читљивом облику, како се право на обавештеност не би технички злоупотребљавало (дуга и компликована обавештења). Значај

[309] Чл. 23, Закона о заштити података о личности (2018), чл. 13, Опште уредбе ЕУ.
[310] Чл. 24, Закона о заштити података о личности (2018), чл. 14. Опште уредбе ЕУ.
[311] Чл. 12, ст. 1, тач. 6, Закона о заштити података о личности (2018) и Чл. 6, ст. 1, тач. Ђ, Опште уредбе ЕУ. Нешто другачија правила предвиђена су за државне органе који су надлежни за спречавање, истрагу и откривање кривичних дела, као и гоњење учиниоца кривичних дела, што превазилази оквире надлежности електронске јавне управе, а тиме и оквире овог истраживања.

информационо-комуникационих технологија у вези са правом на обавештеност, препознат је у праву Србије и у праву ЕУ. Грађани могу бити обавештени и електронским путем о поменутим информацијама, а дозвољено је и коришћење стандардизованих програма (у дигиталном облику) ради пружања обавештења. Програми морају бити лако доступни, концизни и машински читљиви, како би се могли користити у електронској форми.[312]

Можемо закључити да је право на обавештеност (информисаност) предвиђено у правном систему Србије и у правном систему ЕУ. Оба правна система регулишу ово право на истоветан начин. Суштина овог права јесте да се од самог почетка управног поступка или поступка обраде личних података води рачуна о интересима странака, односно лица чији се подаци обрађују. То се постиже пружањем информација о значајним елементима обраде које могу имати утицаја на ток поступка. Примећујемо усклађивање потребе за несметаним вођења управног поступка и потребе за транспаретношћу рада управних органа. Због тога, право на обавештеност у ужем смислу представља једно од основних елемената система заштите података у електронској јавној управи, које помаже остваривању људских права и подстиче транспарентност рада органа управе.

5.2. Право на приступ личним подацима

Постављамо питање, шта се дешава када орган пропусти своју дужност да пружи обавештење о обради података и другим питањима од значаја за обраду и на тај начин ускрати грађанима информације од значаја за заштиту њихових права? У овим ситуацијама неопходно је установити механизам који странкама омогућава увид у поступање органа у вези са њиховим личним подацима.[313]

Такав механизам остварује се у облику права на приступ личним подацима. Уколико право на обавештеност посматрамо као једну страну медаље начела транспарентности рада органа управе, право грађана на приступ подацима можемо посматрати као другу страну исте медаље.

[312] У Србији, Повереник за информације од јавног значаја и заштиту података о личности задужен је за поступак утврђивања стандардизованих икона Чл. 21, ст. 9, Закона о заштити податка о личности (2018).

[313] Уколико је орган управе поступио супротно својим законским овлашћењима, постоји простор и за његову одговорност због неправилног вршења законских овлашћења и дужности.

Право на приступ личним подацима који се налазе у поседу органа управе има одређене сличности са правом на слободан приступ информацијама од јавног значаја. Право на слободан приступ информацијама од јавног значаја заснива се на принципу јавности, које се супротставља идејама тајности и затворености.[314] Наравно, право на приступ информацијама од јавног значаја представља другачију врсту права којим се омогућава приступ информацијама које су од значаја за ширу друштвену заједницу, а налазе се у поседу органа јавне власти. Приступом информацијама од јавног значаја „проширује се слобода информисања и употпуњује гаранција људског права која омогућава да грађани дођу до информација од којих зависи формирање и исказивање њихове суверене политичке воље. То подразумева и лакшу контролу власти и државне управе.“[315]

Код права на приступ личним подацима, грађанима се дозвољава да од органа управе захтевају информације у вези са обрадом њихових личних података. На посредан начин тиме се остварује увид грађана у рад органа управе, односно контрола управе од стране грађана, јер „контролу и одговорност носилаца јавне власти није могуће остварити без увида у рад субјеката који врше функције власти“.[316] Поменута права се разликују у односу на интерес који теже да заштите, док је начин остваривања права и сврха ради које се употребљавају слична. Дакле, по својој правној природи, право на приступ личним подацима можемо посматрати као изведено право из права на слободан приступ информацијама од јавног значаја које се остварује у односу на личне податке конкретног лица.

[314] V. Vodinelić, „Pravo na slobodan pristup informacijama od javnog značaja kao ustavno pravo“, u: *Slobodan pristup informacijama – ustavno jemstvo i zakonske garancije*, Fond za otvoreno društvo, Beograd 2004, 9.
[315] Miroljub Radojković, „Za slobodan pristup informacijama“, *Prizma,* br.4/2002, Centar za liberalno-demokratske studije, Beograd 2002, 29.
[316] J. Вучковић, „Право на слободан приступ информацијама од јавног значаја“, *Зборник радова правног факултета у Нишу* (ур. Радмила Ковачевић-Куштримовић), Правни факултет Универзитета у Нишу, Ниш 2009, 182.

5.2.1. Право на приступ личним подацима у правном систему Србије и правном систему ЕУ

Право на приступ личним подацима заснива се на овлашћењу лица чији се подаци налазе у поседу органа управе да захтева и добије информације о појединим питањима од значаја за заштиту права и интереса у вези са обрадом личних података. У правном систему Србије грађани имају право да захтевају информацију о томе да ли постоје њихови лични подаци у поседу органа управе и да ли се ти подаци обрађују. Уколико је потврдан одговор на ово питање, странка има право да приступи својим личним подацима и да захтева информације од надлежног органа о питањима која се односе на обраду података. То су информације у вези са:

1. Сврхом обраде,
2. Категоријама података о личности,
3. Корисницима или категоријама корисника којима су подаци о личности откривени или ће им бити откривени, што се односи и на кориснике у страним државама и међународним организацијама,
4. Роковима у којима ће се подаци о личности чувати у поседу органа управе,
5. Постојањем права на исправку брисање, приговор или подношење притужбе надлежном органу,
6. Свакој доступној информацији о извору из кога су добијени подаци о личности,
7. Могућношћу аутоматизованог доношења одлука, начину примене аутоматизације и евентуалне последице такве обраде.[317]

Када странка затражи одређену информацију у вези са обрадом својих личних података, надлежни орган је дужан да такву информацију пружи. Орган је дужан да захтеване информације достави „на сажет, транспарентан, разумљив и лако доступан начин, коришћењем јасних и једноставних речи…“.[318] Орган мора увек поступити по захтеву грађана, осим у случају када не може да утврди идентитет лица које захтева информације.

[317] Чл. 26, ст. 1, Закона о заштити података о личности (2018).
[318] Чл. 21, ст. 1, Закона о заштити података о личности (2018) и чл. 12, ст. 1, Опште уредбе ЕУ.

Посебна ситуација се односи на пренос података у трећу државу или међународну организацију. Уколико се врши такав пренос, лице које захтева увид у своје личне податке има право да буде обавештено и о мерама заштите које се примењују у односу на међународни трансфер података. Те мере се прописују обавезујућим актом органа јавне власти и уговорним одредбама између руковаоца и обрађивача. Ово је од великог значаја за поштовање права грађана, будући да се „излази“ из опсега норми домаћег управно-правног система, па лице мора бити правно осигурано у случају недостатака у самом преносу података.

Лице чији се подаци обрађују има право да захтева издавање копије личних података који су у поседу органа и који се обрађују. У том случају, орган може да услови издавање копије накнадом нужних трошкова које има за израду копије. Будући да данас већина грађана поседује техничке уређаје преко којих се врши електронска комуникација, копија се може доставити и у електронском формату. Овде се још једном осликава корист електронске јавне управе, али и неопходност осавремењивања управних органа ради смањивања трошкова поступка и заштите права грађана. Истоветне одредбе у вези са правом лица на приступ личним подацима садржи и Општа уредба ЕУ.[319]

5.2.2. Правна природа одговора органа управе на захтев о приступу подацима

На овом месту постављамо питање правне природе одговора органа управе на захтев за приступ подацима. Од одговора на ово питање зависи могућност коришћења правних средстава и даље поступање органа управе. Сматрамо да по својој правној природи одговор органа на захтев странке о информацијама у вези са личним подацима, представља управну радњу. Управне радње су материјални акти органа управе који утичу на права и правне интересе грађана, а којима се извршавају правни акти.[320] Закон о општем управном поступку у управне радње сврстава издавање уверења и пружање информација.[321] Како у конкретном случају орган управе пружа информацију о личном податку који води у својој евиденцији,

[319] Чл. 15, ст. 1, Опште уредбе ЕУ.
[320] За више о појединачним актима и радњама управа без непосредног правног дејства вид. Д. Милков, *Управно право II- Управна делатности*, Универзитет у Новом Саду- Правни факултет, Нови Сад 2017, 62.
[321] Чл. 27, Закона о општем управном поступку.

одговор на захтев представља излагање чињеничног стања, а не и одлучивање у поступку, па се зато у овом случају не издаје решење. Међутим, у случају када орган одбија остварење права на увид, он то чини решењем којим се одбија захтев, будући да одлучује о праву странке. То значи да се у случају негативног става органа у вези са захтевом за увид доноси управни акт.

То нас даље води до питања, да ли се на издавање информација о личним подацима, када је руковалац орган управе, примењују одредбе Закона о заштити података о личности или Закона о општем управном поступку? Иако су органи управе дужни да поступају по одредбама општег управног поступка, сматрамо да у конкретном случају Закон о заштити личних података (2018) има предност, будући да представља посебан пропис, па самим тим има предност у примени у односу на општи (*lex specialis derogat legi generalis*).[322] Како је у питању посебни управни поступак, на издавање информација о личним подацима, органи управе треба да примењују посебна правила о заштити личних података уз уважавање начела и основних права предвиђених Законом о општем управном поступку.

5.2.3. Рок за пружање информација о обради личних података

Рок у коме је орган (руковалац или обрађивач) обавезан да поступи по захтеву лица за пружање информације о обради личних података износи 30 дана од дана пријема захтева. Према потреби, овај рок се може продужити за још два месеца, уколико то захтева сложеност захтева.

Сматрамо да је предвиђени рок предугачак у односу на важност захтева. Предвиђањем дугачког рока губи се из вида начело делотворности у остваривању права странака, у односу на органе управе који су дужни да странкама омогуће брзо и делотворно остваривање права и правних интереса.[323] У Закону о општем управном поступку предвиђено је да се уверења и друге исправе издају истог дана када је странка поднела захтев, а најкасније у року од 8 дана, осим ако посебним прописом није друкчије предвиђено. Будући да се о личним подацима у поседу органа управе мора водити службена евиденција, сматрамо да нема аргумената да

[322] Овај принцип налази своју примену и у управном праву Републике Србије. О томе вид. Dobrosav Milovanović, „Odnos opšt(ij)eg i posebn(ij)ih, *Polis- časopis za javnu politiku*, br. 11, Stalna konferencija gradova i opština i Centar za javnu i lokalnu upravu, Beograd 2016, 42-47.
[323] Чл. 9, Закона о државној управи.

се у вези са пружањем информацијама о личним подацима предвиди знатно дужи рок од оног предвиђеног Законом о општем управном поступку.

Општа уредба ЕУ предвиђа да се захтеване информације имају пружити без одлагања, а најкасније у року од 30 дана од поднетог захтева, што је идентично са решењем српског закона. Дужи рокови за пружање информација и поступање органа онемогућавају адекватну заштиту интереса грађана, при чему постоји објективна могућност за бржим поступањем по захтевима за увид у личне податке. Употреба савремених информационо-комуникационих технологија омогућава систематизовано чување и брз приступ личним подацима који се чувају. Због тога, сматрамо да би било целисходније и боље за грађане предвидети краће рокове за поступање органа управе по захтеве за увид.

Уколико руковалац не поступи у предвиђеним роковима, дужан је да о таквом пропусту обавести странку, при чему ће је обавестити и о разлозима који су узроковали такав пропуст. Орган обавештава странку и о праву на правно средство, односно праву на притужбу Поверенику. У случају настанка штете због непружања тражених информација, странка има право на накнаду штете од поступајућег органа.

***

Право на приступ личним подацима регулисано је на истоветан начин и у Србији и на нивоу ЕУ. Основни циљ овог права је да грађанима омогући увид у своје личне податке који се налазе у поседу органа управе. Без постојања овог права, рад органа управе могао би остати под велом тајности.

Напомена коју бисмо издвојили јесте да треба скратити рок за издавање тражених информација, јер се на тај начин адекватније штите права и правни интереси грађана. Такође, на тај начин би се остваривала ефикасност и делотворност рада органа управа.

5.3. Право на заборав

У ери интернета и информационо-комуникационих технологија изузетно је тешко потпуно избрисати информацију која је једном ушла у дигитални етар. Упрошћене могућности размене и чувања информација омогућавају свим лицима који једном дођу у контакт са информацијом да је сачувају и даље користе. Зато је неопходно омогућити имаоцу личних података да самостално одлучи о томе да ли жели да његов податак буде сачуван код другог лица које је обрађивало те податке. Значајну улогу у том погледу има право на заборав.

Право на заборав представља једно од основних права у вези са заштитом личних података у модерном свету. Концептуално, право на заборав заснива се на тежњи да грађани не трпе последице због коришћења и употребе личних података у прошлости. Такође, ово право представља својеврсно остварење начела тачности података, јер се може догодити да одређени податак више није тачан, па га треба избрисати. У систему заштите личних података, право на заборав омогућава да се лични подаци који се без одређене сврхе налазе код других, могу обрисати на захтев њиховог имаоца.

У теорији се наводи да је право на заборав поливалентно право које се састоји из више елемената. Први се односи на кривично-правни аспект, односно на заборав података о кривичним и прекршајним поступцима и осуђујућим пресудама. Други елемент се односи на заборав личних података који су у поседу других лица, док се трећи елемент односи на право „дигиталног заборава“, са циљем да се избришу информације и подаци пласирани на друштвеним мрежама и интернету.[324]

Институт рехабилитације из кривичног права функционално је сличан праву на заборав. Рехабилитацијом се брише осуда и престају све њене правне последице, а осуђени се сматра неосуђиваним.[325] На сличан начин делује и право на заборав, које омогућава да се обришу сви подаци које се налазе код другог и да се то лице „заборави“ у историји оног ко је обрађивао личне податке. Међутим,

[324] Cécile de Terwangne, „Internet Privacy and the Right to Be Forgotten/Right to Oblivion“, Monograph "VII International Conference on Internet, Law & Politics- Net Neutrality and other challenges for the future of the Internet", *Revista de internet, derecho y politica,* Universitat Oberta de Catalunya, Barcelona 2012, 109.
[325] Чл. 97, Кривичног законика Србије, *Службени гласник* РС, бр. 85/2005, 94/2016.

основна тенденција права на заборав усмерена је ка заштити појединца. Са друге стране, рехабилитација штити шире друштвене интереса, као што су нормално функционисање друштвене заједнице и повратак кажњених лица у нормалне друштвене токове. Због тога, неопходно је правити разлику између два института, која припадају различитим гранама права, иако имају сличне карактеристике.

Право на заборав изазива и друге полемике у теорији. Спорно је који су тачно елементи овог права, да ли је адекватан назив, из ког правног института потиче, итд. Поједини аутори праве разлику између „права на брисање“ и „права на заборав“.[326]

Такође, јављају се две групе мишљења у односу на питање правне природе „права на заборав“. Једни сматрају да право на заборав представља појавни облик права на приватност.[327] У складу са таквим становиштем, право на заборав помаже у заштити приватности лица чији су подаци објављени. Други сматрају да право на заборав потиче из права на част и углед.[328] Ово становиште се објашњава тиме да свако има право на част и углед, те да објављене информације које нису тачне вређају част и углед лица и морају бити избрисане, односно заборављене.

Независно од теоријских спорења, можемо рећи да „право на заборав“ представља једно од носећих стубова система заштите личних података. У ери информационо-комуникационих технологија и интернета људи се користе великим бројем личних података које користе за учествовање на друштвеним мрежама, форумима и интернет сајтовима. У таквом „мору информација“ тешко је одредити које су информације тачне, а које нису. Због тога, грађанима је гарантовано право да траже уклањање свих нетачних података личне природе. Такође, ово право се односи и на личне податке чија је сврха временом испуњена, а они се идаље налазе у поседу других лица које их могу користити за нове и другачије сврхе од оних због којих су прикупљени.

[326] За више о разлици између „права на заборав“ и права на брисање“ вид. Meg Leta Ambrose, Jef Ausloos, „The Right to Be Forgotten Across the Pond“, *Journal of Information Policy*, vol. 3, Pennsylvania State University Press, Penssylvania 2013, 14-16.
[327] Antoon De Baets, „A historian's view on the right to be forgotten“, *International Review of Law, Computers & Technology*, Vol. 30, Nos. 1-2, Routledge- Taylor & Francis group, online 2016, 57.
[328] Jeffrey Abramson, „Searching for Reputation: Reconciling Free Speech and the „Right to be Forgotten““, *North Carolina Journal of Law & Technology*, vol. 17, issue 1, online 2015, 47.

Иако право на заборав делује као природни део система заштите података, потреба за овим правом и успостављањем у упоредно-правним законодавствима, искристалисала се захваљујући судској пракси.

5.3.1. Случај *Google v. Costeja*

Незаобилазни елемент у формулисању права на заборав имала је пресуда Суда правде Европске уније из 2014. године у предмету *Google Spain SL, Google Inc. Vs. Agencia Espanola de Protecction de Datos (*познатија као *Google v. Costeja).*[329] Иако је донета од стране суда на територији ЕУ, значај ове пресуде је много шири и односи се на кориснике интернета широм света, а тековина ове одлуке нашла је место у многим упоредно-правним системима.

Чињенично стање у овом случају се заснива на томе да су шпанске новине *La Vanguardia* објавиле 1998. године два обавештења о принудној продаји непокретности адвоката Марија Костехе (*Maria Costeje*). Принудна продаја је требала да се изврши ради намирења дуга из социјалног осигурања. У међувремену, Костеха је измирио своја дуговања, али информације о принудној наплати због дуга остале су на интернету. Кад год би неко претраживао његово име на најпопуларнијем интернет претраживачу (*Google*), појављивала би се информација о извршењу на непокретностима ради намирења дуга.

Како би сачувао свој лични и пословни углед, Кореха се обратио шпанској агенцији за заштиту података са приговором у коме је тражио да *Google Spain* уклони све спорне чланке на интернету у вези са случајем и да се наложи поменутом претраживачу да избрише све његове личне податке који се појављују приликом претраживања његовог личног имена. Такође, Костеха је захтевао да новинарска агенција *La Vanguarida* повуче све чланке из новина у вези са њим и његовим судским поступком. Он је указао на то да је његов случај окончан пре неколико година, да више није актуелан, па самим тим не постоји потреба нити интерес јавности да буде упозната са детаљима случаја.

[329] Одлука Суда правде Европске уније у случају *Google v. Costeja* - Court of Justice of the European Union, *Google Spain SL, Google Inc. Vs. Agencia Espanola de Protecction de Datos (Google v. Costeja), Case C-131/12, 2014.* Пресуда је доступна на: *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131* , 09. септембар 2019.

Шпанска агенција за заштиту података само је делимично усвојила његов приговор. Приговор је усвојен у делу који се односи на *Google Spain* и захтев да се повуку (обришу) лични подаци Костехе из база података претраживача, како би се спречио даљи приступ овим подацима. Међутим, агенција је одбила његов захтев у делу који се односи на чланке новина *La Vanguaride*. Агенција је стала на становиште да јавност има интереса да буде упозната са таквим информацијама, па самим тим је постојао и законски основ за објављивање. Због овакве одлуке, *Google Spain* і *La Vanguaria* поднели су одвојене тужбе шпанском суду, захтевајући поништај наведене одлуке агенције.

Шпански суд је затражио помоћ од Суда правде ЕУ у тумачењу одређених питања у вези са случајем. Да ли давалац услуге интернет претраживања приликом пружања услуге претраживања интернета обрађује личне податке, ако су ти подаци добијени из другог извора, а не непосредно од лица чији се подаци објављују? Да ли је давалац услуге интернет претраживања уједно и руковалац обраде личних података који се објављују? И основно питање, да ли ималац може захтевати брисање личних података из резултата претраге одређеног интернет претраживача?

Суд правде ЕУ дао је одговоре на спорна питања, уз осврт на поједина питања која су стварала дилеме у пракси коришћења личних података. Становиште Суда правде ЕУ заснивало се на томе да се тадашње европско законодавство у области заштите података (Директива 95/46/ЕЗ) односи на организације у државама ЕУ, али и на организације изван ЕУ, уколико оне пружају услуге на тржишту ЕУ. То је за конкретан случај било од велике важности, будући да се предмет односио на даваоца услуге интернет претраживања (*Google*) који делује у бројним државама, а не само у Шпанији. Због свеопште повезаности путем интернета омогућена је конзистентност објављених информација свуда у свету, па одлука нема значај само за територију ЕУ. Даље, Суд правде ЕУ је стао на становиште да се *Google* може сматрати руковаоцем података који се објављују на сајту овог интернет претраживача, будући да он утврђује начине и сврху обраде. Интернет претраживач „прикупља“, „снима“ и „организује“ личне податке приликом претраживања кључних речи корисника.

На крају, утврђено је да Кореха има право да захтева уклањање информација са интернет претраживача. Наиме, обрада његових личних података имала је законит циљ који је са временом испуњен, па више не постоји. Због тога је даља обрада неприкладна, ирелевантна и претерана у односу на сврху ради које су подаци прикупљени и обрађени, имајући у виду да је од конкретног случаја прошло доста времена.

На овај начин, суд је формулисао право на заборав личних података у оквиру права ЕУ, као једно од најважнијих средстава за заштиту личних података, иако га није експлицитно одредио под таквим термином. Кроз ово право остварују се начело истине и тачности података који се објављују. Ипак, суд је закључио да ово овлашћење (право) „није апсолутне нарави, већ у сваком конкретном случају треба проценити његову функционалност у односу на друга права и интересе, као што су слобода изражавања и слобода медија.“.[330] Ова одлука утицала је на то да право на заборав нађе своје место у упоредно-правним прописима који уређују заштиту података, како у правном систему ЕУ, тако и у правном систему Србије.

5.3.2. Право на заборав у електронској јавној управи Србије и ЕУ

Право на заборав предвиђено је у Закону о заштити података о личности Србије (2018), као и у Општој уредби ЕУ. Оба прописа на истоветан начин регулишу поменуто право. Право на заборав састоји се од захтева имаоца података упереног према органу управе (руковаоца) да обрише личне податке које поседује о њему.[331] Како би се омогућила ефикасна примена овог права, орган је дужан да то учини „без одлагања“. Међутим, руковалац ће обрисати личне податке само у одређеним случајевима које можемо класификовати у две групе.

Прва група односи се на ситуације тзв. незаконите обраде.[332] У случају када су подаци незаконито обрађивани, орган је дужан да такве податке обрише.

---

[330] Maja Čolaković, Lana Bubalo, „Pravo na zaborav kao instrument zaštite prava ličnosti u Evropskoj Uniji“, *Zbornik radova Pravnog fakulteta u Tuzli*, br. 2/2017 (ur. Vedad Gurda), Pravni fakultet u Tuzli, Tuzla 2017, 26.

[331] Поједини аутори сматрају да овом праву недостаје аутоматско брисање података након извесног периода, на шта треба да сугерише формулација „права на заборав“. За више вид. Nicolai Culik, Christian Döpke, „About Forgetting and Being Forgotten“, у *Big Data in Context- Legal, Social and Technological Insights*, (eds. Thomas Hoeren, Barbara Kolany-Raiser), Springer, online 2018, 23-24.

[332] Чл. 30, ст. 1, 2, 4, Закона о заштити података о личности (2018), и чл. 17, ст. 1, 2, 4, Опште уредбе ЕУ.

Могу се јавити случајеви у којима је постојао законит основ обраде, али је он накнадно отпао, па би даља обрада била неадекватна и незаконита. То значи да је сврха ради које су лични подаци прикупљени и обрађени испуњена, па даље коришћење и чување личних података није неопходно. Такође, постоје ситуације у којима се законитост обраде заснива на пристанку лица чији се подаци обрађују. Када лице које је дало пристанак, тај пристанак повуче, а орган управе (руковалац) нема других законских основа по којима може обрађивати личне податке, он је дужан да обрише податке тог лица.

Друга група односи се на посебне ситуације прописане законом.[333] Тако, када је уложен приговор на обраду личних података, постоји дужност органа да престане са даљом обрадом података лица које је уложило приговор. У овом случају, руковалац је дужан да обрише те податке, осим уколико не постоји неки други правни основ који претеже над интересима, правима или слободама лица чији се подаци обрађују. Претежност интереса орган је дужан посебно образложи у сваком конкретном случају.

Подаци о личности морају бити обрисани у циљу извршења неке од законских обавеза органа. Ова обавеза заснива се на неком од посебних закона. Ово ће бити чест случај у вези са подацима које чувају и обрађују органи управе, будући да законских основа за чување података о грађанима има више. То је случај са јединственим матичним бројем грађана, местом пребивалишта и боравишта грађана и другим подацима који се воде по посебним законима. Не треба изгубити из вида да обавезе вођења евиденције по посебним законима оправдавају континуитет чувања личних података у електронској управи, чак и када не постоји конкретна практична потреба за чувањем и обрадом. На крају, подаци о личности се морају обрисати уколико су прикупљени у вези са услугама информационог друштва које су понуђене деци. Деца представљају категорију лица која уживају посебну заштиту у вези са личним подацима, па се држава превентивно стара о њиховим личним подацима.

У случају неке од поменутих ситуација орган је дужан да „без одлагања“ обрише личне податке који се налазе у његовом поседу. Међутим, уколико је

[333] Чл. 30, ст. 3, 5, 6, Закона о заштити података о личности (2018), и чл. 17, ст. 3, 5, 6, Опште уредбе ЕУ.

орган учинио личне податке јавним, он има и додатну обавезу. Додатна обавеза се односи на предузимање „свих разумних мера у складу са доступним технологијама и могућностима сношења трошкова њихове употребе“ ради информисања других руковаоца који врше обраду истих података да обришу све елементе таквих података или копије података уколико их поседују.

5.3.3. Однос права на заборав и личних података које „установљавају“ органи јавне управе

Уколико посматрамо право на заборав у контексту личних података који грађанима издају органи управе, долазимо до одређених недоумица. Наиме, поставља се питање, како ускладити законске обавезе вођења различитих евиденција о личним стањима грађана и вођење података које установљавају органи управе са правом на заборав ? Ако би право на заборав било апсолутно право које делује према свима, па и према органима управе, вођење државних послова и евиденција би било доведено у питање, јер низ послова јавне управе зависи од личних података грађана, које установљавају државни органи.

Уз то, органи управе имају дужност да поступају по посебним законима који прописују обавезу чувања и вођења одређених личних података, па се такви подаци не могу брисати, односно „заборавити“ вољом грађана, јер је јавни интерес претежнији од приватног. Примера ради, у Србији је такав случај са јединственим матичним бројем грађана који се уређује Законом о јединственом матичном броју грађана.[334] Овај закон одређује јединствени матични број као индивидуалну и непоновљиву ознаку идентификационих података, који се додељује грађанима Србије. Јединствени матични број се користи као средство распознавања у правним односима са другим приватним лицима и органима јавне власти.

Овај и други слични подаци који се воде по посебном законском основу не могу бити „заборављени“ или избрисани на захтев грађана, будући да постоји претежнији јавни интерес државе за чување података. У оваквим случајевима не долази до повреде права на заборав, већ једино до сужавања овлашћења његовог

[334] Закон о јединственом матичном броју грађана, *Службени гласник* РС, бр. 24/2018.

имаоца због претежнијег значаја јавних интереса који се штите овим подацима.[335] Исти је случај и са подацима о месту пребивалишта и боравишта грађана,[336] које морају имати сви грађани Србије, са подацима из матичних књига (чињеница брака која се води у матичној књизи венчаних)[337] и др. За чувањем и вођењем ових података постоји значајан и оправдан јавни интерес који ограничава право на заборав. На тај начин закључујемо да је право на заборав по својој правној природи релативно право.

Овакав став потврдио је и Суд правде ЕУ у својој пресуди *Google vs. Coreha,* са становиштем да право на заборав није апсолутно право и да се мора сагледавати у односу са другим правима и интересима. Због тога је неопходно предвидети изузетке од примене права на заборав, који се тичу одређених облика јавног или приватног интереса, који треба да буде предвиђен законом.

Право на заборав неће се применити када над њим претеже слобода изражавања и информисања, јавни интереси у области јавног здравља, извршење архивских послова у јавном интересу, научном или историјском домену, потребе за вршењем јавних овлашћења руковаоца, у случају подношења одбране од правног захтева, у безбедносне сврхе, итд. У осталим ситуацијама, када не постоји посебан законски основ за чување личних података, органи управе имају дужност да обришу личне податке по поднетом захтеву.

[335] Јединствени матични број грађана служи као средство идентификације у правном промету, што је државним органима од велике важности у ситуацијама када се укаже потреба за чувањем јавног реда и мира, заштите јавног здравља, задовољења потреба вођења судских и управних поступака, итд. Иако се не зна конкретна употребна сврха јединственог матичног броја грађана, она стоји у латентном положају, доступна органима управе, који му приступају у случају настанка неког од појавних облика поменутих јавних интереса.
[336] Закон о пребивалишту и боравишту грађана, *Службени гласник* РС, бр. 87/2011.
[337] Закон о матичним књигама, *Службени гласник* РС, бр. 20/2009, 145/2014 и 47/2018.

5.4. Право на исправку и допуну личних података

Данас се лични подаци користе за идентификацију физичких лица, склапање правних односа, коришћење правних средстава, покретање правних поступака, итд. Због сигурности правног промета и поштовања права и интереса учесника у промету, од велике је важности да лични подаци који се користе буду тачни и потпуни. Један од основних принципа заштите личности у таквим процесима јесте тачност личних података. Због тога, тачност и потпуност личних података остварују се кроз процесно право на исправку и допуну података.

Порекло права на исправку и допуну проналазимо у праву медија. Слобода медија и слобода објављивања информација представљају основе сваког модерног демократског друштва.[338] Међутим, може се догодити да медијска слобода доведе до објављивања информација које нису тачне и то из различитих разлога (погрешно протумачене чињенице случаја, потреба за сензационалистичким извештавањем, погрешно добијене информације од извора, итд.).

Због тога је у медијском праву формулисано право на исправку или допуну нетачне информације. „Право на исправку јесте овлашћење лица чији су право или интерес повређени неистинитом, непотпуном или нетачно пренетом информацијом да захтева да се објави исправка те информације као неистините, непотпуно или нетачно пренете.“[339] Ово посебно право штити физичко лице од неистинитих и нетачних јавности доступних информација, које могу довести до повреде части и угледа лица на кога се нетачне информације односе. Уједно, ово право остварује и интерес јавност да сазна истините и потпуне чињенице о неком догађају или појави, јер се једино на тај начин могу остваривати многи принципи на којима функционише друштво.[340]

На сличан начин, потреба за истинитим и потпуним информацијама постоји и у области личних података. Сигурност правног промета и остваривање

[338] Чак се и право на заштиту личних података ограничава како би слобода медија могла да се оствари. Вид. V. Vodinelić (2005), 69.
[339] Анђелија Адамовић, „Поступак у парницама за објављивање исправке неистините, непотпуне или нетачно пренете информације“, *Зборник радова Правног факултета у Нишу* (ур. Милан Петровић), Правни факултет у Нишу, Ниш 2012, 501.
[340] Владимир Боранијашевић, „Поступак у парницама за објављивање исправке“, *Зборник радова „Владавина права и правна држава у региону“* (ур. Горан Марковић), Правни факултет у Источном Сарајеву, Источно Сарајево 2014, 539-540.

принципа законитости захтевају тачне и потпуне личне податке у свим областима друштвеног живота и правним поступцима. Због тога, системи заштите личних података гарантују грађанима право да захтевају исправку и допуну нетачног или непотпуног личног податка.

Право на исправку и допуну у области заштите личних података разликује се у односу на право на исправку и допуну информације из медијског права, будући да је оно превасходно усмерено на заштиту јавности и јавних интереса, а право на исправку из области личних података штити приватност појединог лица у његовим односима са другим лицима.

5.4.1. Право на исправку и допуну у правном систему Србије и правном систему ЕУ

Право на исправку и право на допуну представљају посебна процесна права грађана у области личних података која грађанима омогућавају коришћење тачних и потпуних личних података у правном промету. На тај начин, штите се не само лични подаци грађана и њихови приватни интереси, већ се омогућава свим учесницима правног промета да буду сигурни и да се могу поуздати у правни систем, што је значајно за све области приватног и пословног живота.

Суштински посматрано, право на исправку и допуну састоји се из два посебна права, права на исправку и права на допуну. Међутим, ова два права теже идентичној сврси, а то је истинито и потпуно чињенично стање у правним односима у односу на личне податке. Због тога, ова два права се обично појављују у јединственом облику. Теоријски, између поменутих права постоји разлика, па ће истраживање анализирати свако право засебно.

5.4.2. Право на исправку

Право на исправку заснива се на томе да свако физичко лице чији се подаци чувају код органа управе има право да захтева исправку погрешног или нетачног податка о личности. Грешка се јавља у случају када се не ради о податку који чињенично постоји (у реалности), већ о неком другом. Примера ради, уместо Републике Србије, као државе рођења, стоји Београд (град), те се ради о

погрешном податку, будући да је информација погрешна, јер се држава и град разликују по својој природи.

Подаци могу бити нетачни, када се ради о правом податку, оном који чињенично постоји, али неки од елемената тог податка није правилно забележен. На пример, уместо датума рођења 01.01.1992. унет је датум рођења 01.02.1992. У овом случају, ради се о правом податку (години рођене), али који је нетачан у погледу месеца, па постоји потреба за исправком.

5.4.3. Право на допуну

Грађани имају право да захтевају и допуну личних података који су похрањени код органа управе. То се дешава у случајевима када је накнадно дошло до одређене промене у личном статусу грађана, али та промена није заведена у базама личних података, односно у односу на конкретан података о личности. Пример: Након венчања жена је свом презимену додала мужевљево презиме, али у одређеном личном документу стоји само женино девојачко презиме (као податак о личности). У односу на овај податак, жена има право да тражи промену презимена у евиденцији, како би лични податак о њеном презимену био употпуњен и усклађен са стањем у пракси. У оваквим ситуацијама, грађани имају право да захтевају да се унесе промена, а то могу учини и давањем допунске изјаве.[341]

***

И у случају захтева за исправком и за допуном, орган је дужан да поступи по поднетом захтеву без непотребног одлагања, како не би дошло до штете и других негативних последица због нетачног или погрешног податка. Непотребно одлагање је правни стандард који обавезује органе управе на ефикасност у раду и подстиче на брзу измену нетачних и непотпуних података. Ово право постоји и у систему заштите личних података Србије на исти начин као и у систему ЕУ.

[341] Чл. 29, Закона о заштити личних података (2018), чл. 16, Опште уредбе ЕУ.

5.5. Право на ограничење обраде

Право на ограничавање обраде личних података представља појавни и конкретизовани облик начела ограничења сврхе обраде. Право на ограничење обраде личних података је самостално право које помаже остваривању правне сигурности у тренуцима када није сигурно да ће обрада личних података бити законита у будућем периоду. У том смислу, ово право служи као привремена мера спречавања обраде података у случајевима постојања неизвесности у погледу законитости даље обраде података, односно када није познато да ли ће и када лични подаци бити обрисани из база података органа (руковаоца).

Право на ограничење обраде делује у посебним ситуацијама провере тачности личних података (до утврђивања тачних и потпуних података од стране органа). Даље, у случају незаконите обраде личних података, када постоји противљење лица на кога се подаци односе да се обришу (већ се захтева само ограничење обраде). Ово право се остварује и када је отпала првобитна сврха обраде, али су подаци потребни њиховом имаоцу ради остваривања правних захтева. У поменутим ситуацијама ималац може захтевати да се ограничи обрада података, уместо да се лични подаци бришу, па је због тога ово право привременог карактера.

- Право на ограничење обраде у правном систему Србије и правном систему ЕУ

Право на ограничење обраде података представља део система заштите података у Србији. Ово право постоји и у систему заштите личних података ЕУ и уређено је на истоветан начин. У оба правна система, лице на које се подаци односе може захтевати од органа да ограничи обраду личних података у неком од следећих случајева:

1. Када лице на које се подаци односе оспорава тачност података који се обрађују (у овом случају обрада се може ограничити у оном периоду који је неопходан органу да испита тачност навода и тачност података),
2. Уколико је обрада незаконита, али лице на које се подаци односе не тражи брисање тих података, већ тражи ограничење њихове употребе (ради задовољења његових личних интереса),

3. Када више не постоји сврха ради које су се подаци обрађивали, али их лице на које се подаци односе захтева, ради остваривања неког другог интереса (ради подношења или одбране од правног захтева у другом управном или судском поступку),
4. Лице на које се подаци односе је уложило приговор на обраду података, у ком случају орган има обавезу да прекине са обрадом, осим ако предочи да постоје легитимни основи за обраду који претежу над интересима лица чији се подаци обрађују. У овом случају обрада се ограничава до коначне оцене по питању да ли правни основ руковаоца претеже над приватним интересом лица чији су подаци.[342]

У вези са овим правом јавља се обавеза органа, која се односи на дужност обавештавања лица на које се подаци односе о престанку дејства права на ограничење обраде. Како је ово право привременог карактера, орган мора упутити обавештење пре него што установљена ограничења престану да важе. На овај начин остварује се транспарентан рад органа управе и омогућава се остварење принципа управно-правне предвидљивости.

Скрећемо пажњу одлуку управног суда на територији ЕУ, Управног суда Стаде (покрајина Доња Саксонија, Немачка),[343] која се тиче оспоравања тачности података (прва група ситуација у којима се може ограничити обрада података). У конкретном случају, подносилац захтева за ограничење обраде био је подносилац захтева за азил, који је тврдио да подаци који се обрађују о њему нису тачни (подносилац је тврдио да потиче из државе Сијера Леоне, а не из државе Гвинеје), па је захтевао ограничење обраде података. Суд је утврдио да ова ситуација код подносиоца захтева не постоји, будући да је он требао да „оспори“ тачност података, а то у конкретном случају није учињено. Наиме, оспоравање подразумева образложење подносиоца о нетачности података, које је поткрепљено доказима, што код подносиоца захтева није био случај. Подносилац је навео само да има порекло државе Сијера Леоне и да је резервни пасош Гвинеје противправно стекао. На основу тога, Суд је одбио захтев и утврдио важну праксу

[342] Чл. 18, ст. 1, Закона о заштити података о личности, и чл. 31, ст. 1, Опште уредбе ЕУ.
[343] Управни суд Стаде, Одлука бр. Az. 1 B 1918/18, од 09.10.2018. год.

за органе управе који немају дужност да прихвате захтев за ограничење обраде, уколико захтев није образложен и поткрепљен доказима.[344]

У сваком случају, када је поднет захтев за остварење права на ограничење обраде, лични подаци у поседу органа управе могу се обрађивати (у ограниченом обиму), али само уколико постоји пристанак лица на кога се подаци односе. Такође, подаци се могу обрађивати и уколико то налажу интереси заштите права других лица, физичких и правних, као и у случају заштите „значајних јавних интереса“. Дакле, интереси морају бити од ширег значаја за друштвену заједницу или државну организацију, што орган посебно мора оправдати У овом случају примењиваће се институт дискреционе оцене органа управе.

5.6. Право на преносивост података

Једна од основних предности информационо-комуникационих технологија тиче се олакшане комуникације између људи и могућности да се велике количине података брзо и лако размењују. У том контексту, интернет има изузетно значајну улогу, као основно средство путем кога се подаци размењују. Ове компоненте утицале су на многе области друштвеног живота чинећи друштвене токове и правне односе далеко бржим и ефикаснијим. Због тога, можемо рећи да су брза комуникација и преносивост информација „заштитник знак“ модерног дигиталног друштва.

Пратећи такве трендове, грађани користе личне податке у различите сврхе, од куповине преко интернета до решавања пореских и других питања са органима управе. У тим ситуацијама јавља се потреба за брзим преносом личних података до оног лица са којима ступају у одређени правни однос. Они то чине ради добијања квалитетнијих, бржих и ефикаснијих услуга или задовољења неког другог интереса.

Потреба за преносом личних података јавља се и приликом преласка са једног производа на други, односно са једне услуге која се на тржишту нуди на другу. Како би се избегли непотребни трошкови, данас се гарантује могућност

[344] За више о чињеничним елементима овог случаја вид. Kanzlei Bahr, *Kein Recht auf Einschränkung der Datenverarbeitung nach Art. 18*, DSGVO, online 2018, *https://www.datenschutz.eu/urteile/Kein-Recht-auf-Einschraenkung-der-Datenverarbeitung-nach-Art-18-DSGVO-Verwaltungsgericht-Stade-20181009/#* , 07. јануар 2019.

преноса личних података са претходног даваоца услуге на новог. Преносивост података омогућава и остваривање ширих друштвених интереса, као што су бржи економски развој, подстицање конкуренције и умрежавање података са другим гранама права (компанијским правом, интелектуалном својином, потрошачким правом, итд.).[345]

Преносивост података има улогу и у електронској управи. Циљ органа управе је да олакшају остваривање права и интереса грађана. То се конкретизује у обавези органа да по службеној дужности врше увид у податке о чињеницама неопходним за одлучивање, о којима се води службена евиденција.[346] Такође, то се односи и на терен прибављања података потребних за одлучивање врши се електронским путем у што краћем року.[347] Због тога, право на преносивост података можемо посматрати и као оваплоћење законске обавезу органа управе код решавања управних ствари.

Основни циљ овог права јесте да пружи додатне могућности грађанима у контроли над својим подацима који се налазе код других лица. Због тога је увођење овог права у правни систем изузетно значајно. „Законодавцу је на уму било стварање окружења у којем би испитаници могли несметано селити своје податке са услуге на услугу, без обавезе да наставе користити лошију услугу само зато што им се тамо налазе подаци. Тренутно је ситуација таква да се корисници тешко одважују на промјену рачуна, е-поште, календара и сличних апликација због података који се тамо налазе. Циљ преносивости података јест доскочити том проблему…“.[348]

[345] Paul De Hert, *et al,* „The right to data portability in the GDPR: Towards user-centric interoperability of digital services“, *Computer law & security review* (ed. Steve Saxby), Amsterdam – Boston - London 2018, 194.
[346] Чл. 9, ст. 3, Закона о општем управном поступку.
[347] Чл. 103, ст. 2, Закона о општем управном поступку.
[348] GDPR Informer, Službene smjernice o prenosivosti podataka, online 2018, *https://gdprinformer.com/hr/gdpr-clanci/sluzbene-smjernice-o-prenosivosti-podataka,* 12. септембар 2018.

- Право на преносивост података у правном систему Србије и правном систему ЕУ

Право на преносивост података јемчи се у правном систему Србије и у правном систему ЕУ. У поменутим системима право на преносивост уређено је на идентичан начин.

Суштина овог права може се разложити на два посебна овлашћења грађана. Прво овлашћење омогућава лицу на које се подаци односе да добије своје податке од руковаоца који их је обрађивао. У остваривању овог права и овлашћења није важан начин чувања података (у дигиталном облику или на физичкој меморији рачунара). У односу на ово овлашћење, право на преносивост података приближава се праву на приступ личним подацима. Друго овлашћење односи се на могућност имаоца да захтева од руковаоца да његове личне податке проследи (трансферише) другом руковаоцу без ометања.[349] У односу на друго овлашћење руковаоци имају дужност да пренесу на новог руковаоца све податке, и то непосредно, уколико је технички изводљиво.

Ово право може се применити уколико је испуњен један од два услова. Први се односи на случај када се обрада података врши на основу пристанка лица, док се други тиче аутоматске обраде података. У овим случајевима, право на пренос уживају само одређени подаци, који се могу повезати са лицем који захтева пренос. Анонимни подаци не спадају у обим заштите овог права.[350]

Ипак, ово право се не сме вршити малициозно, већ мора бити у сагласности са правима и интересима других лица. То значи да када постоје подаци који се тичу више лица, руковалац има дужност да пренесе све податке, али нови руковалац нема право да обрађује податке других лица, већ само оног лица на кога се пренос односи. Како се наводи „не постоји обавеза финансијске институције да одговоре на захтев за пренос личних података као део њихове обавезе на пренос, када то може довести до повреде њихове обавезе спречавања прања новца или других финансијских злочина“.[351]

[349] Чл. 36, ст. 1, Закона о заштити података о личности (2018), и чл. 20, ст. 1, Опште уредбе ЕУ.
[350] Article 29 Data Protection Working Party, Guidlines on the right to data portability, 16/EN WP 242 rev.01, online 2017, 9, *file:///C:/Users/Win/Downloads/wp242_rev01_enpdf.pdf*, 11. септембар 2018.
[351] *Ibid*., 8.

Сматрамо да своју примену ово право налази и у делатностима органа управе, преко института јединственог управног места. Јединствена сервисна магистрала омогућава органима који не воде одређене личне податке, већ се они налазе код других органа, да им приступе електронским путем захваљујући дигиталним базама података органа управе. То значи да и разни централни, односно децентрализовани органи могу приступити централизованим базама података које, примера ради, води један орган, захваљујући информационо-комуникационим системима електронске управе. На тај начин, долази до усклађивања принципа електронске јавне управе и система заштите података.

Праву на преносивост података кореспондира обавеза руковаоца да достави податке лицу или другом руковаоцу по избору лица у „структуираном, уобичајеном и машински (електронски) читљивом формату“. То значи да подаци морају бити уобличени у формату који дозвољава лако сналажење, који се обично користи у правном промету и који може бити рачунарски обрађен.

5.7. Права грађана у вези са аутоматском обрадом личних података

Развој модерних технологија довео је до тога да, на основу претходно постављених правила и улазних елемената, рачунар може сам анализом доћи до предвиђања одређене појаве. Рачунарски програми који аутоматским путем долазе до предвиђања резултата показали су се као изузетно корисно средство у доношењу различитих пословних одлука, санирању економских губитака и у процесу одлучивања у свакодневним стварима. Такво одлучивање помаже око избора најкраћег пута до циља, обавештавања о променама на берзи, променама временских прилика, избору најповољније понуде на тржишту и томе слично.

Велику улогу у доношењу аутоматизованих одлука имају велике базе података у којима се чувају различити подаци, као улазни елемент у процењивању појава и доношењу аутоматизованих одлука. Због тога, аутоматско доношење одлука налази своје место у области финансија, медицине, образовања, спорта, туризма и многим другим.

Илустрације ради, аутоматизована одлука била би у случају програма који на основу претходног живота лица, броја учињених преступа и прекршаја, раније осуђиваности, личних прилика у којима то лице живи, породице и других

фактора, установи да није оправдано пустити конкретно лице на условни отпуст у случају издржавање казне затвора. То је чисто аутоматска одлука која је заснована на обради личних података, по претходно постављеним правилима. Међутим, аутоматско доношење одлука базира се на различитим подацима који служе као полазни елементи на основу којих се врши анализа и доносе одлуке. Овде се могу наћи и оне одлуке које се тичу личних ситуација и стања грађана. Због тога, увођење ових технологија може угрозити приватност грађана у односу на органе управе. Такође, ако се поставе погрешни полазни параметри, могуће је да се донесе и погрешна одлука. Примера ради, неко лице не буде пуштено на условни отпуст.

Електронска јавна управа своје деловање заснива на информационо-комуникационим системима који се могу користити и аутоматским начинима доношења одлука. Имајући у виду количину личних података грађана у поседу органа управе, као и области друштвеног живота у којима ови органи обављају делатности, поставља се питање како заштити приватност грађана у односу на аутоматско доношење одлука ?

Рачунарски системи функционишу на бази установљених техничких алгоритама без улажења у дубљи друштвени контекст конкретног случаја, што елиминише из таквог одлучивања моралну и емотивну компоненту. Такође, аутоматске одлуке које се доносе на основу личних података могу довести до ситуација које угрожавају приватност грађана, јер резултати до којих рачунар дође, могу бити искоришћени, а да лице на које се подаци односе није упознато са тим. Примера ради, може се догодити да рачунарски програми немају у виду целокупну друштвену ситуацију грађана, па резултати могу довести до неоправданих подела међу људима, „етикетирања“ лица и томе слично. Зато је важно установити право грађана да се заштите од „рачунара“, односно од потпуно аутоматски донетих одлука.

5.7.1. Права грађана у вези са аутоматизованим доношењем одлука у правном систему Србије и правном систему ЕУ

Како би заштити грађане од нежељених последица аутоматских одлука рачунарских програма, системи заштите података признају грађанима посебно право у вези са таквим начином доношењем одлука. Такав је случај са правним системом Србије и правним системом ЕУ. У овим системима предвиђено је право лица чији су подаци да одлучи о томе да ли ће се на њега примењивати одлука која је донесена искључиво на основу аутоматске обраде личних података од стране рачунарског програма. Таква одлука мора имати одређени правни значај, па се имају у виду само оне одлуке које производе правне последице или које значајно утичу на права и интересе одређеног физичког лица.

Осим аутоматске обраде података, грађани имају право да одлуче да ли ће се на њих примењивати и одлуке које се заснивају на „профилисању“. Профилисање се одређује као начин аутоматске обраде података који користи личне податке ради предвиђања и разумевања појединих личних аспеката живота и навика у односу на одређено лице, а посебно у вези са предвиђањем квалитета личних и професионалних способности, финансијском ситуацијом, здравственим стањем, афинитетима и другим карактеристикама које говоре више о самом профилу (личности) одређеног лица.

Као пример за одлучивање на основу профилисања и аутоматске обраде података можемо навести рачунарске програме у здравству, као важном сегменту јавног сектора. Рачунарски програми у здравству могу сврстати одређено лице у категорију лица која је најподложнија срчаним болестима. Ово профилисање не значи да лице већ болује или ће боловати од поменутих обољења. Зато, лице може дати изјаву којом прихвата аутоматску обраду личних података, засновану на претходно постављеним здравственим параметрима.[352]

Свакако, лице чији се подаци користе у аутоматској обради података мора имати могућност да изнесе свој став у вези са конкретном одлуком (уколико је то потребно), као и да уложи правна средства уколико сматра да одлука није правилна или законита. Са друге стране, орган мора предузети адекватне мере да

[352] *Ibid*., 18.

би заштитио права и интересе лица чији се подаци користе код аутоматске обраде података. Орган ће то чинити укључивањем људског фактора у контролу процеса аутоматизоване обраде и ревизијом донетих одлука (закључака) рачунара, од стране надлежног лица. Заштитне мере захтевају и да се избегне неоправдано прављење разлике између људи, односно да се дође до диксриминативних одлука.

Захваљујући овом праву грађани имају могућност да самостално одлучују о томе да ли ће поверити одлучивање о личним питањима рачунарским програмима.[353] На тај начин остварују се основни принципи заштите личних података као што су транспарентност, законитост обраде, заштита легитимних интереса лица чији се подаци обрађују, итд. Уз то, остварују се и основни принципи управног права, попут права странке да учествује у поступку и да се изјасни о чињеницама од значаја за свој предмет. То значи да је за сваки систем заштите неопходно успостављање равнотеже између нових технологија и људских права, како би друштво могло неометано да напредује, чувајући при томе појединачна права и интересе.

5.7.2. Ситуације у којима је дозвољена аутоматска обрада података о личности

У одређеним случајевима грађани не могу да избегну примену резултата аутоматске обраде података. Разликујемо три групе случаја у којима се мора прихватају резултати аутоматске обраде података.

Прва група случаја односи се на ситуацију када је одлука донета на основу посебног прописа који дозвољава аутоматску обраду. На овај начин оставља се могућност да се у посебним случајевима у којима органи управе обављају важне друштвене послове (као што је национална безбедност и јавно здравство нпр.) омогући аутоматска обрада личних података као правило. Свакако, пропис који дозвољава аутоматску обраду података мора бити посебно образложен, заснован на легитимним очекивањима грађана и у складу са системом заштите података. Сматрамо да није упутно дозволити овакав начин обраде података, будући да

[353] За критике у вези са правом на аутоматску обраду вид. Sandra Wachter, Brent Mittelstadt, Luciano Floridi, „Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation“, *International Data Privacy Law*, No. 2/2017 (ed. Nora Ni Loideain), Oxford 2017, 76-99.

рачунарски програми нису на том степену развоја да могу доносити одлуке на исти начин као и човек.

Друга група се односи на ситуацију када је аутоматска обрада података потребна ради склапања и извршења правног односа између лица чији су подаци и руковаоца (органа управе). У одређеним ситуацијама, руковалац има потребу да се ослони искључиво на аутоматске начине обраде личних података, а лица чији се подаци обрађују имају потребу да са руковаоцем ступе у одређени правни однос. Примера ради, код расписивања конкурса за посао у органима јавне управе може се пријавити велики број кандидата. Послодавац (орган) може се одлучити да се аутоматски направи ужи круг кандидата на основу претходно унетих параметара. У тој ситуацији оправдана је употреба аутоматске обраде, будући да кандидати желе да ступе у пословни (правни) однос са руковаоцем (органом управе). То значи да кандидати својом пријавом, имплицитно пристају на аутоматску обраду података.

Трећи и последњи случај односи се на давање изричитог пристанка на аутоматизовану обраду лица чији се подаци обрађују.[354] Будући да пристанком лице износи свој став о томе да сматра да су му заштићена права и интереси, нема препреке за вршење аутоматске обраде података.

Даљим усавршавањем информационо-комуникационих технологија и посебно вештачке интелигенције, развијаће се и степен правилности и тачности резултата аутоматизованих обрада. До тада, неопходно је пружити грађанима сигурност у односу на аутоматску обраду њихових личних података и сузити простор за нове технологије, у случајевима када је људски фактор поузданији од технолошког.

[354] Чл. 22, ст. 2, Опште уредбе ЕУ.

5.8. Право на правно средство у вези са обрадом личних података

5.8.1. О појму права на правно средство

Како би правне норме могле да остварују своје друштвену улогу неопходно је да их поступајући орган правилно примени у сваком појединачном случају. Ипак, постоји вероватноћа да појединачни правни акти које управни органи доносе или управне радње које врше буду незаконите. Због тога, као важно средство правног система којим се обезбеђује законитост одлука и рада управних органа, јавља се право на правно средство, односно право на правни лек. Сматра се да држава омогућава грађанима право на правни лек, као субјективно јавно право које спречава државну самовољу и омогућава контролу над монополом државе и њених органа, што омогућава остваривање легитимних интереса грађана и могућност контроле неправилних и незаконитих одлука.[355] Због тога, „право на правни лијек тијесно је повезано са појмом људских права уопће, посебице и због тога што и само право на дјелотворан правни лијек спада у основна људска права“.[356]

Правно средство, односно правни лек, представља овлашћење незадовољног лица (странке у управном поступку) да оспори одређену појединачну одлуку која производи правна дејства или управну радњу која има посредно правно дејство, на тај начин да одлука буде испитана од стране надлежног надзорног органа.

Значај права на правно средство препознат је у најважнијим међународним документима. Тако, у Општој декларацији о правима човека[357] гарантовано је свакоме право на делотворно правно средство против аката којима се крше основна права гарантована уставом или законом.[358] Декларација садржи и обавезу држава да омогуће правним нормама остваривање овог права. Такође, Европска конвенција за заштиту људских права и основних слобода[359] посвећује пажњу

[355] Tadija Bubalović, „Pravo na pravni lijek protiv odluka tijela državne vlasti prema domaćem i međunarodnom pravu“, *Zbornik sveučilišta Libertas*, br.3/2018, Libertas međunarodno sveučilište, Zagreb 2018, 266.
[356] *Ibid.*
[357] Општа декларација о правима човека, Организација Уједињених нација, 1948.
[358] Чл. 8, Опште декларација о правима човека.
[359] Европска конвенција за заштиту људских права и основних слобода, Савет Европе, Рим, 1950.

праву на делотворни правни лек.[360] Од важнијих међународних докумената, право на правни лек познаје и Међународни пакт о грађанским и политичким правима.[361]

5.8.2. Право на правно средство у управном поступку

Право на правни лек представља незаобилазни елемент у свим гранама правама, па постоји у кривичном, грађанском, управном, итд. Према томе, правни систем не може се замислити без могућности улагања правног лека, односно правног средства које омогућава грађанима да изразе своје незадовољство неправилним и незаконитих одлукама и радњама управних органа. Једино се на тај начин може остварити контрола законитости и правилности рада органа јавне управе у вези са личним подацима грађана, јер „...када је реч о правној контроли управе, онда се том појму мора додати још један елемент више: онај ко контролише треба да је у стању да врши известан утицај на рад контролисаног".[362]

Правни лек представља важан институт управног права где се обично остварује кроз право на правно средство. „Правна средства представљају процесне радње предвиђене правним прописима којима се омогућава побијање незаконитих и неправилних аката донетих у управном поступку".[363] Основна сврха правног средства је да осигура доношење законите и правилне одлуке органа управе у појединачном случају. На тај начин долази до задовољења јавног и приватног интереса. Јавни интерес је задовољен будући да се тиме остварује примена основних демократских принципа, као што су начело законитости, начело правне државе, јединствености правног поретка, итд. Са друге стране, приватни интерес је задовољен будући да су опште правне норме правилно примењене у односу на чињенице конкретног случаја, као и да је извршена контрола рада првостепеног органа и његовог акта.[364]

Правно средство јесте инструмент надзора над радом органа управе који омогућава законито и правилно одлучивање у сваком поједином случају. Значајна

[360] Чл. 13, Европске конвенције за заштиту људских права и основних слобода.
[361] Међународни пакт о грађанским и политичким правима, Генерална скупштина УН, 1966.
[362] Nikola Stjepanović, *Upravno pravo u SFRJ – opšti deo*, knjiga II, Prosvetni pregled, Beograd 1973, 221.
[363] Д. Милков (2017), 222.
[364] Упор. *Ibid*.

улога вишестепених органа огледа се у обавези надзираног органа да поступи према инструкцијама и предлозима надзорног органа, у вези са решавањем конкретног случаја. На тај начин се ствара управна пракса која олакшава рад органа управе и омогућава остваривање правне предвидљивости. Оно подразумева могућност правно релевантног изношења мишљења, односно тврдње незадовољног лица да је појединачно одлука у његовом случају незаконита или неправилна.

У позитивном управном праву Србије постоје два редовна правна средства, жалба и приговор. Жалба представља опште управно правно средство које се може уложити против свих управних решења донетих у првом степену. Приговор јесте редовно правно средство који се може уложити против посебних, законом предвиђених аката управе (управни уговори, управне услуге, управне радње). На одлуку донету по приговору може се уложити жалба.[365]

Могло би се рећи да се право на правно средство састоји у могућности оспоравања одлуке, односно другог поступања првостепеног органа управе, што означава јавно-правну могућност лица да се правно супротстави неповољном акту. У оспоравању се налазе елементи неслагања, који чине основу захтева незадовољног лица да поништи или укине одлуку, „што означава право грађана да очекују и захтевају стварну, али и процедуралну праведност“.[366]

5.8.3. Право на правно средство у вези са личним подацима у правном систему Србије и правном систему ЕУ

Право на правно средство у вези са обрадом личних података регулисано је на истоветан начин у правном систему Србије и правном систему ЕУ. У правном систему Србије, Устав гарантује право на једнаку заштиту права грађана пред органима управе. То значи да свако има право на жалбу или друго правно средство против одлуке којом се одлучује о његовом праву, обавези или на законом заснованом интересу.[367] Закон о заштити података о личности (2018) познаје „прао на приговор“ као правно средство против одлука и обрада личних података које су неправилне или незаконите.

[365] Упор. *Ibid*., 224.
[366] T. Bubalović (2018), 268.
[367] Чл. 36, ст. 2, Устава РС.

„Ако сматра да је то оправдано у односу на посебну ситуацију у којој се налази, лице има право да у сваком тренутку поднесе приговор на обраду података о личности који се на њега односе (*у вези са обрадом која је неопходна у циљу обављања послова у јавном интересу или извршења овлашћења руковаоца, обраду која је неопходна у циљу остварења оправданих интереса руковаоца или трећих лица* (додао аутор)), укључујући и профилисање које се заснива на овим одредбама. Руковалац има обавезу да прекине са обрадом података о лицу које је поднело приговор, осим ако је предочио да постоје легитимни основи за обраду који претежу над интересима, правима или слободама лица на који се подаци односе, или су у вези са подношењем, остваривањем, односно одбраном од правног захтева“.[368] Дакле, лице може поднети приговор у сваком тренутку у односу на обраду његових личних података. Језички тумачећи, ово значи да се приговор може поднети без временског ограничења против обрада које су завршене, као и против обрада које су у току.

Ипак, приговор се може уложити само у појединим случајевима обраде личних података. Прво, органи управе у вршењу многих послова морају да користе личне податке грађана. У тим ситуацијама, подаци грађана могу бити угрожени, па им се признаје право на приговор против обраде која је неопходна за извршење одређеног посла из надлежности органа. Други случај тиче се ситуација у којима орган управе обавља послове из своје надлежности, у корист једног лица (чији интерес претеже), па је за решавање поступка неопходно обрадити личне податке неког другог лица. Та лица, иако нису учесници у управном поступку, имају интерес да заштите своје личне податке, па могу уложити приговор. Такође, у случају аутоматских обрада података о личности, лице чији се подаци аутоматски обрађују може уложити приговор.

Када је уложен приговор, орган мора да престане са обрадом података како би се спречио евентуални настанак штете. Орган има могућност да настави са обрадом, уколико образложи легитимну потребу за обрадом података која је важнија од интереса лица чији су подаци и које је уложило приговор. Када се

[368] Чл. 37, ст. 1, Закона о заштити података о личности (2018), и чл. 21, ст. 1, Опште уредбе ЕУ.

обрађују лични подаци у циљу припремања одбране од правног захтева, орган нема обавезу да прекине са обрадом.

Важан елемент права на приговор представља обавеза органа да приликом првог успостављања контакта са лицем чији ће се подаци обрађивати, упозна то лице са постојањем могућности да изјави приговор. На тај начин повећава се правна сигурност, а уједно се орган „подсећа“ на своју обавезу да законито и правилно обрађује личне податке. Орган то мора учинити на начин који омогућава да се странка јасно упозна са могућношћу изјављивања приговора. Ова обавеза органа може се извршити и електронским путем.

Једно од најважнијих питања у вези са правом на приговор јесте начин поступања по приговору, односно правила поступка по приговору. Наиме, Закон о заштити података о личности (2018) и Општа уредба ЕУ не садрже детаљнију регулативу у вези са питањем поступка који руковалац треба да спроведе по примљеном приговору.

Поменути прописи једино предвиђају да орган има рок од 30 дана од дана пријема захтева да обавести лице о основаности његовог захтева. Рок се може продужити за исти временски период уколико је захтев сложен или се односи на велики број података. Ако пропусти поменуте рокове, јавља се обавеза органа да обавести лице које је уложило приговор да има право на притужбу Поверенику, односно тужбу суду.

5.8.4. Однос правила општег управног поступка у вези са правом на приговор против обраде личних података у правном систему Србије

Право на приговор предвиђено Законом о заштити података о личности (2018) односи се на обраде личних података коју врше како субјекти приватног права, тако и органи управе. Уколико су предвиђена посебна правила за поједину управну област, орган ће поступати по правилима посебног управног поступка. Међутим, органи управе дужни су да поступају по правилима општег управног поступка, који је уређен Законом о општем управном поступку, уколико нису предвиђена посебна правила. Органи поступају по одредбама овог закона када

непосредно примењују законе, друге прописе и опште акте на појединачну ситуацију и тиме правно или фактички утичу на положај странке.[369]

Будући да у области заштите података нису предвиђена посебна правила за поступање по правним средствима, органи управе су дужни да поступају по правилима Закона о општем управном поступку, али уз уважавање правила која уређују области заштите личних података.

5.8.4.1. Правна природа и однос права на приговор у управном поступку и права на приговор у систему заштите личних података

Питање односа обраде података и права на приговор од изузетног је значаја за правну сигурност. Наиме, правна природа права на приговор, као правног средства из Закона о општем управном поступку, није идентична праву на приговор предвиђеном у Закону о заштити података о личности (2018). Овде се јавља проблем, будући да су органи управе дужни да поштују одредбе оба закона.

У зависности од тога која ће правила применити у конкретном случају, зависи и низ других елемената. Они се тичу надлежности органа за поступање по приговору, временских рокова за доношење решења по приговору, могућности улагања тужбе управном суду против коначне одлуке органа управе, итд. Због тога је потребно испитати правну природу права на приговор из области заштите личних података и одредити његов однос са приговором из општег управног поступка, јер од тога зависи заштита права грађана и сигурност правног система.

Сваки правни захтев у вези са личним подацима које обрађују органи управе покреће механизам управног деловања, што усмерава орган да поступа у складу са правилима општег управног поступка. Закон о општем управном поступку, као основни закон у материји управног поступања, наводи да се другим законом могу уредити само поједина питања и то ако постоји потреба за посебном регулативом, под условом да се поштују начела општег управног поступка и да се тиме не угрожава постигнути ниво заштите права и правних интереса странака. Дакле, органи управе су дужни да поступају по одредбама Закона о општем управном поступку у односу на процесна питања која се тичу обраде и заштите

[369] Чл. 2, ст. 1, Закона о општем управном поступку.

личних података, што се односи и на поступак по правним средствима изјављеним у вези са обрадом личних података.

Као што је поменуто, у позитивном управном праву Србије постоје два редовна правна средства, жалба и приговор. Жалба се у случајевима обраде личних података не може изјавити, будући да се она изјављује против решења првостепеног органа. Како орган нема обавезу доношења решења у вези са обрадом, тако се жалба не може користити у овом случају.

Приговор се може изјавити због неиспуњавања обавеза из управног уговора, због незаконите управне радње, пропуштања предузимања управне радње или због неадекватног начина пружања јавних услуга.[370] У односу на изложене разлоге за изјављивање приговора управном органу, приговор у вези са обрадом личних података можемо уподобити приговору против управне радње или пропуштања њеног предузимања.

Управне радње су материјални акти органа управе које немају непосредно правно дејство, али фактички утичу на правну позицију грађана. Са друге стране, обрада личних података коју врше органи управе могла би се окарактерисати као врста управне радње.[371] Обрада не представља правни, већ фактички (материјални) акт који има утицаја на права и обавезе лица чији се подаци обрађују, а односи се на конкретно лице, односно правну ситуацију.

Међутим, уколико се прихвати став да обрада личних података коју врше органи управе представља управну радњу, долазимо до питања по којим правилима је дужан да поступи орган (руководилац) који обрађује податке? Од одговора на ово питање зависе друга процесна питања (дужина рокова за решавање по приговору, могућност улагања жалбе на одлуку по приговору, могућност вођења управног спора, итд.).

Аутор сматра, у односу на тренутно позитивно-правно решење, да поступак по приговору на обраду података треба да се води по правилима општег управног поступка, уз уважавање одређених посебности система заштите личних података. При томе, не сме се изгубити из вида да степен заштите мора бити најмање исти или већи од оног предвиђеног општим управним поступком. На овај

[370] Чл. 147, ст. 1, Закона о општем управном поступку.
[371] За више о појму и врстама управних радњи, вид. Д. Васиљевић (2015), 221-232.

начин се не смањује ниво правне заштите који је предвиђен правилима општег управног поступка.

Закон о заштити података о личности (2018) омогућава изјављивање приговора у било ком тренутку, док се приговор на управну радњу, према Закону о општем управном поступку, може изјавити у року од 15 дана од пропуштања да се предузме управна радња или од предузимања исте. То значи да лице чији се подаци обрађују ужива виши степен правне заштите по посебном закону, па орган треба да примени посебан пропис у погледу рока за изјављивање приговора.

Даље, рок за доношење одлуке по приговору и по једном и по другом закону износи 30 дана. Ипак, правила поступка и одлучивање о самој садржини приговора треба вршити по правилима општег управног поступка, будући да нису прописана посебна правила за поступању по приговору на обраду личних података. То значи да се по приговору на обраду личних података руководилац органа одлучује управним актом, односно решењем.

5.8.4.2. Питање надлежности за одлучивање по приговору против обраде личних података

Као додатак дилеми о општем и посебном поступку, поставља се питање који орган је надлежан да поступа по приговору на обраду личних података коју врше органи управе? Закон о заштити података о личности (2018) предвиђа Повереника за информације од јавног значаја и заштиту података о личности као орган коме се странка може обратити приговором у вези са обрадом личних података.

Међутим, управни орган који одлучује као првостепени у управном поступку, по правилу има надзорни, односно другостепени орган. Како се лични подаци могу обрађивати од стране органа управе у оквиру управног поступка, ради сагледавања чињеница конкретног случаја и извођења доказа, о приговору на обраду може одлучивати и надзорни орган, који је надлежан да одлучује по жалби и приговорима у вези са управном ствари која је предмет поступка.

Како се у управном поступку приговор изјављује руководиоцу органа на чије се поступање односи, он и одлучује по приговору на обраду личних података. Међутим, у другом степену, због природе решења управног органа које се побија (решење по приговору на обраду личних података) сматрамо да је целисходно да

о њему одлучује Повереник за информације од јавног значаја и заштиту података о личности, а не другостепени управни орган. Служба Повереника својим стручним компетенцијама и квалификацијама у материји личних података, гарантује разумевање потребе за пружањем заштите личним подацима грађана, посебно у вези са поступањем управних органа.

Такође, у случају обраде података реч је о посебном управном поступку, па треба следити правила посебног закона. Свакако, странка би морала да добије помоћ од првостепеног органа по питању ком органу може да се обрати у циљу заштите од незаконите или неправилне одлуке или незаконитог поступања у вези са личним подацима.

Будући да смо обраду личних података квалификовали као управну радњу, у случају да је обрада личних података део управног поступка (због утврђивања чињеничног стања), лако се могу издвојити елементи поступка који се тичу обраде личних података и доставити Поверенику на одлучивање.

Поменутим тумачењем долазимо до задовољавајућег решења у коме ће грађанима бити омогућена правна заштита када органи управе обрађују личне податке. Наравно, странка не би требала да трпи штетне последице у колико је орган упути да остварује своје право на правно средство пред другостепеним управним органом. У таквим ситуацијама, другостепени орган требао би да проследи предмет по жалби Поверенику на одлучивање, као стварно надлежном органу.

6. ОГРАНИЧЕЊА ПРАВА У ВЕЗИ СА ОБРАДОМ ЛИЧНИХ ПОДАТАКА

Права у вези са заштитом личних података од велике су важности за правну сигурност грађана. Она представљају темељ система заштите података, без којих грађани не би могли да се поуздају у сигурност њихове приватне сфере пред органима управе. Ипак, као и код осталих људских права, постоје случајеви у којима се од загарантованих права мора одступити. Ови изузеци морају бити посебно предвиђени како се не би злоупотребљавали и редовно користили. Због тога, од примарног је значаја уско одредити ситуације које оправдавају одступања од гарантованих права.

Пракса установљавања изузетака и могућност одступања од људских права позната је у најважнијим међународним документима који промовишу људска права и обавезе држава у вези са њиховим поштовањем. Тако, у Универзалној декларацији о људским правима наводи се да „у вршењу својих права и слобода свако се може подвргнути само оним ограничењима која су предвиђена законом у циљу обезбеђења нужног признања и поштовања права и слобода других и општег благостања и у циљу задовољења правичних захтева морала, јавног поретка и општег благостања“.[372] Могућности ограничења људских права предвиђена су и Европском конвенцијом за заштиту људских права и основних слобода. Међутим, Конвенција предвиђа и границу ограничења која су дозвољена, па наводи да се предвиђена ограничења неће примењивати у друге сврхе, осим оних које су дозвољене Конвенцијом.[373] Ову праксу прате и правни системи држава широм света.

Поменуто стање ствари присутно је и у систему заштите личних података. У правним системима предвиђају се ситуације које оправдавају ограничење уживања права у вези са личним подацима. Те ситуације обично стоје у вези са неким од појавних облика јавног интереса. То значи да јавни интерес може створити потребу да обрада одређених података буде претежнија од поштовања појединог права, па се у конкретном случају људско право неће примењивати.

Ипак, и у таквим ситуацијама неопходно је користити се најмањим могућим степеном одступања од појединог права, односно „најнужнијом мером коју захтева ситуација“.[374] Нужност мера односи се на ускраћивање права искључиво у односу на конкретну ситуацију, али и ускраћивања права само онолико колико је потребно. Уз то, неопходно је јасно образложити јавни интерес и разлог за ускраћивањем појединог права.

---

[372] Чл. 29, ст. 2, Универзалне декларације о људским правима.

[373] Чл. 18, Европске конвенције за заштиту људских права и основних слобода. У погледу права на приватност, Конвенција је предвидела да се јавне власти неће мешати у приватност грађана, осим уколико је то у складу са законом и ако потребе демократског друштва то захтевају, а посебно интереси националне и јавне безбедности, економског развоја, јавног здравља и морала, као и права и слобода грађана.

[374] Milan Paunović, Boris Krivokapić, Ivana Krstić, *Međunarodna ljudska prava*, Pravni fakultet Univerziteta u Beogradu, Beograd 2013, 65.

6.1. Ограничења права у вези са личним подацима у правном систему Србије и правном систему ЕУ

Закон о заштити података о личности (2018), на исти начин као и Општа уредба ЕУ, предвиђа ситуације у којима се, под одређеним условима, могу ограничити одређена права у вези са обрадом података (право на увид, обавештење, преносивост, приговор, итд.). Ситуације се односе на случајеве када је потребно заштити националну безбедност, јавну безбедност грађана и државе, предузети одређене радње у вези са кривичним поступком (спречавања кривичног дела, истраге и гоњења учиниоца кривичних дела), заштитити привредне и финансијске интересе државе, независност правосуђа и судских поступака, спровести регулаторну улогу државе, заштитити основна људска права лица на које се подаци односе, итд.[375]

Ситуације у којима је могуће увести ограничење права у вези са обрадом података, обично су у вези са пословима органа управе, будући да су они задужени за заштиту јавног интереса. Због апстрактне формулације изузетака и сложености послова органа управе, поменуте ситуације захтевају и одређени степен дискреционог одлучивања у односу на то да ли конкретан случај оправдава ускраћивање појединог права.

6.1.1. Могућност ограничења права у вези са заштитом података у правном систему ЕУ

Како би се смањио простор за злоупотребе и погрешне процене, Општа уредба ЕУ прописује да се ограничење појединог права може увести „једино законом“, ако се на тај начин поштује суштина основних права и слобода грађана. Уз то, ограничавајуће мере морају да буду сразмерне и у складу са принципима демократског друштва. Ово је изузетно значајна одредба, јер не допушта дискрециону оцену органа управе да ли ће ускратити или ограничити појединo право у вези са обрадом, већ органи могу поступити једино на основу закона. Законодавни орган је једина грана власти која може проценити да ли се у одређеном случају треба прописати могућност ограничења појединог права. Ови

[375] Чл. 23, ст. 1, Опште уредбе ЕУ.

изузеци пролазе кроз филтере правне контроле надлежних одбора и правну контролу уставности и законитости уставног суда.

6.1.2. Ограничења права у вези са заштитом личних података у правном систему Србије

За разлику од правног система ЕУ, Закон о заштити података о личности (2018) прописује да се права „могу ограничити ако та ограничења не задиру у суштину основних права и слобода и ако то представља неопходну и сразмерну меру у демократском друштву“.[376] У овој одредби не постоји одредница да ограничења могу бити уведена једино законом, што оставља широко поље дискреционе оцене управних органа у ограничавању људских права.

Поставља се питање да ли оваква одредба законодавца уопште дозвољава дискреционо одлучивање, будући да орган нема понуђене опције на основу којих може поступити? Прописани критеријуми на основу којих се врши процена оправданости ограничења представљају основу за вршење дискреционих овлашћења органа управе. За дискреционо одлучивање се наводи да представља „право избора између више могућих и правно допуштених алтернатива у конкретном случају“.[377] Такво одлучивање има позитивних и негативних аспеката, будући да омогућава избегавање правно-техничких немогућности да се уреде све могуће животне ситуације. У литератури се наводи да дискрециона оцена доприносу утемељењу друштвене сигурности и правичности, као и то да у појединим ситуацијама законодавац нема посебна знања из поједине области друштвеног живота, те је адекватније оставити могућност оцене у одређеним питањима управном органу, будући да је он у непосредном односу са грађанима и конкретном ситуацијом.[378]

Свакако, када доноси одлуку о ускраћивању појединог права „треба имати у виду да се и у тим случајевима орган управе налази под правним поретком, што значи да приликом бирања између више алтернатива у конкретном случају, мора

[376] Чл. 40, ст. 1, Закона о заштити података о личности (2018).
[377] Д. Васиљевић, *Законитост управе и дискрециона оцена*, Криминалистичко-полицијска академија, Београд 2012, 99.
[378] Мирјана Дреновак Ивановић, *Дискрециона оцена у управном праву Србије са освртом на упоредно право и европске стандарде*, Правни факултет Универзитета у Београду, Београд 2011, 16.

да изабере ону, која по његовој оцени најбоље одговара јавном интересу, а не интересу неког појединца или неке уже групе“.[379]

Дакле, органи управе имају на располагању дискрециону могућност одлучивања о ускраћивању појединог права у вези са личним подацима. У сваком случају, како би одлука о ускраћивању била законита и легитимна, она мора бити заснована на анализи и процени одређених критеријума. Ти критеријуми су следећи:

1. Сврха или врста обраде,
2. Врсте података о личности,
3. Обим ограничења,
4. Мере заштите у циљу спречавања злоупотребе, недозвољеног приступа или преноса податка,
5. Особености руковаоца,
6. Временски период чувања и применљиве мере заштите,
7. Ризике по права и слободе лица,
8. Право на информисање о ограничењу.[380]

Дакле, могућност ограничења права у вези са заштитом података увео је закон, али он дозвољава да о ограничењима одлучују органи управе (појединачним или подзаконским општим актима). То значи да је законодавац са постављеним критеријумима успоставио ограничења, односно параметре за дискрециону оцену, јер он није у могућности да регулише све могуће животне ситуације, па тим препушта одлуку управним органима, који имају директан однос са грађанима и конкретним ситуацијама. У том смислу, треба јачати способност службеника да могу квалитетно да доносе дискреционе одлуке по овим питањима. У пракси остаје да се види на који начин ће бити примењивана одредба о ускраћивању права од стране органа управе.

[379] Д. Васиљевић (2012), 99.
[380] Чл. 40, ст. 2, Закона о заштити података о личности (2018), и чл. 23, ст. 2, Опште уредбе ЕУ.

6.2. Основни принципи ограничења права на приватност

Да би мере којима се ограничава уживање појединог права биле легитимне, закон мора бити предвидљив и доступан јавности, а мере ограничења морају бити пропорционалне (да што мање ограничавају људско право). То су ставови заузети од стране највиших судских инстанци, попут Европског суда за људска права и Уставног суда Србије, приликом оцене да ли су ограничавајуће мере адекватне, довољне и дозвољене у демократском друштву. Једино уколико се поштују принципи за увођење ограничавајућих мера, може се очекивати заштита приватности грађана.

Доступност прописа (закона) јавности значи да грађани имају могућност да се без већих потешкоћа упознају са текстом прописа и одредбама које представљају ограничење права. У предмету *Mikhaylyuk and Petrov v. Ukraine*[381] који се нашао пред Европским судом за људска права, поставило се питање да ли се може ограничити право на приватност, односно право на преписку, министарским одлукама који су интерне природе, али су акт надлежног органа.

Предмет се односио на повреду преписке затвореника, чиме се ограничило њихово право на приватност. Тужена страна (држава) је истакла да је поступала законито, те да је имала правни основ за ограничење права у виду одлуке министра. Европски суд за људска права је стао на становиште да на овај начин повређено право на приватност и право на преписку затвореника. Наиме, ограничавајуће мере нису биле доступне затвореницима, јер се радило о интерном акту који није доступан јавности, те он не може представљати адекватан правни основ за ограничење права на приватност, односно права на преписку.

Предвидљивост прописа (закона) представа други неопходан елемент за легитимно ограничење одређеног права. Предвидљивост је својство закона које омогућава грађанима да имају легитимна очекивања на основу општих правних норми. Пропис је предвидљив када грађани знају шта могу да очекују од општих правних норми, односно каква су њихова права, дужности и обавезе према том закону. Наравно, општи правни акти не регулишу сва питања поједине области,

[381] *Mikhaylyuk and Petrov v. Ukraine*, app no. 11932/02, Европски суд за људска права, 2009.

већ се конкретизација општих правних норми често врши подзаконским општим и појединачним правним актима.

На таквом становишту је и Европски суд за људска права који наводи да закони не могу бити у потпуности прецизни, већ могу садржати и апстрактне појмове који се конкретизују у пракси.[382] У предмету *Rotaru v. Romania*[383], још једном је потврђен принцип предвидљивост као важан сегмент приликом ограничења права на приватност и право на заштиту личних података.

Подносилац представке сматрао је да му је повређено право на приватност, будући да су румунске тајне службе годинама прикупљале његове личне податке. Суд је установио да румунски закони нису предвиђали могућности ограничења права у вези са личним подацима и приватношћу, посебно не актима управних (државних) служби. На тај начин повређено је право на приватност подносиоца представке, будући да он ни на који начин није могао очекивати такво мешање јавних власти у личну сферу.

О принципу предвидљивости изјаснио се и Уставни суд Србије. *У одлуци ИУз-252/2002*[384] суд је оцењивао уставност одредби Закона о безбедносно-информативној агенцији. Овај закон је предвидео да директор агенције има могућност, када то налажу безбедносни интереси Републике Србије, да доносе решење којим одређује „мере одступања“ од начела неповредивости тајне писама. Такво решење морало је да буде засновано на претходној одлуци суда.

У својој одлуци, Уставни суд је навео да „мере одступања“ представљају неодређен појам, који је нејасан и непрецизан, будући да се не одређују које мере се могу изрећи решењем директора, као ни круг лица којима се могу изрећи. Независно од тога што Безбедносно-информативна агенција обавља важне безбедносне послове, закон мора бити такав да омогућава предвидљивост грађанима, у зависности од конкретних околности, до разумног степена.

Одредбу о могућности доношења мера одступања суд је прогласио неуставном, будући да не постоји предвидљивост законских одредаба што

[382] Овај став је заузет у случају који се односи на повреду личних података (података о здравственом стању), који су без одговарајућег правног основа прослеђени Министарству здравља од стране Комитета за здравство без пристанка лица на које се односе. *Y.Y. v. Russia*, app. no. 40378/06, Европски суд за људска права, 2016.
[383] *Rotaru v. Romania*, app no. 28341/95, Европски суд за људска права, 2000.
[384] Одлука Уставног суда ИУз-252/2002, од 27.02.2014. год.

онемогућава грађане да знају шта је правно правило у конкретном случају, што води ограничењу права на приватност и права на преписку.

Принцип пропорционалности означава да мере којим се ограничава одређено право морају бити тако предвиђене да на најмањи могући начин утичу на права грађана. Принцип пропорционалности посматра се како у односу на регулативу, тако и у односу на органе које примењују право. Тако, у случају *Peck v. the United Kingdom,*[385] Европски суд за људска права је оцењивао пропорционалност предузетих мера у односу право на приватност.

У овом случају подносилац представке снимљен је надзорним камерама како се креће градом са ножем у руци, о чему је обавештена и полиција која је реаговала у циљу заштите јавне безбедности. У жељи да укаже на ефикасност сигурносних камера, полиција је доставила снимак подносиоца представке са ножем локалним медијима. Подносилац представке је сматрао да је на овај начин повређено његово право на приватност (личне податке у облику видео записа). Европски суд је прихватио представку, изводећи закључак да су власти могле да предузму одговарајуће мере како би сакриле идентитет подносиоца представке. Због тога, суд је стао на становиште да предузете мере нису биле пропорционалне циљу које су власти желеле да остваре.

***

Поменути принципи гарантују одређену заштиту од произвољног мешања органа управе у односу на ограничење појединих права грађана. Ограничења у демократском друштву морају постојати ради заштите важних јавних интереса. Ипак, када постоји потреба за увођењем ограничења у примени права грађана, неопходно је да се поштују принципи доступности, предвидљивости и пропорционалности закона, јер се само на тај начин могу остварити принципи законитости и владавине права.

Таква је ситуација и у материји личних података, где могу настати бројне штетне последице због ускраћивања појединих права које гарантују приватност и заштиту личних података грађана. Што се тиче Србије, у пракси остаје да се види на који начин ће реаговати Уставни суд и друге институције у односу на

[385] *Peck v. the United Kingdom,* app no. 44647/98, Европски суд за људска права, 2003.

ограничења права грађана одлукама органа управе, будући да доступне праксе још нема.

Свакако, људска права не смеју остати само слово на папиру, већ се морају поштовати и примењивати у пракси. У случају када органи управе не примене основна начела и права грађана у вези са њиховим личним подацима, на сцену ступају предвиђени механизми правне заштите личних података грађана. Ови механизми представљају основну „правну муницију“ у заштити легитимних интереса грађана.

VI МЕХАНИЗМИ ПРАВНЕ ЗАШТИТЕ ЛИЧНИХ ПОДАТАКА У ЕЛЕКТРОНСКОЈ ЈАВНОЈ УПРАВИ

Механизми правне заштите личних података у електронској јавној управи представљају начине путем којих се остварује заштита личних података грађана које чувају и које обрађују органи управе. У праву Србије и праву ЕУ можемо одредити три врсте правних механизама заштите личних података. То су механизам заштите који се остварују пред независним контролним телом, механизам судске заштите и механизам овлашћеног лица за заштиту података у оквиру органа управе.

Прва две механизама превасходно су усмерена на заштиту права грађана у вези са њиховим личним подацима. У том смислу, права грађана у вези са личним подацима представљају примарни објекат њихове заштите. Трећи механизам усмерен је на правилно обављање управног рада у вези са личним подацима грађана у оквиру органа управе, па се превасходно штити законитост рада управе, а посредно и права грађана у вези са личним подацима.

Иако се поменути механизми разликују по субјекту који пружа заштиту и методологији пружања заштите, сва три механизма остварују свој пун потенцијал и допуњују један другог у узајамном деловању. Уз то, њихов основни циљ јесте да обезбеде контролу рада органа управе и санкционишу пропусте у вези са обрадом личних података грађана. Због специфичности и значаја механизама, истраживање ће обрадити сваки механизам посебно.

1. НЕЗАВИСНО КОНТРОЛНО ТЕЛО КАО МЕХАНИЗАМ ПРАВНЕ ЗАШТИТЕ ЛИЧНИХ ПОДАТАКА

1.1. Правна контрола рада органа управе

Једно од најзначајнијих питања у вези са функционисањем јавне управе јесте питања контроле над радом и актима управних органа.[386] У односу на органе управе контрола је усмерена на исправљање грешака у раду и актима. „Јавна управа се често доживљава као безлична и монолитна категорија, па се од ње и очекује униформно поступање. Она је, међутим жив организам који чини људе оптерећени бројним слабостима сопствене природе“.[387]

За постизање законитог и правилног рада неопходно је успоставити механизме контроле који су усмерени на различите аспекте рада органа управе. У пракси се зато јављају различити облици контроле рада органа управе који се у зависности од начина вршења и саставних елемената могу сврстати у правне, политичке или друштвене облике контроле управе.

У односу на предмет овог истраживања најважнија врста контроле јесте правна контрола. Правна контрола усмерена је на испитивање законитости, правилности, а понекад и целисходности рада органа управе. Овај облик контроле остварује се кроз деловање органа управе (управна контрола управе коју врше првостепени и другостепени управни органи), судских органа (судска контроле управе) и надзор који врше независна контролна тела. У оквирима правне контроле можемо направити класификацију на управну, судску и контролу управе коју врше независна контролна тела.

Прва два облика контроле (управна и судска) представљају опште начине контроле рада органа управе који се одвијају у свим областима управног деловања. Са друге стране, контрола коју врше независна контрола тела одвија се само у појединим областима друштвеног живота и управног деловања, за које су

[386] Као што се наводи „свака власт настоји да сакрије од очију јавности неправилан и незаконит рад носилаца јавних функција („свака власт је као печурка најбоље се осећа и успева у мраку“)“. Славиша Орловић, „Независна тела- четврта грана власти или контролор власти“, у *Савремена држава: структура и социјалне функције* (ур. Чедомир Чупић), Konrad Adenauer Stiftung, Факултет Политичких наука и Центар за демократију, Београд 2010, 232.
[387] М. Давинић (2013), 94.

ова тела основана. Такав је случај и са правом на заштиту личних података, за које се обично установљава независно надзорно тело.

1.2. Контрола рада органа управе коју врше независна надзорна тела

Независна контролна тела понекад се сврставају у тзв. „четврту грану власти“.[388] Четврта грана власти се користи као теоријска конструкција који тежи да обухвати оне државне органе и тела који обављају специфичне задатке, обично регулаторне и контролне, али који се због специфичног правног статуса и посебних овлашћења не могу сврстати у традиционалне гране власти (законодавну, извршну или судску грану власти). Зато се независна контролна тела могу одредити као „четврта грана власти“, будући да је њихова делатност обично усмерена ка остваривању људских права у појединим областима друштвеног живота, контроли органа јавне власти, старању о правилној примени прописа у појединим областима, итд. Ипак, у Србији четврта грана власти нема утемељења у прописима, али поменути органи ипак поседују независну и посебну правну природу.

Под независним контролним телима подразумевају се заштитници грађана (омбудсман), повереници (повереник за информације од јавног значаја и заштиту података о личности, повереник за равноправност), агенције (агенција за борбу против корупције, агенција за заштиту јавних набавки, итд) и други. Основна одлика ових тела јесте независност у обављању послова из своје надлежности, што је у пракси упитно због начина избора и државног карактера ових институција. Независност се огледа у односу на органе јавне власти и у односу на лица приватног права. Такође, финансијска независност и начин избора запослених представљају елементе који гарантују независност ових тела. Снагом свог ауторитета и специјалним овлашћењима независна тела надзиру одређену област управног деловања и друштвеног живота и помажу у остваривању људских права.[389]

[388] С. Орловић (2010), 232.
[389] Упор. Georges Dupuis, Marie-Jose Guedon, *Institutions administratives – Droit administratif*, Armand Colin, Paris 1988, 59.

Независност не значи да рад ових тела не подлеже правној контроли. У пракси су установљени механизми контроле рада ових тела у облику судске контроле, као и представљања извештаја пред органом који је основао тело (обично Народна скупштина).

Надлежност и оснивање ових тела обично се установљава уставом и законима. У највећем броју случајева бира их народна скупштина, као представничко тело које изражава вољу грађана и тиме им омогућава независност у односу на судску и извршну власти. Области деловања независних тела разликују се од државе до државе. Ова тела се могу основати ради заштите појединог права или поједине области друштвеног живота у којој се јавља потреба за већом стручношћу, посебним знањима или независним контролним овлашћењима у односу на органе управе.

Такав је случај са равноправношћу полова, конкуренцијом, јавним набавкама, борбом против корупције, итд. Једна од уобичајених области у упоредно правном законодавству у којој се установљава независно заштитно тело, јесте област заштите личних података.

1.3. Контрола органа управе коју врше независна контролна тела у области заштите личних података

Како би се приватност грађана у потпуности заштитила у односу на органе јавне власти неопходно је установити посебне „спољне“ видове контроле обраде података. То је неопходно због структуре и правне природе органа управе. Електронска јавна управа као затворени организам тешко може „сама себе“ да контролише, посебно што се контрола тиче личних података чија је безбедност у електронском окружењу константно угрожена.

Због тога, државе успостављају посебне облике контроле управе у вези са личним подацима, које се не могу сврстати ни у управну ни у судску врсту контроле. Овај посебан облик контроле обично се остварује путем независног надзорног (контролног) тела чија је надлежност усмерена на заштиту личних података грађана, њихових права у вези са личним подацима (и информацијама од јавног значаја) и надзор над питањима од значаја за целокупан систем заштите личних података у једној држави. „Код овог модела установљени су посебни, независни и самостални, инокосни или колегијални државни органи, којима је

поверено вршење управно-правне контроле, а чије коначне одлуке (најчешће решења) могу бити подвргнуте преиспитивању од стране суда, покретањем поступка управно-судске заштите)“.[390]

Независна тела носе опште карактеристике других независних институција. Самостална су у обављању послова из својих надлежности, па за предузимање њихових аката и овлашћења није неопходно никакво претходно или накнадно одобрење или овлашћење. У зависности од облика у коме обављају своју делатност, постоје независни контролни органи у инокосном облику, као што је случај са повереником за информације од јавног значаја и заштиту података о личности или у облику зборног (колективног) органа, какав је случај са агенцијама (примера ради, у Хрватској постоји Агенција за заштиту особних података).

Ради несметаног обављања своје делатности, државе им поверавају јавна овлашћења. У односу на њихове акте и радње предвиђена је могућност контроле, коју обично врше судски органи (у односу на правне акте) и парламент (у односу на сврсисходност и успешност рада).

2. НЕЗАВИСНО КОНТРОЛНО ТЕЛО У ОБЛАСТИ ЗАШТИТЕ ПОДАТАКА У ПРАВНОМ СИСТЕМУ СРБИЈЕ

2.1. Историјска перспектива независног контролног тела у правном систему Србије

У правном систему Србије постоји инокосно независно тело које контролише стање и штити права грађана у области личних података. Ову улогу обавља Повереник за информације од јавног значаја и заштиту података о личности (у даљем тексту: Повереник). Институција Повереника не представља уставну категорију, већ он установљен посебним законом.

Историјски посматрано, институција независног контролног тела у области информација од јавног значаја, први пут је у Србији уведена Законом о слободном приступу информацијама од јавног значаја.[391] Овим законом уређена су питања од

[390] D. Milenković, „Upravno-procesni i drugi slični oblici zaštite prava na pristup informacijama u komparativnom pravu“, *Strani pravni život*, 3/2015, Beograd 2015, 121.
[391] Закон о слободном приступу информацијама од јавног значаја је усвојен 2004. године.

значаја за приступ информацијама од јавног значаја којима располажу органи јавне власти. Ради остваривања права грађана на приступ информацијама и интереса јавности да буде упозната са важним чињеницама од јавног значаја, установљена је институција Повереника за информације од јавног значаја, као самосталног државног органа који је независан у вршењу послова из своје надлежности.[392]

Ипак, основне надлежности Повереника биле су усмерене искључиво на остваривање приступа подацима који се налазе у поседу органа јавне управе, не и на заштиту личних података. Заштиту личним подацима, и то на посредан начин, контролисањем аката и радњи органа управе и заштитом људских права и слобода пружао је Заштитник грађана (Омбудсман), као још један облик независног контролног тела. Можемо закључити да у овом периоду у Србији није било независног контролног механизма заштите личних података у поседу органа управе.

Четири године након доношења Закона о слободном приступу информацијама од јавног значаја, Народна скупштина Србије усвојила је Закон о заштити података о личности (2008), којим је уредила област заштите личних података. Тај закон је предвиђао да послове заштите личних података грађана обавља Повереник за информације од јавног значаја и заштиту података о личности, као самостални државни орган, независан у вршењу своје надлежности.[393]

Од тренутка ступања тог закона на снагу, Повереник за информације од јавног значаја мења своју правну природу и наставља са радом под измењеним називом - Повереник за информације од јавног значаја и заштиту података о личности. Осим назива, институција Повереника добија и нову правну природу са измењеним дужностима и овлашћењима.[394] Институција Повереника наставила је свој континуитет, са додатно измењеним овлашћењима, ступањем на снагу Закона о заштити података о личности (2018).

[392] Чл. 1, Закона о слободном приступу информацијама од јавног значаја.
[393] Чл. 1, ст. 3, Закона о заштити података о личности (2008).
[394] С. Лилић (2013), 243.

2.2. Правна природа Повереника за информације од јавног значаја и заштиту података о личности

Основна надлежност Повереника за информације од јавног значаја и заштиту података о личности у српском праву је двојака, што утиче и на правну природу овог тела. Његове надлежности усмерене су на заштиту права приватности и личних података грађана и остваривању потреба јавности да буде обавештена о важним чињеницама за друштво, у области информација од јавног значаја.[395]

Повереник се не може сврстати ни у једну од традиционалних „грана власти“ које су предвиђене Уставом Србије, будући да његова овлашћења, као ни однос према осталима гранама власти не омогућава сврставање у познате гране власти. Иако Повереника бира Народна скупштина, као орган законодавне власти, не можемо рећи да он представља тело Народне скупштине, односно да припада законодавној власти. Јасно је да ово тело не припада ни судској грани власти. На основу надлежности и поверених овлашћења можемо рећи да је институција Повереника најближа извршној (управној) грани власти, на коју је његов рад суштински и усмерен.[396]

2.2.1. Независан статус Повереника

Повереник ужива независан статус у правном систему Србије. Независност се гарантује у односу на друге гране власти, али и у односу на сва лица приватног права. Наравно, Повереник није потпуно изолован од спољних утицаја. Њега бира Народна скупштина, а уз то, није потпуно независтан ни од судске гране власти, будући да су његове одлуке подложне судској контроли, као контроли у којој се штити законитост. Независност се остварује и кроз посебне услове које мора да испуњава лице које се бира на ту функцију. Због тога, могло би се рећи да се независност Повереника највише огледа у његовом односу према органима

[395] У стручној литератури се наводи да оваква позиција чини Повереника „јединственом институцијом у правном систему Републике Србије“. М. Давинић (2018), 23.

[396] Против одлука Повереника могуће је покренути управни спор пред Управним судом, који је законски „резервисан“ за акте и радње органа управе. Такође, ово тело представља другостепени орган у вези са остваривањем права на приступ информацијама од јавног значаја и другим правима у вези са личним подацима.

извршне гране власти, грађанима и привредним субјектима који морају да се уздрже од било каквог утицаја на рад ове институције.

Независност Повереника значи да ова институција треба да остане слободна од било каквог спољног директног и индиректног утицаја јавности или појединаца. То значи да Повереник нема „непосредно надређеног“ од кога прима директиве и налоге за вршење својих овлашћења. Такође, финансијски моменат је од значаја за независно функционисања канцеларије Повереника. Повереник има право на државна новчана средства која су му неопходна за рад и вршење његових овлашћења, а она се остварују из посебних државних фондова. Финансијска независност се остварује и кроз финансијска примања лица које се бира за Повереника, чија плата је у рангу са платом судија Врховног суда, што говори о значају улоге коју он има у друштву Уз то, Повереник може да запошљавања лица која гарантују квалитетно и непристрасно остваривање послова из његове надлежности.[397]

Одредбе о инкомпатибилности (неспојивости) било које друге делатности са делатношћу коју Повереник обавља представљају још један израз независности ове институције. Лице које је изабрано за Повереника, како би одржало свој независтан статус, нема право да врши било коју другу функцију у приватној или јавној сфери. Такође, то лице нема право да буде члан политичке партије или удружења. На овај начин стриктно је одређен круг послова који може обављати лице изабрано за Повереника. Ипак, може се поставити питање оправданости забране чланства у удружењима, јер она не морају бити „политички обојена“, већ могу представљати удружења у областима које могу допринети развоју друштва у области личних података или то могу бити међународна удружења Повереника, односно независних тела, када треба омогућити изузетак од забране чланства.

Занимљиво је напоменути да Закон о слободном приступу информацијама од јавног значаја одређује Повереника за информације од јавног значаја, као независан и самосталан државни орган.[398] Са друге стране, Закон о заштити података о личности (2018) предвиђа да је Повереник за информације од јавног

[397] Надзор над финансијским стањем и коришћењем финансијских средстава Повереника обавља Државна ревизорска институција, што не би требало да утиче на обележје независности Повереника. Вид. чл. 74, ст. 5, Закона о заштити података о личности (2018).
[398] Чл. 32, Закона о слободном приступу информацијама од јавног значаја.

значаја и заштиту података о личности независан државни орган, али не и самосталан. Иако се теоријски може правити разлика између независности и самосталности у односу на начин обављања функције, можемо рећи да практично појам независности у деловању обухвата и појам самосталности.

Ипак, остаје питање терминолошке непрецизности и недоследности два закона која одређују правну природу Повереника. То отвара и питање оправданости постојања једног повереника за две различите области друштвеног живота, и поред значајних веза између информација од јавног значаја и личних података.

2.2.2. Услови за избор Повереника

Један од битних услова за независан рад ове институције јесте начин избора и услови који се постављају да би једно лице могло да буде бирано за Повереника. Закон о заштити података о личности не садржи одредбе у вези са условима за избор Повереника, већ упућује на Закон о информација од јавног значаја, што је још један од разлога због које би требало раздвојити институцију која се баве информацијама од јавног значаја и институцију која се бави заштитом података. Закон о информацијама од јавног значаја наводи да се за Повереника бира лице са признатим угледом и стручношћу у области заштите и унапређења људских права, које испуњава услове за рад у државним органима, које је завршило правни факултет и које има најмање 10 година радног искуства.[399]

2.2.3. Да ли би требало поставити конкретније услове за избор Повереника?

Чини се да су изложени правни стандарди сувише апстрактно постављени. Наиме, "признати углед" и „стручност у области заштите унапређења људских права" не представља конкретан услов који би обезбеђивао да је кандидат обављао послове у области заштите података или информација од јавног значаја. Јавља се и питање компетентности народних посланика у процени нечијег угледа да обавља функцију заштитника података и информација једног друштва, будући да нема конкретније постављених услова за његов избор. Уз то, услов који се

[399] Чл. 30, Закона о слободном приступу информацијама од јавног значаја.

односи на године радног искуства није у вези са надлежностима за које се бира Повереник, већ је довољно 10 година радног искуства у било којој области.

Сматрамо да су поменуте одредбе неодређене и да би их требало заменити конкретнијим, које ће омогућити лакшу процену квалитет одређеног лица да обавља функцију Повереника. У тренутном стању ствари, на основу воље скупштинске (политичке) већине, на место Повереника може бити изабрано лице које нема превише искуства у вези са надлежностима ове институције. На тај начин „политизује“ се институција Повереника и доводи у питање његова независност, будући да је могућ избор лица које не поседује неопходна стручна знања, али има подршку владајуће већине у скупштини.

Избором стручног лица које има искуства у вези са пословима заштите личних података, информацијама од јавног значаја и људским правима, спречава се незаконитост, неправилност и спорост рада Повереника. Такође, сматрамо да би било адекватно поставити услов од 10 година рада у струци, односно у пословима који се односе директно на информације од јавног значаја и заштиту личних података.

Због тога, неопходно је установити прецизне и конкретне услове који ће обезбедити да независно и стручно лице буде изабрано на позицију Повереника. Такође, треба радити на повећању транспарентности приликом пријављивања лица за ову функцију и приликом процеса селекције кандидата. На тај начин, грађани би имали увид у то које се лице бира на важно и одговорно место Повереника, чиме би се повећало поверење грађана у ову институцију, али и у државу.

Требало би размислити и о формирању два различита тела, од којих ће се једно бавити информацијама од јавног значаја, а друго заштитом личних података, будући да се ради о материјално другачијим областима, које су само донекле повезане. И област заштите података и област информација од јавног значаја имају истог имениоца у подацима који су од значаја за грађане. Међутим, ове две области су квалитативно другачије по питању права грађана у овим областима (подаци о личности се штите, а информације од јавног значаја се остварују) и начину остваривања тих права. Такође, правна регулатива је другачија по питању ових института, па тренутно стање ствари осликава

нормативну недоследност и раздвојеност услова и надлежности Повереника у два закона.

2.3. Послови Повереника у вези са подацима о личности

Послови Повереника у делу који се односи на заштиту личних података, бројни су и усмерени ка заштити приватних и јавних интереса. Надлежности и овлашћења ограничена су на територију Србије и то у односу на личне податке који обрађују органи јавне власти и грађани. Из надлежности Повереника изузете су обраде личних података коју врше судови у вршењу њихове надлежности.

Најважнија дужност Повереника тиче се праћења примене Закона о заштити података о личности. То значи да је служба Повереника дужна да прати стање у области безбедности личних података и да усмерава примену законских норми ка правилној примени. Из ове дужности, произлази овлашћење Повереника да пружа стручна мишљења у вези са заштитом личних података предлагачима правних прописа (Народна скупштина, Влада) и онима који примењују прописе у области личних података (сви органи управе). Под праћењем стања подразумева се праћење начина примене правних норми, али и примене техничких и организационих елемената заштите података. Технички елементи заштите односе се на стање информационо-комуникационих технологија и њихову употребу у јавној управи. То значи да служба Повереника мора вршити правну и техничку анализу постојећег стања ствари, како би државни систем заштите података адекватно функционисао.

Правна природа Повереника омогућава му да се у вршењу послова из своје надлежности „приближи грађанима“. У том смислу Повереник има специфичну улогу која се састоји у развијању свести грађанима о ризицима, правилима, мерама заштите и правима у вези са обрадама личних података. На овај начин Повереник утиче на стање правне културе у области заштите података, врши утицај на јавно мњење и развија, својим ауторитетом, свест грађана о важности заштите личних података. То значи да Повереник упознаје грађане са правним механизмима заштите. Поменута овлашћења иду за тим да спрече евентуалне штетне последице у вези са обрадом личних података, како по грађане, тако и по запослене у органима управе.

Чисто правни послови Повереника односе се на решавање о притужбама грађана на рад и акте органа управе у вези са прикупљањем и обрадом личних података. Захваљујући инспекцијским овлашћењима, Повереник надзире и контролише поступање органа управе у вези са личним подацима.

У послове Повереника спада и израда стандардних уговорних клаузула, подстицање израде кодекса поступања, подстицање успостављања поступака сертификације заштите личних података и одговарајућих жигова, периодично преиспитивање сертификата, објављивање критеријума за акредитацију лица за надзор обраде личних података, одобравање одговарајућих одредаба уговора, обавезујућих пословних правила, итд.[400]

У односу на захтеве грађана, Повереник обавља своје послове без накнаде, што је још један израз независности ове институције, будући да не зависи од новчаних средстава грађана. Међутим, у одређеним ситуацијама, Повереник може да захтева накнаду нужних трошкова, уколико то оправдавају околности конкретног случаја. Тако, уколико је неки захтев очигледно неоснован или се понавља Повереник може да одбије поступање по таквом захтеву, уз тражење накнаде нужних трошкова које је имао за поступање по њима. На овај начин спречава се злоупотреба институције Повереника, односно подношење неистинитих и малициозних захтева који отежавају рад ове институције. Због тога, установљена је накнада нужних трошкова, као адекватно средство борбе против малициозних правних захтева.

2.4. Инспекцијска овлашћења Повереника

Појам инспекције обично се односи на вршење контроле рада неког лица или организације са циљем да се отклоне пропусти и исправе неправилности у њиховом раду. Према томе, основни циљ инспекцијског надзора је „да се превентивним деловањем или налагањем мера обезбеди законитост и безбедност пословања и поступања надзираних субјеката и спрече или отклоне штетне последице по законом и другим прописом заштићена добра, права и интересе“.[401] Начин на који се врши инспекцијски надзор разликује се у зависности од

[400] Вид. чл. 78, Закона о заштити података о личности (2018).
[401] Закон о инспекцијском надзору, *Службени гласник* РС, бр. 36/2015.

предмета контроле, па се контрола може вршити прегледом докумената, просторија, непосредним опажањем предмета, испитивањем лица, и на друге адекватне начине. „Та овлашћења се своде на могућност ауторитативног иступања ради несметаног вршења инспекцијског надзора, а служе и отклањању незаконитости или, ако је могуће, само репресивно деловање, да се незаконито понашање санкционише“.[402]

Претходни Закон о заштити података о личности (2008) није експлицитно предвиђао инспекцијска овлашћења Повереника. Тај закон садржао је одредбу по којој надзор над применом норми закона врши Повереник преко овлашћених лица. Међутим, закон није конкретизовао о каквој се врсти надзора ради. У оквиру надзорних овлашћења Повереник је могао, и то искључиво на основу налаза овлашћених лица (инспектора), да нареди одређеном субјекту да отклони учињене недостатке, да престане са обрадом личних података или да обрише личне податке грађана у његовом поседу.

Законом о заштити података о личности (2018) Поверенику су омогућена широка инспекцијска овлашћења која му помажу у контроли законитости и правилности у области заштите података. У вршењу инспекцијских овлашћења, Повереник може предузети различите врсте мера. Тако, он може предузети мере које му омогућавају боље разумевање чињеничног стања и тиме ефикаснију контролу. У том смислу, Повереник може наложити органима управе да му доставе све информације које су неопходне за контролу. Он може захтевати и добити приступ свим просторијама, средствима и опреми која је од непосредног утицаја на обраду и чување личних података. Како би могао успешно да обавља своја инспекцијска овлашћења, инспектор може предузети и неку од корективних мера. На основу корективних мера, он може:

1. да упозори надлежно лице у органу јавне власти да се одређеним радњама обраде могу повредити одредбе прописа у области личних података,
2. да изрекне опомену надлежном лицу у органу када својим поступцима у вези са обрадом повређују одредбе прописа,

[402] Д. Милков, „Инспекцијски надзор и заштита животне средине“, *Зборник радова Правног факултета у Новом Саду*, 4/2015, Нови Сад 2015, 1443.

3. да наложи поступајућем органу да поступи по захтеву лица на која се подаци односе у вези са остваривањем његових права,
4. да наложи поступајућем органу да усклади обраде података о личности са одредбама одговарајућих прописа,
5. да наложи надлежном органу да обавести лице на које се подаци односе о повреди безбедности његових података,
6. да наложи исправљање, односно брисање података или ограничење обраде,
7. да изрекне новчану казну на основу прекршајног налога, уз или уместо других мера прописаних законом,
8. да обустави пренос података о личности примаоцу у другој држави или међународној организацији.[403]

Корективна овлашћења Повереника су разноврсна и разликују се по степену принуде и начину спровођења.

Према степену принуде у инспекцијским овлашћењима, можемо направити разлику између превентивних мера, које обично иду за тим да упозоре и скрену пажњу надзираном субјекту на евентуалне пропусте и могуће последице и накнадне мере (санкције), које се изричу након већ настале повреде, обично уз коришћење ауторитативних метода ради исправљања насталих грешака и неправилности.

У односу на начин спровођења инспекцијских овлашћења, надзор Повереника можемо разврстати у редован и ванредан. Редовни надзор представља ону врсту надзора која се обавља по предвиђеном плану контроле. Са друге стране, ванредни надзор је последица потребе за предузимањем хитних мера, па се не спроводи по унапред предвиђеним елементима у смислу датума, обима и начина, већ у складу са потребама конкретног случаја. Инспекцијски надзор може бити покренут по службеној дужности или по захтеву странке.[404]

Важно је поменути да против одлука Повереника донетим у вршењу инспекцијског надзора, физичка и правна лица, као и органи управе могу покренути судске механизме заштитите. Судска заштита се остварује у управном

[403] Чл. 79, ст. 2, Закона о заштити података о личности (2018).
[404] За више о инспекцијском надзору и инспекцијском надзору у Републици Србији, вид. М. Влатковић, З. Јовановић (2016), 113-182.

спору пред Управним судом и не представља сметњу за покретање других поступака (управних и судских) у вези са личним подацима. Ово је занимљиво решење будући да ће се у случају исказаног незадовољства органа управе одлуком Повереника водити управни спор између два државна органа. Сматрам да је ово решење адекватно, јер се у поступку пред Повереником орган управе појављује као један од учесника, поред подносиоца притужбе. Дакле, није у питању класичан хијерархијски однос као када другостепени орган одлучује по жалби у управном поступку. Позиција органа управе у том поступку, слична је позицији туженог органа у управном спору. Поменута законска решења су значајна јер судска контрола омогућава контролу рада друге независне институције.

Широка инспекцијска овлашћења свакако доприносе остваривању друштвене улоге Повереника. Надзор над правилношћу обраде и усклађеност поступања органа управе у односу на прописе који регулишу заштиту личних података, од кључног су значаја за правилан рад целокупне јавне управе и поштовања личности грађана. Повереник, захваљујући независности и одговарајућим овлашћењима, подстиче остваривање начела законитости и предвидљивости у функционисању органа управе.

2.5. Пракса Повереника у области заштите података о личности у праву Србије

Будући да је примена Закона о заштити података о личности (2018) тек у почетним фазама развоја, пракса Повереника по овом закону још није формирана. Међутим, пракса Повереника у области заштите података о личности установљена је на основу претходног Закона о заштити података о личности (2008). Највећи број доступних случајева односи се на поступање лица приватног права у односу на личне податке грађана. Пракса која се односи на поступање органа управе у вези са личним подацима грађана мало је оскуднија, али ипак постоји. Ради свеобухватности истраживања и разумевања посебне улоге и специфичности аката које доноси Повереник, аутор је обрадио и значајније случајеве који се тичу лица приватног права, али који су од утицаја на чување и обраду података грађана у поседу органа управе.

У вршењу послова из своје надлежности Повереник се у највећем броју случајева користио мишљењима. Мишљења представљају посебне акте Повереника, којима он указује на пропусте органа у вези са чувањем и обрадом личних података. Ови акти не представљају управне акте, али имају обавезујући карактер, будући да пропуштање поступања по мишљењима може бити санкционисано. Такође, Повереник се користио и другим актима као што су решења и упозорења.[405]

2.5.1. Мишљења Повереника

Мишљење Повереника у вези са узрастом малолетног лица и способношћу давања сагласности за обраду података о личности

Малолетна лица у правном систему Србије уживају посебну заштиту. То се односи и на област заштите личних података. Једно од важнијих мишљења Повереника односило се на питање старосне доби лица које може дати пристанак на обраду својих података о личности. У тадашњем праву Србије, Законом о заштити података о личности (2008), није била предвиђена прецизна старосна граница у вези са могућношћу малолетних лица да дају сагласност на обраду њихових личних података. Према одредбама Закона о заштити података о личности (2008), сагласност за обраду личних података малолетника могли су да дају родитељ или малолетно лице о чијим подацима је реч, али искључиво у ситуацијама предвиђеним (посебним) законом.

Потпуна способност да се одлучује о обради личних података, према домаћем праву стицала се са 18. година живота. Ипак, други законски прописи предвиђали су (неки од њих су идаље на снази) различите старосне границе за вршење правних радњи и послова малолетника. На пример, лице које је навршило 14. година може предузимати оне правне послове којима стиче искључиво права, којима не стиче ни права ни обавезе и правне послове мањег значаја.[406] Лице са 15 година живота стиче радну способност и могућност да располаже својом

[405] Обрађена пракса Повереника може се односити и на питања која су уређена новим Законом о заштити података о личности (2018), која међутим нису била обухваћена претходним законом из ове области. Свакако, и такве одлуке су од значаја, будући да су имале утицаја на формирање регулативе и нових законских решења у овој области.
[406] Чл. 64, Породичног закона, *Службени гласник* РС, бр. 18/2005, 72/2011.

зарадом.[407] Такође са 15 година живота може се дати пристанак на учествовање у истраживању у јавном здрављу, под условом да то не производи директну корист и да не носи ризик по дете. Исти број година живота омогућава детету да самостално изврши увид у своју медицинску документацију.[408]

У вези са старосном границом за пристанак на обраду података Повереник је изнео следећи став: „Хипотетички, малолетно лице са навршених 14 година, па чак и са не навршених 14 година, може да дâ свој пристанак на обраду података, као што су електронска или кућна адреса, уколико би ти подаци били неопходни за предузимање правних радњи које ова лица по (посебном) закону могу да предузимају. Притом, могућност давања сагласности не односи се на све податке о личности, већ само на оне податке који се неопходни за предузимање одређене правне радње за коју је лице пословно способно, односно оне радње за коју је законом прописано да је може предузети лице одређене старосне границе“.[409]

Из овог мишљења Повереника можемо извести неколико закључака. Прво, Закон о заштити података о личности (2008) не представља једини релевантан пропис у вези са годинама малолетника које су неопходне за давање сагласности на обраду личних података, већ се морају узети у обзир и други релевантни прописи. Примера ради, када се обрађују подаци деце морају се узети у обзир и прописи који уређују породичну, грађанску и радно-правну материју. Друго, сврха обраде је од великог значаја за решавање спорних питања у вези са самом обрадом личних података малолетника. У односу на конкретан случај, Повереник је извео закључак да је неопходно утврдити конкретну сврху обраде, као претходно питање, а тек након тога консултовати релевантне прописе и утврдити која је старосна граница применљива за пристанак у конкретном случају, односно да ли постоји законито поступање.

У новом Закону о заштити података о личности (2018) проблем је решен прописивањем прецизне старосне границе за обраду личних података. Дете које је навршило 15 година живота може самостално дати пристанак за обраду својих

[407] Чл. 24, Закона о раду, *Службени гласник* РС, бр. 24/2005, 113/2017.
[408] Чл. 24-25, Закона о пацијентима, *Службени гласник* РС, бр. 45/2013.
[409] Вид. Мишљење Повереника бр. 011-00-00607/2013-05, од 16.10.2013. год., 2.

података у коришћењу услуга информационог друштва.[410] Уколико дете није навршило 15 година, пристанак могу дати законски заступници детета. Такође, уколико се случај не односи на услуге информационог друштва, неопходно је утврдити сврху обраде и консултовати релевантне посебне прописе (Породични закон, Закон о облигационим односима, Закон о раду, итд.).

Ово решење је у складу са европским стандардима и говори о важности праксе Повереника која може да утиче на измену непрецизних прописа у области заштите личних података, али и да усмери руковаоце података да се норме у вези са личним подацима налазе у различитим прописима, које је неопходно системски тумачити.

Мишљење Повереника у вези са обрадом података од стране Регистра националног интернет домена Србије

Регистар националних интернет домена Србије је стручна, невладина, и непрофитна фондација која управља домаћим интернет доменима. Она је основана 2006. године.[411] У управљању и додељивању интернет домена организација заступа општи интерес грађана, а своје послове обавља у складу са принципима квалитета, ефикасности, независности и транспарентности. Делатност управљања интернет доменима у Србији заснива се на овлашћењу Интернет корпорације за додељивање назива и бројева (*Internet Corporation for Assigned Names and Numbers, скраћено- ICANN*) које врши активности управљања глобалним системом интернет адреса и бројева.[412]

И поред несумњиво важне улоге које Национални регистар интернет домена има у Србији, његове надлежности и организација нису уређене посебним законом. То значи да Национални регистар може обрађивати само оне личне податке за које постоји сагласност, док би обрада личних података грађана без

[410] Чл. 16, Закона о заштити података о личности (2018).
[411] Неки од оснивача Регистра националних интернет домена Србије су: Електротехнички факултет Универзитета у Београду, Универзитетска библиотека „Светозар Марковић“, Привредна комора Србије, Телеком Србија и други.
[412] За више о Регистру националних интернет домена Србије, *https://www.rnids.rs/%D0%BE-%D0%BD%D0%B0%D0%BC%D0%B0/%D0%BF%D1%80%D0%B8%D0%BD%D1%86%D0%B8%D0%BF%D0%B8,* 10. јул 2018.

пристанка, без обзира на важне активности Националног регистра, била незаконита.

На неадекватност постојеће законске праксе указао је Повереник и изразио потребу да активности Регистра треба да представљају предмет посебне законске регулативе, имајући у виду улогу интернета у савременом друштву. Такође, Повереник је дао своје мишљење у вези са могућношћу обраде јединственог матичног броја грађана приликом регистрације физичког лица за добијање интернет домена. За такву обраду неопходан је адекватан образац за давање сагласности лица за обраду који је изричито прописан у Општим условима пословања. Уједно, Повереник је препоручио Регистру измену тадашњих услова пословања како би се заштитили лични подаци грађана.[413]

Захтев за издавање мишљења од Повереника, које је у конкретном случају поставио Регистар, представља пример добре праксе усмеравања руковаоца и обрађивача личних података. Такву праксу требало би да следе органи управе и друга лица која обављају делатности у вези са обрадом личних података, а имају одређене недоумице у примени прописа из поменуте области.

Скрећемо пажњу на то да органи имају могућност да се обрате Поверенику у случају недоумица или тешкоћа у примени регулативе о заштити личних података, посебно када се ради о нерегулисаним областима друштвеног живота, попут интернета и нових информационо-комуникационих технологија. На тај начин ствара се квалитетна управна пракса коју могу следити сви органи управе.

Мишљење Повереника о законитости преноса података Националној корпорацији за осигурање депозита

Једно од питања са којим се Повереник сусрео у свом раду односило се на могућност преноса личних података са једног руковаоца на другог. Наиме, Поверенику се обратила банка са питањем законитости обраде података о личности клијената са којима друге банке закључују стамбене кредите. Такође, банка је поставила и питање могућности преноса тих података Националној корпорацији за осигурање стамбених кредита, ради осигурања наплате

[413] Вид, Мишљење Повереника бр. 011-00-00548/2010-05, од 01.09.2010. године.

потраживања по основу стамбених кредита.[414] Национална корпорација осигурава кредите које банке одобре физичким лицима за куповину, адаптацију и изградњу некретнина, а који су обезбеђени хипотеком. Национална корпорација је основана Законом о Националној корпорацији за осигурање стамбених кредита.[415]

Ради закључења уговора о осигурању, Националној корпорацији потребни су детаљи уговора о стамбеним кредитима које су банке закључиле, а који неминовно садрже и личне податке грађана. Ипак, Национална корпорација је у том правном односу треће лице, па се поставило питање законитости обраде личних података грађана који су добили кредит од домаћих банака коју корпорација врши.

Како не би дошло до повреде приватности и личних података Повереник је изнео мишљење да би банке податке о личности клијената са којим закључе уговор о стамбеном кредиту, могле да прикупљају једино на основу писане сагласности која мора да буде саставни део уговора. Овај образац сагласности може да буде део општих услова пословања банке, али би морао да буде и саставни део уговора о кредиту. Такође, образац би морао да садржи и обавештење упућено лицу са којим банка закључује уговор да ће његови подаци бити прослеђени на коришћење Националној корпорацији за осигурање стамбених кредита.[416]

На тај начин, одговорност за заштиту података пренела би се на банку, која мора да спроведе све неопходне мере да би се лични подаци грађана заштитили. Ово питање Повереник је искористио да скрене пажњу банкама да сачине евиденцију о обради података о личности за све збирке личних података које оне воде, како би се базе уписале у Централни регистар збирки које води Повереник.

[414] Мишљење Повереника бр. 011-00-00223/2011-05, од 30.05.2011. год.
[415] Закон о Националној корпорацији за осигурање стамбених кредита, *Службени гласник* РС, бр. 55/2004.
[416] Мишљење Повереника бр. 011-00-00223/2011-05, од 30.05.2011. год., 2.

Мишљење Повереника у вези са обрадом података Агенције за приватизацију

У једном од случајева, Повереник је издао мишљење Агенцији за приватизацију,[417] као органу управе, у циљу отклањања специфичних ризика у вези са обрадом личних података, у циљу спречавања повреде права и слобода грађана.

Чињенично стање се заснивало на томе да Агенција за приватизацију прикупљала и обрађивала личне податке грађана у циљу провере испуњености услова за стицање статуса носиоца права на бесплатне акције, према Закону о праву на бесплатне акције и новчану накнаду коју грађани остварују у поступку приватизације. Уз то, Агенција је имала обавезу да доставља личне податке у вези са правом на остваривање бесплатних акција Централном регистру, депоу и клирингу хартија од вредности, као и Нафтној индустрији Србије (НИС-у), јавном предузећу чије су акције.

У свом мишљењу Повереник је истакао да је Агенција дужна да поштује све обавезе у вези са обрадом личних података, што значи предузимање мера заштите личних података до којих је дошла у поступцима приватизације. То даље значи да је Агенција дужна да упозна сва заинтересована лица са мерама за заштиту тајности података. Уз то, Агенција је била дужна да престане са чувањем свих података који нису потребни у циљу провере захтева појединаца, те се створила потреба да се такви подаци уклоне из евиденција (то се односило на податке о држављанству, бирачком праву, податке из Фонда пензионог и инвалидског осигурања, итд.).[418]

На овај начин Повереник је извршио утицај на орган управе у циљу подизања свести о улози руковаоца и обрађивача података, која се намеће приликом управљања посебним управним поступцима. Због тога, констатујемо да мишљење Повереника треба да утиче не само на конкретан случај, већ и на све друге који се налазе у позицији руковаоца и обрађивача података. Један од циљева мишљења јесте да се развије свест руковаоца и обрађивача и да спречи могуће повреде људских права, посебно пред органима управе.

[417] Мишљење Повереника бр. 011-00-00292/2010-05, од 22.07.2010. год.
[418] Вид. Мишљење Повереника бр. 011-00-00292/2010-05, од 22.07.2010. год., 2-3.

Мишљење Повереника о овлашћењима Министарства унутрашњих послова и тражењу података о националној припадности од руковаоца

Специфична улога и природа Повереника захтева од њега да у одређеним ситуацијама узме у обзир различите интересе конкретног случаја и да на основу сопствене процене интереса донесе одлуку да ли су одређени акти и радње руковаоца законити. То се посебно односи на овлашћења органа у области унутрашњих послова и одбране земље, где може доћи до укрштања и сукобљавања различитих интереса, јавних и приватних.

Припадници Министарства унутрашњих послова (у даљем тексту МУП-а) у вршењу својих овлашћења приступају са позиције јавног интереса, али тај јавни интерес не сме да угрози права и слободе појединаца, када за то не постоји конкретан разлог. Тако, у сфери личних података који се налазе у поседу органа јавног реда, може доћи до преклапања интереса, када са једне стране постоји потреба за вођењем управног поступка у вези са питањима безбедности, а са друге се налази приватни интерес за заштитом личних података.

У једном случају Повереник је закључио да „Министарство унутрашњих послова нема изричиту законску дозволу да у конкретној ситуацији тражи податке о националне припадности одређеног лица код Педагошке академије, као руковаоца подацима о личности полазника. Због тога би Педагошка академија, са становишта Закона о заштити података о личности, била дужна да одбије такав захтев МУП-а као неоснован“.[419] Наиме, Повереник је закључио да би у конкретном случају дошло до повреде приватног интереса, односно права на приватност и заштиту личних података лица. Повереник је МУП-у предложио да би најбоље било да се подаци добију непосредно од лица чији су, како би се избегло кршење основних права и слобода, а уједно би се остварио јавни интерес, односно несметано би се наставио поступак пред МУП-ом.

Оваквим мишљењем Повереник је на саветодаван начин утицао на помирење приватног и јавног интереса који у одређеним ситуацијама могу да буду у колизији. Такво поступање представља још један пример добре праксе, који може да помаже у будућим сличним ситуацијама, где је неопходно водити

[419] Мишљење Повереника бр. 011-00-00181/2011-05 од 23.05.2011. год, 2.

управни поступак ради заштите општих интереса, али уједно и заштити приватност појединца.

2.5.2. Упозорења Повереника

У вршењу овлашћења из своје надлежности Повереник, између осталог, врши и контролну функцију која може резултирати издавањем акта у облику упозорења, којим се на ауторитативан начин упозорава руковалац или обрађивач података на неправилности у свом раду и саветује о начину исправљања недостатака. Упозорења имају превентивну улогу, зато што се руковаоцу или обрађивачу „даје шанса“ да исправи уочене пропусте код чувања и обраде личних података.

Упозорење здравственој установи у вези ас кршењем права приватности запослених новим технологијама

У поступку надзора над здравственом установом „Др Драгиша Мишовић“ из Чачка, у вези са спровођењем и извршењем Закона о заштити података о личности (2008), Повереник је издао упозорење о одређеним актима којима су прекршене одредбе у вези са заштитом личних података.[420] Повереник је упозорио здравствени центар „Др Драгиша Мишовић“ да је поступио незаконито набавком, инсталирањем и конфигурацијом система за евиденцију радног времена запослених путем снимања кажипрста и средњег прста леве руке, за потребе здравственог центра Чачак - Опште болнице Чачак. На овај начин, здравствени центар је починио недозвољену обраду личних података запослених, из разлога што није постојало законско овлашћење руковаоца да прикупља биометријске податке запослених. Преко 800 запослених није дало свој пристанак на предметно коришћење отисака прстију, чиме је прекршена њихова приватност, односно лични подаци.

Провера радног времена и испуњавање радних задатака код руковаоца података може се остварити и на други начин, који мање тангира приватност запослених, па је снимање отисака прстију и обрада биометријских података несразмерна сврси прикупљања и обраде. Уз то, пропуст је учињен и тиме што је

[420] Упозорење Повереника бр. 164-00-00193/20110-07 од 22.09.2011. год.

прикупљањем биометријских података направљена збирка података са личним подацима, која није пријављена и достављена Поверенику, иако постоји таква законска дужност руковаоца података. Здравствени центар је овим упозорењем обавезан да исправи уочене неправилности и да обавести Повереника о мерама предузетим у циљу отклањања недостатака и неправилности. Ово упозорење је значаја не само за управне органе, већ и за све послодавце који желе да на сличан начин контролишу испуњење радних обавеза запослених.

Упозорење Повереника Министарству унутрашњих послова због пропуштања предузимања одговарајућих мера заштите података у вези са видео надзором

Министарство унутрашњих послова представља (МУП) део јавне управе који обавља послове од значаја за очување јавног поретка, сигурности и безбедности грађана. У обављању својих делатности МУП предузима различите мере како би посматрао и контролисао друштвене токове и употребио одговарајуће мере ради заштите безбедности. У том смислу од посебног значаја је коришћење нових информационо-комуникационих технологија, као што је видео надзор над прометним јавним површинама.

Коришћење технологија видео надзора доводи у везу МУП са личним подацима грађана, што може угрозити њихову приватност. Управо се то и догодило у Србији 2011. године, када је Повереник издао упозорење МУП-у које није предузело одговарајуће кадровске, организационе и техничке мере ради заштите података о личности који се налазе у архивама Полицијске управе за град Београд.[421] Поменуте мере морале су бити предузете како би се спречила злоупотреба и неовлашћен приступ личним подацима.

Упозорење је издато будући да је у поступку надзора Повереник пронашао да руковалац подацима (МУП) не располаже унутрашњим актима у вези са поступањем лица која користе или раде на одржавању система видео надзора, односно који посматрају и снимају саобраћајне улице у граду Београду. На тај начин, МУП није поступио у складу са обавезама руковаоца подацима према Закону о заштити података о личности (2008).

[421] Упозорење Повереника бр. 164-00-00030/2011-07, од 31.03.2011. год.

Такође, уочено је и одсуство примене техничких мера надзора од стране лица која располажу оперативним и надзорним овлашћењима за управљање системима видео надзора, као што је одобрење приступа радној станици путем електронске картице. Рачунарске системе преко којих се одвија снимање и надзор није користио један службеник, већ је могућност приступа имало неколико њих, па се на тај начин изгубила индивидуална одговорност, која би морала да постоји приликом вршења послова безбедности који задиру у приватност грађана. Могућност коришћења система видео надзора имало је и неколико начелника МУП-а. За такву праксу Повереник је навео да је незаконита, будући да се ради о посебној врсти обраде личних података за коју начелници нису имали законско овлашћење.[422]

Због тога, Повереник је обавезао МУП да исправи уочене недостатке и усклади своје пословање са одговарајућим законским прописима, како би се отклонила опасност по личне податке и слободе грађана. МУП-у је остављен рок од 15 дана да обавести Повереника о предузетим мерама и планираним активностима.

Ово упозорење указује на велику важност поштовања одредби закона који уређује заштиту података о личности у области безбедности, као важној карици управног рада. Коришћење електронских технологија у корелацији са задацима и овлашћењима органа управе ствара бројне ризике за безбедност личних података. Због тога је деловање Повереника као независног надзорног органа, који упозорава на пропусте надлежних органа, од изузетног значаја за правилно чување и обраду личних података у електронској јавној управи.

[422] Упозорење Повереника бр. 164-00-00030/2011-07, од 31.03.2011. год., 1-2.

2.5.3. Решења Повереника у поступку инспекцијског надзора

Решење Повереника у вези са спровођењем и извршењем Закона о заштити података о личности (Случај општине Нови Београд)

Када грађани пријаве Поверенику неправилност у раду неког органа или кршење њихових права у одређеном поступку, он може покренути поступак инспекцијског надзора. У овом поступку, овлашћена лица испитују да ли су тачне тврдње о прекорачењу или кршењу одредаба Закона о заштити података о личности. Уколико се утврди да су постојали недостаци, Повереник може донети решење којим одређује мере за исправљање уочених неправилности.

У једном од таквих случајева, Повереник је у поступку инспекцијског надзора поступао по пријави грађана у којој је указано на злоупотребу личних података грађана у поступку уписа у посебан бирачки списак, према одредбама Закона о националним саветима националних мањина.[423]

Као резултат спроведеног инспекцијског надзора Повереник је привремено забранио обраду личних података јединици локалне самоуправе (Градској општини Нови Београд - Управи градске општине) у предмету лица које је поднело пријаву. У конкретном случају, Управа градске општине поступила је супротно одредбама Закона о заштити података о личности (2008), будући да су овлашћена лица евидентирала личне податке (име и презиме, име оца, ознака пола, година рођења, ЈМБГ, број личне карте, место пребивалишта, општина, улица и број и припадност националној мањини) у посебан бирачки списак бошњачке националне мањине за шта нису имала одговарајући правни основ. Радило се о томе да је лице добио решење Градске општине Нови Београд о упису у посебан бирачки списак бошњачке националне мањине, иако није никада подносио захтев за такав упис.

У поступку инспекцијског надзора утврђено је да је захтев за упис потписало неко друго лице, својеручним потписом у списку, без одобрења лица које је уписано, чиме су испуњени елементи кривичног дела неовлашћеног прикупљања личних података и фалсификовања исправа. У циљу исправљања

[423] Решење Повереника у вршењу инспекцијског надзора, бр. 07-00-01090/2010-05, од 27.07.2010. год.

уочених неправилности, Повереник је наредио руковаоцу података да обрише из евиденције све личне податке прикупљене без правног основа. Уз то, Повереник је поднео Првом основном јавном тужилаштву кривичну пријаву против Н. Н. извршилаца кривичног дела неовлашћеног прикупљања личних података и фалсификовања исправа.[424]

Можемо приметити да је Повереник у поступку инспекцијског надзора вршио своја овлашћења штитећи појединачни интерес лица које је против своје воље уписано у посебан бирачки списак, али и јавни интерес, подношењем кривичне пријаве за дело које се гони по службеној дужности.

2.5.4. Закључци Повереника

Закључак о дозволи за изношење података из Србије

Једна од надлежности Повереника тиче се одлучивања о захтевима за изношење података из Србије у иностранство. Ово је важно овлашћење Повереника, будући да изношењем личних података из државе нестаје заштита коју пружају домаћи управни, судски и други органи, па дозвола Повереника представља брану злоупотреби личних података у иностранству. Претходни закон није регулисао питање међународног трансфера података.[425] Иако се у пракси нису појављивали захтеви органа управе за изношењем података, претпоставка је да је таквих изношења било, посебно у вези са институтом међународно – правне помоћи. На овом месту изложићемо случај из праксе којим се дозвољава изношење података у иностранство.

Повереник је у овом случају[426] дозволио руковаоцу података, предузећу *Lexmark International*, да изнесе податке из Србије у Сједињене Америчке Државе.[427] У Решењу којим се дозвољава изношење података, Повереник је прецизно означио који се подаци могу изнети из земље (име и презиме, звање,

[424] Решење Повереника у вршењу инспекцијског надзора, бр. 07-00-01090/2010-05, од 27.07.2010. год., 2.
[425] Наравно и у тренутном Закону о заштити података о личности (2018) Повереника има одређена овлашћења у вези са међународним трансфером података о личности у друге државе или међународне организације, где дозвољава и надгледа правилност преноса података.
[426] Решење Повереника бр. 011-00-00102/2009-05, од 08.03.2011. год.
[427] У даљем тексту уместо Сједињених Америчких држава биће коришћена скраћеница - САД.

електронска адреса, број телефона за контакт и број рачуна у банци запослених), ком обрађивачу у САД се могу проследити и у коју сврху (подаци су се износили у сврху успостављања централизоване базе података за сва привредна друштва *Lexmark* групе). Такође, одлучено је да ће дозвола за изношење података важити док буде трајао *Уговор о обради и преносу података*, закључен између подносиоца захтева и повезане фирме у САД. Такође, подносиоцу је наложено да определи начин поступања са подацима након престанка уговора, као и да успостави мере заштите.[428]

У оваквим случајевима Повереник мора да има у виду значај података који се износе из државе, разлог изношења и сврху обраде података у иностранству. Та дужност се односи на лица приватног и јавног права. Уколико Повереник оцени да сврха није адекватна, да су за одређене личне податке неопходни строжи услови за изношење или уколико процени да руковалац неће бити у могућности да испуни обавезе које има да заштити податке, он може да одбије захтев за изношење. Зато је значајно да институција Повереника буде независна од било каквог спољног утицаја, како би се спречиле злоупотребе и неправилности избегавањем територијалне и функционалне државне надлежности за заштитом личних података.

2.5.5. Питања грађана

Транспарентност рада Повереника огледа се и у блиском односу са грађанима. Грађани се у свакодневном животу сусрећу са различитим питањима и изазовима у вези са коришћењем њихових личних података. Будући да Повереник представља орган који је задужен за развијање свести и праћење начина примене прописа у вези са личним подацима, грађани су се често обраћали служби Повереник са неформалним питањима у вези са њиховим личним подацима.

Због великог интересовања грађана и потребе да се јавно објаве смернице за решавање одређених питања у вези са личним подацима, Повереник је развио праксу објављивања питања и одговора на најзначајнија питања у области

[428] Решење Повереника бр. 011-00-00102/2009-05, од 08.03.2011. год., 1-2.

заштите података.[429] Питања се односе на различите теме, а обухватају и поступање органа јавне власти са личним подацима грађана. У истраживању смо обрадили нека од значајнијих питања.

Могућност објављивања личних података акционара на интернету без њихове сагласности

Једно од питања грађана односило се на могућност објављивања личних података акционара на интернету без њихове сагласности. Многа јавна предузећа могу бити у форми акционарских друштва, па се ово питање односи и на органе управе. У одговору на ово питање, служба Повереника је стала на становиште да лични подаци акционара не могу бити објављени на интернету без њихове сагласности.

Законом о привредним друштвима и Законом о тржишту капитала, стриктно су прописани разлози (сврха) обраде података, прибављених из Јединствене евиденције акционара из Централног регистра (ради одржавања Скупштине акционара). Свако јавно објављивање личних података акционара на сајту без сагласности би представљало обраду без правног основа и адекватне законске сврхе, па је таква обрада супротна начелу законитости обраде података.[430]

Да ли политичка странка има право увида у бирачи списак општинске управе у којој се подаци воде ?

Од значаја за употребу информационо-комуникационих технологија у вези са личним подацима је питање да ли политичка странка има право да изврши увид у бирачки списак или да добије податке у електронском облику од стране општинске управе у којој се ти подаци воде ?

Повереник сматра да није дозвољено давати на увид и коришћење личне податке бирача (било да се ради о бирачком списку било делова бирачког списка за уже подручје, као што је подручје јединице локалне самоуправе). Уколико би надлежни орган управе, у овом случају Министарство надлежно за послове

[429] Питања и одговори се постављају на сајту Повереника за информације од јавног значаја и заштите података о личности. Питања су постављена у анонимној форми.

државне управе, уступило одређеном лицу (политичкој странци) податке о бирачима, то би представљало прекршај, а лице у оквиру органа власти би учинило кривично дело недозвољеног објављивања личних података.

Одступања су могућа једино у случајевима које су предвиђени Законом о јединственом бирачком списку. Примера ради, право на увид проглашене изборне листе има подносилац изборне листе. Такође, када министарство надлежно за послове државне управе донесе решење о закључењу бирачког списка, оно има законску обавезу да их достави Републичкој изборној комисији. Дакле, једино у поменутим законом предвиђеним ситуацијама одређена лица имају право да изврше увид у бирачки списак или да добију податке у електронском облику.[431]

Да ли постоји могућност обраде и коришћења података у друге сврхе у односу на коју су законски прикупљени ?

У пракси се поставило питање, да ли општинска управа податке о корисницима борачко инвалидске заштите, које обрађује на основу закона, може користити у друге сврхе, као што је слање честитки (новогодишњих, рођенданских и слично) ?

Одговор на ово питање у уској је вези са сврхом обраде података, односно са принципом да се подаци могу користити и обрађивати само у сврху због које су прикупљени, а не и у друге сврхе. Због тога, органи управе морају добити изричиту сагласност лица чији су подаци, како би користили њихове личне податке у друге сврхе (као што је слање честитки и промотивног материјала) у односу на оне ради које су првобитно прибављени.

[431] Повереник за информације од јавног значаја и заштиту података о личности, Питања и одговори, *https://www.poverenik.rs/sr/%D0%B7%D0%B0%D1%88%D1%82%D0%B8%D1%82%D0%B0-%D0%BF%D0%BE%D0%B4%D0%B0%D1%82%D0%B0%D0%BA%D0%B0/%D0%BF%D0%B8%D1%82%D0%B0%D1%9A%D0%B0-%D0%B8-%D0%BE%D0%B4%D0%B3%D0%BE%D0%B2%D0%BE%D1%80%D0%B84/1600-%D0%BF%D0%B8%D1%82%D0%B0%D1%9A%D0%B0-%D0%B8-%D0%BE%D0%B4%D0%B3%D0%BE%D0%B2%D0%BE%D1%80%D0%B8.html*, 19. новембар 2018.

Коришћење биометријских података запослених ради контроле поштовања радних обавеза

У вези са радним правом поставило се питање да ли послодавац може обрађивати биометријске личне податке запослених ради контролисања квалитета рада и поштовања радних обавеза, попут радног времена.

Ово питање тангира и органе управе, будући да прописи о раду важе и за запослене у овим органима. Повереник је у свом одговору навео да „увођење биометријских мера само и искључиво ради контроле коришћења радног времена је прекомерно, несразмерно и њихово увођење представља непотребно задирање у приватност појединца, јер се сврха обраде може постићи и на друге начине као што су боља организација запослених, одређивање лица која ће контролисати одлазак и долазак запослених, а штета која може настати злоупотребом ових података већа је од користи коју руковалац података може имати“.[432]

***

Пракса Повереника у области заштите података је од великог значаја за све органе управе. Штавише, она је од значаја за сва лица која обрађују и чувају личне податке. Иако се одлуке Повереника односе на посебне случајеве, они служе као смерница за будуће поступање свих оних који се нађу у сличним ситуацијама. Зато је неопходно да се приликом обраде личних података у органима управе води рачуна о пракси Повереника, чиме се осигурава законитост обраде личних података, али и поштовање правила општег управног поступања.[433] Уз претходно речено, истичемо предлог да све одлуке Повереника треба да буду

[432] Повереник за информације од јавног значаја и заштиту података о личности, Питања и одговори, *https://www.poverenik.rs/sr/%D0%B7%D0%B0%D1%88%D1%82%D0%B8%D1%82%D0%B0-%D0%BF%D0%BE%D0%B4%D0%B0%D1%82%D0%B0%D0%BA%D0%B0/%D0%BF%D0%B8%D1%82%D0%B0%D1%9A%D0%B0-%D0%B8-%D0%BE%D0%B4%D0%B3%D0%BE%D0%B2%D0%BE%D1%80%D0%B84/1596-%D0%BF%D0%B8%D1%82%D0%B0%D1%9A%D0%B0-%D0%B8-%D0%BE%D0%B4%D0%B3%D0%BE%D0%B2%D0%BE%D1%80%D0%B8.html*, 19. новембар 2018.

[433] У оквиру начела законитости и предвидљивости управног поступања, Законом о општем управном поступку предвиђено је да орган приликом доношења одлуке води рачуна о претходним одлукама у истим или сличним управним стварима, што је од посебног значаја за област заштите личних података. Вид. чл. 5, ст. 3, Закона о општем управном поступку. На овај начин остварује се функционалност система заштите података у оквирима електронске јавне управе и управног поступања.

јавно објављене на интернет презентацији и доступне за преузимање (разуме се, без личних података, већ анонимно). На тај начин, руковаоци и обрађивачи би се лакше сналазили у обављању својих послова и усклађивали би пословање са објављеном праксом, до би грађани били упознати са праксом Повереника и на тај начин би лакше разумели и заштитили своја права. Такође, објављивање праксе би се могло схватити и као ширење свести о значају и улози података о личности у свакодневном животу.

3. НЕЗАВИСНА КОНТРОЛНА ТЕЛА У ОБЛАСТИ ЗАШТИТЕ ЛИЧНИХ ПОДАТАКА У ЕУ

3.1. Правна природа независних контролних тела у ЕУ

Ради бољег разумевања независног контролног тела у Србији, кратко ћемо се осврнути на сличне институције у оквиру ЕУ. Систем заштите личних података ЕУ заснива се на јаким механизмима правне заштите који омогућавају остваривање права и интереса грађана пред различитим органима. Један од таквих механизама односи се на правну заштиту личних података коју пружају независна надзорна тела држава чланица.

Како би обезбедили примену одредаба основног прописа у овој области, Опште уредбе ЕУ, њени творци су предвидели обавезу држава чланица да на својим територијама установе независни надзорни орган који ће се бавити питањима заштите личних података. Независни надзорни орган по својој правној природи представља тело са јавним овлашћењима који се оснива ради вршења надзора над применом уредбе и националних прописа у вези са личним подацима. У зависности од структуре држава чланица, могуће је установити више надзорних органа. У том случају неопходно је именовати водећи надзорни орган који је надлежан за читаву територију државе чланице и прекограничну сарадњу са иностраним надзорним органима и институцијама ЕУ.[434]

Како би успешно обављао своју функцију надзорни орган мора да буде у потпуности независан од сваког спољног утицаја и инструкција грађана, привредних субјеката, органа јавне власти, других држава и међународних

[434] Чл. 56, Опште уредбе ЕУ.

институција. Независност се остварује кроз самостално обављање посла и избегавању вршења делатности које су неспојиве са пословима надзорног органа. Такође, сваки надзорни орган има могућност именовања свог особља које води и усмерава руководилац органа. Да би независно обављао своју функцију, контролни орган је подвргнут финансијској контроли која ни на који начин неће утицати на његову независност, а сам рад органа финансираће се из буџета државе чланице. Независност се огледа и томе да члан независног надзорног органа може бити разрешен дужности искључиво због тешке повреде радне обавезе или због тога што више не испуњава услове који су неопходни за обављање тог посла.

Независни орган може бити именован од стране народне скупштине, владе, шефа државе или другог тела које је правом државе овлашћено да врши именовање.[435] Сви запослени у оквиру независног надзорног тела морају поседовати личне и професионалне квалитете у области заштите података о личности, како би могли да обављају функцију на правилан и целисходан начин. Дакле, предвиђен је широк круг субјеката који могу именовати надзорни орган, имајући у виду разлике у правним системима држава чланица ЕУ.

На овом месту постављамо питање оправданости широко постављеног круга субјеката који могу да именују контролни орган, посебно због његове независности. Влада или шеф државе представљају органе извршно-политичке власти. Именовањем контролног органа од стране владе или шефа државе доводи се у питање независан рад, будући да то лице, односно орган, „зависи“ од политичких промена, а уз то може имати „обзира“ према органу који га је именовао и који га може сменити.

Међутим, ситуација у вези са независношћу не побољшава се умногоме ни када независне контролне органе бирају представници парламента или другог независног органа.[436] Наиме, представници парламента обично припадају одређеним политичким опцијама, те уколико они бирају одређено лице или тело

[435] Чл. 53, Опште уредбе ЕУ.
[436] Овде се ствара зачарани круг, будући да се опет поставља питање ко бира независни орган који именује независни надзорни орган у области заштите личних података.

за надзорни орган, оно може бити наклоњено тој већини, трудећи се да сачува свој положај.

Такође, политички договори могу довести до тога да се за контролно тело не изаберу најбољи и најстручнији кандидати, већ они који су најбоље прошли у политичким споразумима и договорима. Због тога, сматрамо да је најадекватније решење да се законом пропишу строги услови који се захтевају за руководећег или члана надзорног независног тела. Једино на тај начин се може очекивати интегритет обављања делатности и стручност у раду надзорног независног органа. Прописивањем обавезних услова попут стручности у области права и информатике и дугогодишњег рада у области заштите података и људских права, омогућавају стабилне полазне тачке за стручан и квалитетан рад ове важне институције, што треба да се узме у обзир и у правном систему Србије.

3.2. Надлежност и задаци независних контролних тела у ЕУ

Свака држава чланица ЕУ има обавезу да донесе пропис којим ближе уређује услове неопходне за обављање функције независног контролног органа. У сваком случају, надлежност независног надзорног органа поједине државе чланице простире се искључиво на њеној територији према одредбама о територијалној примени Опште уредбе ЕУ.[437]

Основни задатак независног контролног тела тиче се контроле примене одредаба Опште уредбе ЕУ и домаћих прописа који уређују област личних података, заштите приватности и других права у вези са личним подацима грађана. Контролна улога се остварује и кроз решавање притужби које подносе грађани у вези са повредама њихових личних података. Поступање по притужбама подразумева поступак у коме се испитује да ли је дошло до одређене повреде, доношење одговарајућег акта и налагање мера којим се исправљају уочене незаконитости и неправилности у раду.

[437] Општа уредба ЕУ се примењује на обраду података о личности у оквиру активности коју врши руковалац, односно обрађивач са седиштем на територији ЕУ, на обраду података о личности лица које је из ЕУ, а обраду врше руковалац или обрађивач који немају седиште у ЕУ (у случају нуђења робе или услуга лицима на територији ЕУ или у случају активности тих лица на територији ЕУ). Вид. чл. 3 Опште уредбе ЕУ.

Развијање свести и упознавање јавности са ризицима и начинима заштите личних података представља још један задатак овог тела. Тежња је да се превентивним деловањем спрече повреде и створи свест о неопходности заштите личних података свих субјеката друштвеног живота. Превентивна улога се остварује одговорима на захтев грађана, пружањем информација и саветодавних мишљења органима јавне власти у доношењу аката у вези са личним подацима, сарадњи са органима јавне управе, страним државама и међународним организацијама у циљу побољшања деловања, развијања сарадње и размене добре праксе између надзорних тела различитих држава.

Будући да је ЕУ наднационална творевина, сарадња између надзорних органа држава чланица остварује се кроз узајамно пружање информација и помоћи у циљу остваривања адекватне заштите података на територији ЕУ. Контролни органи држава чланица могу вршити заједничке послове, истраге и мере ради решавања предмета који се односе на више држава чланица. То подразумева да гостујући надзорни орган може добити овлашћења од домаћег надзорног органа у циљу спровођења мера које су неопходне ради решавања предмета поступка, а односе се и на податке грађана гостујућег надзорног органа. Треба поменути и питање одговорности за штету у овим случајевима. Уколико особље гостујућег надзорног органа приликом вршења делегираних овлашћења од стране државе домаћина причини некоме штету, за њу одговара држава чланица надзорног органа домаћина.

3.3. Овлашћења независних контролних тела у ЕУ

У вршењу послова из своје надлежности независни контролни органи располажу јавним овлашћењима. Јавна овлашћења надзорних органа могу се сврстати у три групе. То су: истражна, корективна и саветодавна овлашћења.[438]

Прва група овлашћења усмерена је на испитивање правилности рада и аката у вези са обрадама личних података грађана. Када примењују овлашћења из ове групе, независни надзорни органи држава чланица могу издавати обавештења о повредама и начинима њиховог отклањања, издавати наредбе у циљу вршења

[438] Чл. 58, Опште уредбе ЕУ.

контроле, вршити испитивање обрада и разгледати документацију и просторије у циљу вршења надзора. Такође, ова група овлашћења усмерена је на обавештавање руковаоца и обрађивача о евентуалним повредама прописа.

У корективна овлашћења независних надзорних органа убрајамо давање упозорења руковаоцима и обрађивачима због уочених неправилности и могућих повреда права грађана, издавање опомени због незаконитости и неправилности у раду, издавање налога у циљу правилнијег вршења обраде или брисањем података, а могу изрицати и административне новчане казне. Независна надзорна тела имају могућност да наложе обуставу преноса података корисницима у иностранству или у међународним организацијама.

Трећа група овлашћења је саветодавне природе и усмерена је на превентивно деловање код доношења општих и појединачних аката у вези са личним подацима. Независна надзорна тела могу саветовати руковаоце и обрађиваче приликом прикупљања и обрађивања података, давати мишљења и одобрења у вези са кодексима понашања, уговорних клаузула, управних уговора, итд.

3.4. Положај независних контролних тела у појединим државама чланицама ЕУ

3.4.1. Независно контролно тело у Хрватској

Република Хрватска[439] је држава чланица Европске уније од 2013. године, па прописи у области заштите података ЕУ важе и у овој држави. То се односи на Општу уредбу ЕУ која важи на целој територији ЕУ, без потребе да се посебно имплементира у правни систем државе чланице. Ипак, ради конкретизације одредаба Уредбе, Хрватска је донела свој Закон о примени Опште уредбе о заштити података (*Zakon o provedbi opće Uredbe o zaštiti podataka*).[440] Овим законом у области заштите података именована је Агенција за заштиту особних

[439] У даљем тексту уместо Република Хрватска биће коришћена скраћеница Хрватска.
[440] Zakon o provedbi Opće uredbe o zaštiti podataka, Narodne novine Hrvatske 42/12, od 25.05.2018. год.

података, као државно тело које је самостално и независно у свом раду и које за свој рад одговара Хрватском сабору.[441]

Агенција функционише у облику правног лица којем су поверена јавна овлашћења у циљу вршења управних и стручних послова у вези са заштитом личних података. У надлежност Агенције, између осталог, спадају послови: надзирања примене заштите личних података, решавање о захтевима у вези са повредом права, праћење стања у области заштите података, праћење изношења личних података из државе, итд.

Радом агенције руководи директор кога именује и разрешава Хрватски сабор на предлог Владе Хрватске.[442] Директор мора бити хрватски држављанин који има високу стручну спрему и 10 година радног искуства (није потребно да радно искуство буде у пословима заштите личних података). Такође, заменика директора поставља Хрватски сабор на предлог Владе. Директор и заменици се бирају на период од 4 године, са правом реизбора.

На овом месту можемо поставити питање да ли Агенција може у свему независно и самостално обављати своју функцију будући да директора предлаже Влада, као орган политичко-извршне власти ? Иако то не мора да буде случај, сматрамо да је целисходније решење по коме директора овог тела предлаже Парламент (Народна скупштина), као орган у коме се налазе представници грађана, односно носилаца државног суверенитета. Влада управља и усмерава политиком једне земље, па су њене одлуке у највећем делу политичке природе.

Предлог Владе да одређено лице постане директор може представљати „отежавајући“ фактор у независном обављању послова читаве агенције, будући да на тај начин директор „дугује“ Влади која управља и радом органа јавне управе. Уз то, Влада има могућност да предложи разрешење директора Агенције у законом предвиђеним случајевима (осуда, губитак пословне способности, повреди закона у обављању послова и дужности).[443]

[441] Чл. 4, ст. 1 и ст. 2, Zakona o provedbi Opće uredbe o zaštititi podataka.
[442] Чл. 11, Статута Агенције за заштиту особних података од 04.07.2004. год. Текст Статута је доступан на: *https://azop.hr/images/dokumenti/159/statut_agencije_za_zastitu_osobnih_podataka.pdf*, 30. септембар 2018.
[443] Чл. 15, Статута Агенције за заштиту особних података.

Унутрашња структура Агенције подељена је на службе (одјеле) и одсеке. Службама руководе начелници службе, док управници одсека руководе одсецима. Тренутно постоје три службе, а то су служба за заштиту личних података, служба за надзор и средишњи регистар и служба за међународну сарадњу, ЕУ и правне послове. Директор, заменик директора и начелници сектора чине стручни колегијум који је саветодавно тело које помаже ради дефинисања основних питања у раду Агенције.

Основни циљ Агенције за заштиту личних података је адекватна примена одредаба прописа ЕУ и Хрватске у области заштите података, као и заштита основних права и слобода грађана у вези са личним подацима. Уз то, Агенција води рачуна о подизању свести о правима и дужностима у области заштите података.

3.4.2. Независно контролно тело у Француској

Република Француска[444] је једна од највећих држава чланица ЕУ, што значи да се на њеној територији примењује Општа уредба ЕУ. Француска је донела свој Закона о заштити личних података.[445] Уз поменути закон, важно је поменути још два прописа. То су Закон о информационим технологијама, подацима и грађанским слободама из 1978. год. (више пута мењан)[446] и Декрет о примени Закона о информационим технологијама, подацима и личним слободама,[447] као једним од првих европских прописа у области заштите података, којима је установљено независно надзорно тело.

У Француској постоји независно контролно тело које надзире примену прописа и закона у области заштите података. Реч је о Националној комисији за информатику и слободе (*Commission nationale de l'informatique et des libertés-*

[444] Уместо Република Француска у даљем тексту биће коришћена скраћеница Француска.
[445] Закон о заштити личних података Француске- Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles (Закон о заштити личних података Француске).
[446] Закон о информатици, подацима и грађанским слободама *Loi infromatique et liberties act* no. 78-17 of 06.01.1978, *https://www.cnil.fr/sites/default/files/typo/document/Act78-17VA.pdf* , 01. новембар 2018.
[447] Decree No. 2005-1309 of 20 October 2005, *https://www.cnil.fr/sites/default/files/typo/document/Decree_20_October_2005_English_version.pdf*, 01. новембар 2018.

CNIL) која представља независну контролну организацију.[448] Ово тело је основано доношењем поменутог Закона о информационим технологијама, подацима и грађанским слободама из 1978. године, али је прихватило измењене надлежности Законом о заштити личних података.

Независност тела омогућена је специфичном композицијом његових чланова. Национална комисија састоји се од 17 чланова, при чему су 4 члана представници парламента (2 из Народне скупштине и 2 из Сената), 2 члана су представници Француског економског, социјалног и еколошког савета, 6 су представници судства (2 члана Државног савета, 2 члана Касационог суда и 2 члана Рачунског суда), као и 5 стручних лица које бирају председавајући Народне скупштине, Председник сената, и Француски кабинет (3 лица). Мандат свих чланова траје 5 година, осим у случају представника Парламента који су на тој функцији колико им траје мандат. Чланови међу собом бирају председавајућег.[449] Независност тела значи да оно не прима инструкције или налоге од било ког органа или лица. Такође, ово тело је и финансијски независно и финансира се из посебног дела буџета Француске. Национална комисија Француске свакако има специфичан положај и несвакидашњи састав. Тежња са оваквим унутрашњим саставом комисије јесте да се обезбеди независност чланова, као и да тело не буде хомогено, што омогућава различитост мишљења и балансирање „снага“ оних који бирају представнике у ово тело.

Чланови заседају на пленарним седницама које се одржавају једном недељно, на основу предлога дневног реда који установљава председавајући. Основни задаци Националне комисије односе се на информисање и едукацију грађана у области заштите личних података, надзор над применом релевантних норми у области заштите података, саветовање и давање мишљења институцијама у поступању са личним подацима, итд. Наравно, грађани се могу обратити Националној комисији ради заштите личних података, као и права у вези са подацима о личности.

[448] G. Dupuis, M. Guedon (1988), 59
[449] CNIL, Status and Composition, *https://www.cnil.fr/en/node/287* , 11. новембар 2018.

3.4.3. Независно контролно тело у Аустрији

Као и остале државе чланице ЕУ, Република Аустрија[450] (у даљем тексту: Аустрија) донела је свој закон којим ближе уређује питања у области заштите података и личности. Федерални закон о заштити личних података (*Bundesgesetz über den Schutz personenbezogener Daten)*[451] ступио је на снагу 25. маја 2018. године, у исто време када и Општа уредба ЕУ.

У Аустрији, делатност надзора над поштовањем норми у вези са заштитом података обавља Повереник за заштиту података (*Datenschutzbehörde*). Ово тело надледа и усаглашеност пословања са европским и аустријским законима и обавља друге задатке поверене на основу Опште уредбе ЕУ.[452] Повереник је основан као национално надзорно тело које је независно од сваког спољног утицаја, што се огледа и у инкомпатибилности других делатности које могу довести у сумњу његову независност или повредити јавни интерес. Повереник се бира на период од 5 година, уз могућност реизбора. Кандидата за директора предлаже Влада Аустрије, а именује га Федерални Председник. Кандидат мора да има завршен правни факултет, мора да поседује личне и професионалне способности које га квалификују за ову функцију, да поседује изврсна знања из области права заштите података и људских права на територији Аустрије и ЕУ, као и да има минимум 5 година професионалног искуства у правној струци.[453]

Што се тиче начина избора Повереника, сматрамо да независност није омогућена у пуној мери. Разлог лежи у предлагачу Повереника, односно Влади, која представља орган извршне власти, те се не може очекивати потпуна неутралност Повереника у односу на тело које га предлаже и које усмерава органе управе које после сам Повереник треба да контролише (у области заштите личних података). Уз све то, Повереник може да буде разрешен дужности на предлог Федералне Владе, а одлуком Федералног Председника.

---

[450] У даљем тексту уместо Република Аустрија биће коришћена скраћеница Аустрија.

[451] Федерални закон о заштити личних података Аустрије- Bundesgesetz über den Schutz personenbezogener Daten- Datenschutzgesetz 2000 – DSG 2000. Текст овог закона на немачком и енглеском језику доступан је на: *https://www.ris.bka.gv.at/Dokumente/Erv/ERV_1999_1_165/ERV_1999_1_165.html*, 01. новембар 2018.

[452] За више о Аустријском телу за заштиту података вид. поглавље 2, део 4. Закона о заштити личних података Аустрије

[453] Вид. Део 2, параграф 20, Аустријског федералног закона о заштити личних података.

Ипак, личне, професионалне и стручне квалификације које се захтевају за Повереника обезбеђују потребан квалитет и интегритет кандидата, што у одређеној мери има утицаја и на независност ове институције. У односу на друге државе ЕУ, Аустрија је прописала строжије услове за избор Повереника. Прописивањем строжијих услова долази до природне селекеције, те се у обзир могу узети само квалитетни кандидати који својим минулим радом гарантују адекватно обављање послова које спадају у надлежност Повереника.

Сматрамо да је оваква законодавна пракса пожељна и да је треба имплементирати у правни систем Србије, како би се обезбедио ефикасан и квалитетан рад институције Повереника за информације од јавног значаја и заштиту података о личности.

3.5. Значајније одлуке независних контролних органа у вези са Општом уредбом ЕУ

Општа уредба ЕУ ступила је на снагу маја 2018. године, нешто пре почетка рада на истраживању, па пракса независних надзорних тела на основу овог прописа није развијена. Ипак, појавиле су се прве значајније одлуке, које садрже високе казне због повреде личних података. У складу са доступном праксом, поменућемо неке од случајева.

Једну од строжијих казни због непоштовања одредаба Опште уредбе ЕУ изрекло је португалско надзорно тело – Национална комисија за заштиту података (*The CNPD – Comissão Nacional de Protecção de Dados*). Комисија је изрекла Бареиро болници (*The Centro Hospitalar Barreiro Montijo*) казну у износу од 400.000 евра, због чињења доступним јавности нарочито осетљивих личних података у вези са здравственим стањем грађана.

Наиме, надзорни орган је пронашао да је девет социјалних радника имало право приступа лекарским документима који су садржали осетљиве здравствене податке грађана. Уз то, чак 985 лица је било регистровано за електронским приступ подацима на „нивоу доктора“ иако је од тог броја само 296 особа запослено у тој болници. У своју одбрану болница је изнела став да је велики број од 985 лица у ствари и не постоји, већ да су то само „привремени профили“ за докторе који раде на уговорној основи. Такође, болница је изнела тврдњу да је за

одржавање информационог система у њиховој болници надлежно португалско министарство здравља.

Укупан износ од 400.000 евра односи се на две казне. Прва износи 300.000 евра и изречена је због тога што болница није поштовала поверљивост личних података пацијената будући да је омогућила приступ неовлашћеним лицима. Други део казне у износу од 100.000 долара изречен је због неспособности болнице да обезбеди интегритет система заштите података у оквиру свог електронског система. На ову одлуку независног надзорног тела, болница је најавила да ће покренути судске поступке.

Аустријско надзорно тело (*Datenschutzbehörde*) донело је одлуку по Општој уредби ЕУ, у вези са употребом системом географског праћења (ГПС) у области радних односа. Одлука је донета у вршењу инспекцијског надзора који је покренут по службеној дужности, а суштински се односило на питање да ли је потребан одговарајући пристанак запосленог у односу на ГПС надзор, према одредбама Опште уредбе ЕУ.

Предузеће је навело да се користило системом лоцирања ради заштите имовине, олакшавања финансијског обрачуна са фирмом од које су узета кола на лизинг, као и ради планирања, оптимизације и скраћивања пута којим се креће запослени. Уз то, предузеће је навело да податке прикупљене на тај начин чува 93 дана и да је обрада законита, будући да је запослени дао свој пристанак на обраду личних података у поменуте сврхе.

Ипак, аустријски надзорни орган сматра да је упитно да ли у радно-правним односима постоји могућност за давањем добровољног пристанка запосленог, управо због потчињеног положаја запосленог. Надзорни орган је истакао да се не може идентификовати видљива предност за запослене приликом праћења, па је упитна добровољност код таквог пристанка. Зато је донета одлука којом се налаже предузећу да усклади обраду података запослених са одредбама Опште уредбе ЕУ, будући да не постоји адекватан правни основ за обраду, а тиме и одговарајући пристанак запослених.

У образложењу је наведено да је неопходно да послодавац установи и конкретизује легитимне интересе за праћење запослених, будући да се не може говорити о добровољности пристанка потчињеног лица у радно-правним

односима у поменутом случају. Од значаја је поменути да када постоји синдикат запослених (радни савет), тада мора да постоји споразум између послодавца и радног савета у вези са поменутим питањима. Када не постоји радни савет код послодавца, тада је неопходно прибавити писмену сагласност запосленог.[454] Ова одлука је од великог значаја за поступање свих послодаваца на европском нивоу, па тако и органе јавне управе, у случајевима када се одлуче на употребу информационих система који прате кретање запослених.

Најстрожију казну у краткој историји заштите података (за сада), а самим тим и на основу Опште уредбе ЕУ, изрекла је Француска комисија за заштиту података. На основу представки удружења *None of Your Business* и *La Quadrature du Net,* Комисија је извршила инспекцијски надзор и казнила компанију *Google LLC,* због мањка транспарентности, неадекватних информација о обради личних података и недостатку одговарајућих сагласности за обраду података, у износу од 50 милиона евра.[455]

У поступку инспекцијског надзора Комисија је пронашла да значајни елементи обрада, попут сврха обраде, периода чувања личних података, коришћење података у сврхе другачије од оних за које су прикупљене нису усклађене са правилима Опште уредбе ЕУ. Подаци о овим елементима нису били лако доступни лицима чији се подаци обрађују, већ да би се дошло до ових података, лице је морало да прође неколико корака на интернет адреси компаније, што је у супротности са основним начелима Опште уредбе ЕУ. Такође, сврхе обраде су неретко констатоване веома апстрактно и нејасно, па је било неопходно да се пристанак за обраду личних података добије за појединачну сврху, док је компанија користила податке за своје различите сервисе без посебног одобрења.

Због кршења одредби Опште уредбе ЕУ, Комисија је одлучила да казни компанију новчаном казном у износу од 50 милиона евра. Оваква одлука Комисије је од значаја за све оне који обрађују податке грађана у различите сврхе,

---

[454] Matthias Schmidl, „100 Tage DSGVO aus Sicht der Datenschutzbehörde, Keine freiwillige Einwilligung zur Verwendung eines „GPS-Trackers““, y: *Firmenfahrzeugen newsletter*, 3/2018, online 2018, 3, *https://www.dsb.gv.at/documents/22758/115212/Newsletter_DSB_4-18.pdf/8d475c88-615c-4a1f-a014-464e0018a9c0* , 20. јануар 2019.

[455] Одлука CNIL - Délibération n°SAN-2019-001 du 21 janvier 2019, *https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000038032552&fastReqId=2103387945&fastPos=1,* 20. јануар 2019.

јер неправилна примена правила у вези са личним подацима може водити значајним финансијским губицима, али и губљењу угледа код корисника и клијената.

4. МЕХАНИЗАМ СУДСКЕ ЗАШТИТЕ ЛИЧНИХ ПОДАТАКА

Осим независних контролних тела, важну улогу у поштовању људских права и контроли законитости обраде личних података у електронској јавној управи има судска грана власти. Судска власт представља значајан механизам контроле, будући да је она независна од других грана власти, што омогућава непристрасност у одлучивању. Основни циљ судске заштите јесте да пружи заштиту правима, слободама и интересима грађана. Иако је потпуно одвојена од извршне гране власти, којој припада јавна управа, судска власт је повезана са управом на тај начин што врши контролу законитости над радом органа управе,[456] али и контролу законитости аката и рада независног контролног тела у области заштите личних података.

4.1 Облици судске заштите личних података у Србији

Као што је поменуто, Устав гарантује заштиту података о личности.[457] У случају повреде или злоупотребе личних права, грађанима је уставом загарантовано право на судску заштиту личних података, која се ближе уређује законом.

Иако је Устав донет 2006. године, претходни Закон о заштити података о личности (2008) није детаљније регулисао питање судске заштите личних података. Само у одређеним сегментима, као што је обрада података и нарочито осетљивих података после опозива пристанка, Закон је предвиђао право на накнаду оправданих трошкова и право на накнаду штете, у складу са прописима којима се уређује одговорност за штету.[458] Друга питања која су од значаја за судску заштиту личних података поменути закон није предвиђао.

[456] „Како је законитост управе у свим правним системима основно начело управног права, то и судска контрола управе има посебно место у његовом изучавању“. Jelena Jerinić, *Sudska kontrola uprave*, Pravni fakultete Univerziteta Union, Beograd 2012, 13.
[457] Чл. 42, Устава Републике Србије.
[458] Чл. 11, ст. 3, и чл. 18, Закона о заштити података о личности (2008).

Тако је у правном систему остала празнина, будући да је законодавац пропустио да регулише специфичности материје личних података и да уреди поједине елементе судског поступка у коме се остварује заштита личних података (рокови, надлежност, и томе слично).

Са друге стране, закон који уређује питања одговорности за штету, Закон о облигационим односима,[459] предвиђа могућност накнаде штете у случају повреде права личности. Права личности могу се на посредни начин довести у вези са личним подацима. Ипак, лични подаци не могу се изједначити са правима личности, већ се они односе само на одређене објекте појединих права личности, као што су право на име, право на лични идентитет, право на глас, итд.[460] То значи да није јасно одређено да су грађани имали право на накнаду материјалне или нематеријалне штете због повреде личних података, по овом закону.

Нови Закон о заштити података о личности (2018) исправио је пропусте и детаљније уредио начине остваривања судске заштите података о личности. На основу тренутног стања регулативе, судску заштиту личних података у Србији можемо поделити на четири облика заштите. Први се односи на судску заштиту против одлука Повереника, други се односи на пружање судске заштите у случају повреде личних података од стране руковаоца и обрађивача (органа управе), трећи облике се односи на судску заштиту у поступцима за накнаду штете због повреде личних података, док се четврти облик односи на прекршајни судски поступак који се води због прекршаја у вези са личним подацима.

[459] Закон о облигационим односима, *Службени лист* СФРЈ, бр. 29/78, 39/85, 45/89 – одлука УСЈ и 57/89, *Службени лист* СРЈ, бр. 31/93 и *Службени лист* СЦГ, бр. 1/2003- Уставна повеља. Уместо Закон о облигационим односима у даљем тексту биће коришћена скраћеница ЗОО

[460] Dragan Prlja, Stefan Andonović, „Naknada štete kod povrede ličnih podataka“, u: Odgovornost za štetu, naknada štete i osiguranje (ur. Zdravko Petrović, Vladimir Čolović), Institut za uporedno pravo, Udruženje za odštetno pravo, Pravosudna akademija, Valjevo-Beograd 2018, 232.

4.2. Право на судску заштиту против одлука Повереника

Иако представља независну и стручну службу која пружа заштиту личним подацима грађана, може се десити да Повереник донесе одлуку која није правилна или законита. Због тога, у правни систем Србије уведена је могућност судске заштите против одлука Повереника, будући да његова овлашћења (могућност упозоравања и кажњавања) могу значајно утицати на правну позицију лица на које се одлука односи.[461]

Лице чији се подаци чувају и обрађују, руковалац, обрађивач, односно друго физичко или правно лице на које се односи одлука Повереника, имају право да против те одлуке покрену управни спор у року од 30 дана од дана пријема.[462] Поступак се покреће тужбом, а покретање овог поступка пред управним судом не представља сметњу за вођење других управних и судских поступака у вези са личним подацима о којима се у спору расправља. То значи да је могуће истовремено водити више судских поступака против акта или радње којом су повређени лични подаци.

Такође, могуће је водити управни спор против „ћутања“ Повереника. Наиме, када Повереник не донесе одлуку у року од 60 дана од дана подношења притужбе, може се покренути управни спор због „ћутања“ управе, односно непоступања Повереника.[463] Иако Повереник није орган управе, могућност вођења управног спора предвиђена је посебним законом, па се системски тумачећи, проширује и на институт „ћутања“.

Тужба у овом спору подноси се Управном суду, а уперена је против одлуке или пропуштања поступања Повереника. Активну легитимацију у овом спору

---

[461] У последњем доступном годишњем извештају Повереника за 2017. годину, наводи се да ниједно решење ове институције није поништено од стране Управног суда, при чему је овом суду у тој години поднето 57 тужби. Вид. Повереник за информације од јавног значаја и заштиту података о личности, *Извештај о спровођењу закона о слободном приступу информацијама од јавног значаја и закона о заштити података о личности за 2017. годину*, Београд 2018, 9, *https://www.poverenik.rs/images/stories/dokumentacija-nova/izvestajiPoverenika/2017/LAT2017GodisnjiIzvestaj.pdf*, 09. 20. фебруар 2019.

[462] Чл. 83, ст. 1, Закона о заштити података о личности (2018).

[463] За више о управном спору због ћутања управе вид. Ратко Радошевић, „Управни спор због ћутања управе“, *Зборник радова Правног факултета у Новом Саду* бр. 4/2015 (ур. Слободан Орловић), Нови Сад 2015, 1971-1986, као и С. Лилић (2013), 579-580.

имају лице на које се подаци односе, руковаоци и обрађивачи података и друга лица која су незадовољна одлуком Повереника, када се одлука односи на њих.

У управном спору суд може одлучивати искључиво о законитости коначних управних и других аката. То значи да суд неће испитивати правилност и целисходност одлука Повереника. Такође, суд неће моћи да одлучује у спору пуне јурисдикције када је Повереник поступао по дискреционом овлашћењу, будући да он може одлучивати у спору пуне јурисдикције само када природа предмета спора то дозвољава и уколико чињенице конкретног случаја стварају адекватан основ за одлучивање.[464]

- Оправданост испитивања законитости одлука Повереника пред Управним судом ?

Друга недоумица у вези са могућношћу вођења управног спора против одлука Повереника односи се на прихватљивост испитивања одлука независног стручног тела пред Управним судом. Наиме, Повереник представља независни надзорни орган који поседује посебна знања из области заштите личних података. Због тога, може бити упитно да један суд испитује вршење јавних овлашћења независног органа (Повереника) у материји која изискује посебна стручна знања.

Сматрамо да је овакво решење оправдано и у складу са Законом о управним споровима који прописује да суд у управном спору одлучује о законитости „других појединачних аката када је то законом предвиђено“.[465] Управни суд може одлучивати једино о законитости одлука Повереника. То значи да се суд неће упуштати у питања целисходности и сврсисходности рада Повереника, већ ту улогу обавља Народна скупштина, приликом излагања извештаја Повереника. Иако је тачно да суд има мање посебних знања од Повереника, из области заштите података, али његов посао се своди на контролу законитости аката Повереника, што значи да суд представља још једну инстанцу у вези са појединачним одлукама које се односе на личне податке грађана.

Због тога, сматрамо да је контрола законитости Повереникових одлука у управном спору адекватан механизам законитости рада институције Повереника и

[464] Вук Цуцић, *Управни спор пуне јурисдикције*, Правни факултет Универзитета у Београду, Београд 2016, 260.
[465] Чл. 3, ст. 4, Закона о управним споровима.

његових аката. Тиме се не утиче на његову независност, већ се остварују предуслови за правилну примену правних норми. Такође, грађани на тај начин имају на располагању још један степен правне заштите.

4.3. Судска заштита права грађана у вези са повредама података о личности

Гарантовање посебних права грађана у односу на њихове личне податке створило је потребу и за механизмима који ће осигурати њихову примену. Механизми примене остварују се, између осталог, и кроз судску контролу поштовања права у вези са личним подацима. Због тога, новину у законодавству Србије представља могућност остваривања судске заштите у случају повреде неког од посебних права у вези са личним подацима. Овај облик заштите спада у грађанско-правни облик заштите, а може се остварити и уколико се орган управе налази у улози руковаоца или обрађивача података.

Физичко лице на које се подаци односе има право на судску заштиту ако сматра да је неко од његових посебних права, прописано Законом о заштити података о личности (2018), повређено обрадом или неком другом радњом органа управе. Такође, судска заштита може се тражити и када нема повреде, али је орган поступао супротно одредбама закона, што знатно проширује обим заштите.[466] Покретање овог поступка не представља сметњу за вођење других управних или судских поступака у вези са истим личним подацима.

Тужбом којом се покреће судски поступак, тужилац може да захтева остварење ускраћеног права, односно омогућавање коришћења тог права у пуном обиму. Права која могу бити ускраћена лицима јесу право на пружање информације о чувању и обради података физичких лица, право на исправку података, право на брисање података, право на приступ подацима у одређеној форми (у структуираном, уобичајеном и машински читљивом облику), право на прекид обраде и право на преношење података са једног руковаоца у посед другог. Тужилац може захтевати од суда да донесе пресуду којом се утврђује да је аутоматизовано доношење одлука, укључујући и профилисање, извршено супротно закону.

[466] Чл. 84, ст. 1, Закона о заштити података о личности (2018).

Треба поменути да је у споровима заштите права у вези са личним подацима увек дозвољена ревизија против правоснажне судске пресуде. Наравно у овим поступцима важе правила парничног поступка. Увођење судске заштите представља логичан корак у побољшању позиције грађана у вези са личним подацима грађана.

- Питање надлежности суда када је орган управе у улози руковаоца или обрађивача обраде

За овај судски поступак предвиђена је алтернативна месна надлежност суда. Тужба се може поднети вишем суду у месту пребивалишта, боравишта или седишта руковаоца или обрађивача података или пребивалишта, односно боравишта лица на које се подаци односе. На овај начин повећава се степен заштите лица на кога се односе подаци, будући да може да бира ком суду ће поднети тужбу ради заштите својих права.

Међутим, прописано је да се ова надлежност не односи на руковаоце, односно обрађиваче података који припадају органима јавне власти. Због овакве непрецизности, поставља се питање, који суд ће бити надлежан за поступање по тужби која се подноси против органа управе, који је у својству руковаоца/обрађивача повредио неко од посебних права грађана у вези са личним подацима ?

Неспретна законска формулација оставља дилему да ли се у овом случају тужба може поднети вишем суду на територији седишта органа управе или се тужба мора поднети Управном суду, као суду који одлучује о законитости коначних појединачних управних аката.

Сматрамо да је једино исправно прво решење по којем је надлежан виши суд на територији седишта органа управе. Наиме, у надлежност виших судова, између осталог, спада и одлучивање у споровима о заштити права на приватни живот, односно права на лични запис.[467] У складу са таквом надлежношћу је и остваривање људских права у вези са правом на заштиту личних података. Једноставно, одлучивање о заштити и остваривању људских права не може бити предмет управног спора, те Управни суд иако надлежан да контролише

[467] Чл. 23, ст. 1, тач. 7, Закона о уређењу судова, *Службени гласник* РС, бр. 116/2008, 65/2018.

законитост аката органа управе, не би био надлежан да поступа у овим случајевима. Једино у случају негативног решења Повереника по притужби, којим би била потврђена исправност поступања или акта органа управе у вези са личним подацима, може се говорити о вођењу управног спора. Скрећемо пажњу да одлучивање Повереника пре подношења тужбе због повреде права грађана у вези са личним подацима није предвиђен као неопходан услов за тужбу.

4.4. Право на накнаду штете због повреде личних података

Трећа врста судског поступка у вези са личним подацима, односи се на могућност потраживања накнаде за претрпљену штету због повреде личних података. Свако ко је претрпео неки облик материјалне или нематеријалне штете „због повреде одредаба закона (о заштити података о личности)“ има право да пред судом тражи накнаду од руковаоца или обрађивача (органа управе). Иако је прописано да се право на накнаду штете може захтевати само због повреде одредаба Закона о заштити података о личности (2018), то ипак није једини услов за остваривање права на материјалну или нематеријалну штету. За потраживање накнаде штете неопходно је да тужилац докаже да је претрпео и одређену штетну последицу која се огледа у материјалном губитку, претрпљеном страху или болу или повреди права личности због неправилне или незаконите примене законских одредби.

Сва правила одштетног права примењују се и у случају потраживања накнаде штете настале у вези са повредом личних података. Због тога, анализа истраживања биће усмерено једино ка основним питањима које доводе у вези институте накнаде штете и личних података.

Основно одштетно правило гласи да свако ко другоме начини штету дужан је исту накнадити, осим уколико докаже да је штета настала без његове кривице. Постоје два облика штете, материјална и нематеријална. Материјална штета представља умањење нечије имовине или спречавање њеног повећања (измакла корист). Са друге стране, нематеријална штета настаје наношењем другоме физичког или психичког бола или страха[468] и повредом права личности. Будући да

[468] Чл. 155, Закона о облигационим односима.

Закон о заштити података о личности (2018) још није почео да се примењује, судске праксе у вези са накнадом штете код повреде личних података још нема. Због тога, принуђени смо да теоријском конструкцијом анализирамо могућност настанка и накнаде материјалне и нематеријалне штете.

4.4.1. Накнада материјалне штете због повреде личних података

Материјална штета се назива и имовинска штета. Она се класификује у два облика, па постоји стварна штета и измакла корист. „Стварна штета је умањење постојеће имовине, губитак постојеће имовинске вредности. Она се најчешће састоји у уништењу или оштећењу ствари или губитку неког имовинског права…Изгубљена добит је неостварена имовинска вредност, имовинска вредност која би према редовном току ствари или околностима конкретног случаја била остварена да није било штетниковог поступка, нпр. неостварена зарада…“.[469]

На основу појма материјалне штете, постављамо питање да ли она уопште може настати повредом личних података ? Правно посматрано лични подаци не представљају физичку ствар, будући да нису материјализовани. Они могу бити оваплоћени у материјалном облику кроз документ или друго писмено које садржи одређене личне податке грађана. Међутим, ни у том случају се не може говорити о материјалном облику личних података.

Како лични подаци представљају нематеријалне ствари, тешко је замислити ситуацију у којој настаје право на накнаду материјалне (имовинске) штете. Ипак, законска формулација, која наводи да је могуће потраживати накнадну материјалне штете „због повреде одредаба закона“,[470] отвара простор за могућност накнаде материјалне штете. Примера ради, због повреде неког од права у вези са личним подацима (праву на заборав) тужиоцу је умањена имовина или је спречено њено повећање, због тога што је податак о личности био неопходан за реализацију неког другог правног односа који би донео материјалну корист. Такође, уколико је објављен податак о личности, који је требао да буде обрисан, па је таква објава представљала сметњу за закључење правног односа или разлог

[469] Обрен Станковић, Владимир Водинелић, *Увод у грађанско право*, Номос, Београд 2007, 216.
[470] Чл. 86, ст. 1, Закона о заштити података о личности (2018).

за раскид неког другог правно-пословног односа, можемо говорити о могућој накнаде материјалне штете.

Према томе, ширина законске формулације која се односи на разлоге за потраживање накнаде штете омогућује конструкције које подразумевају и накнаду материјалне штете због повреде личних података, али на посредан начин. Напомињемо да се материјална штета не може захтевати искључиво због повреде личних података, већ због повреде неке од законских одредби због које су настале штетне последице (стварна штета или измакла корист) у имовини лица које потражује накнаду.

4.4.2. Накнада нематеријалне штете због повреде личних података

Због правне природе и ширине појма, у теорији није постигнута сагласност око универзалног појма нематеријалне штете.[471] Нематеријална штета, према одређењу Закона о облигационим односима, огледа су у наношењу другоме физичког или психичког бола или страха, као и повреди права личности.[472] Можемо говорити о два облика нематеријалне штете. Један облик нематеријалне штете односи се на негативне последице у облику психичког или физичког бола и страха. Психички бол и страх, као појавни облици нематеријалне штете, могу се јавити као негативна последица објављивања и чињења доступним јавности осетљивих података грађана. Постојање бола и страха неопходно је доказати и стручно потврдити, што је посао судских вештака.

Други облик нематеријалне штете тиче се повреде права личности. Право личности може се одредити као „државном принудом зајамчена могућност субјекта, да неометано, од других реализује лично добро“.[473] У теорији је изложено становиште да ова права припадају човеку, да се тичу одређених личних добара тог човека, као и да се њима штити физичко и морално биће човека.[474] У складу са основним елементима могуће је одредити различита права

[471] Duško Medić, „O naknadi nematerijalne štete“, u: Odgovornost za štetu, naknada štete i osiguranje, (ur. Zdravko Petrović, Vladimir Čolović), Institut za uporedno pravo, Udruženje za odštetno pravo, Pravosudna akademija, Valjevo-Beograd 2018, 93-94.
[472] Чл. 155, и чл. 199, Закона о облигационим односима.
[473] Alojzije Finžgar, *Pravo ličnosti*, Službeni list SFRJ, Beograd 1988, 43.
[474] *Ibid*., 43-48.

личности, као што су право на живот, право на лични идентитет, право на психички интегритет, право на име, итд.[475]

То значи да се појам права личности не може изједначити са личним подацима. Међутим, можемо рећи да неки од објеката права личности (име, глас, фотографија, вероисповест), представљају личне податке. Због тога, када се говори о накнади нематеријалне штете код повреде личних података, по правилу ће бити реч о повреди права личности.[476]

За остваривање права на накнаду нематеријалне штете није довољно да је утврђена повреда личних података, што сматрамо као неадекватно нормативно решење. Један од неопходних услова за остваривање накнаде нематеријалне штете јесте и одређена последица која се огледа у претрпљеном психичком или физичком болу или страху.[477] Када се утврди постојање нематеријалне штете, заједно са штетном последицом и ако је то у складу са околностима конкретног случаја, суд може досудити правичну новчану накнаду. Правична новчана накнада „није по својој природи репарација, већ сатисфакција…због повреде уставом и законом заштићеног личног права или добра. У том смислу, новчана накнада за овај вид штете има превасходно значај моралне сатисфакције".[478]

Правична новчана накнада мора да одговара околностима конкретног случаја и тежини повређеног добра, односно значају повређених личних података. Повреда личних података може се поновити, уколико су подаци јавно објављени. Након повреде личних података у информационом друштву, тешко је пратити њихово даље кретање, будући да се информације лако размењују, па је тешко констатовати да ли су они завршили код још неког неовлашћеног лица. Осим правичне новчане накнаде, суд може наредити штетнику да учини радњу која би остварила сврху накнаде.[479] Примера ради, то може да буде брисање свих

[475] *Ibid*., 73-162.
[476] Овакво становиште потврђује се и ставом да повреда права личности представља основу права на накнаду неимовинске штете. Antonio Radolović, „Pravo osobnosti u novom Zakonu o obaveznim odnosima", *Zbornik Pravnog fakulteta Sveučilišta u Rijeci*, br. 1/2006, (ur. Velinka Grozdanić), Rijeka 2006, 135.
[477] Чл. 155, Закона о облигационим односима.
[478] Пресуда Апелационог суда у Београду, Гж 8976/12 од 10.01.2013. год.
[479] Ови принципи спадају у домен „меког права", па је њихова природа више усмеравајућа него обавезујућа. о облигационим односима.

података у поседу тог лица, или упућивање извињења у средствима јавног информисања.

4.4.3. Објективна концепција нематеријалне штете код повреде личних података

Због неопходног услова у виду штетне последице, поставља се питање могућности остваривања сврхе накнаде нематеријалне штете код повреде личних података.

Повреда личних података не настаје на материјалним добрима, па је готово сигурно да физичко лице неће трпети физичке болове због повреде личних података. Евентуално, повредом података може доћи до негативне последице у виду психичког бола или страха. На овај начин, у великом броју случајева, повреда личних података неће довести до права на накнаду нематеријалне штете, управо због изостанка штетне последице.

Због тога, сматрамо да би у случају повреде личних података требало прихватити објективан појам накнаде нематеријалне штете. Овакав став заузет је и у Начелима европског одштетног права које је усвојила Европска комисија. Начела предвиђају да се нематеријална штета односи и на објективну повреду заштићеног права личности, а не само претрпљене физичке болове и страх.[480] Одређена законодавства, попут Хрватског, такође прихватају ову концепцију. Код објективне концепције, повредом самог права личности настаје право на накнаду нематеријалне штете, док су штетне последице у виду физичког бола или страха једино елемент за одређивање и процењивање накнаде.[481]

Такође, и у теорији проналазимо ставове који се залажу за прихватање објективне концепције накнаде нематеријалне штете. „Нема никаквог разлога да се у одређеним случајевима повреде права личности, када то околности конкретног случаја оправдавају, на захтев оштећеног не досуди новчана накнада

[480] European Group on Tort Law, Principles of European Tort Law, Text and Commentary, Springer, New York, Wien, 2005, 171-178. Ипак Међутим, ови принципи спадају у основне вредности европског права.

[481] Marijana Bukovac Puvača, „Deset godina nove koncepcije naknade neimovinske štete“, *Zbornik Pravnog fakulteta Sveučilišta u Rijeci* (ur. Dionis Jurić), br. 1/2015, Rijeka 2015, 161.

за претрпљену нематеријалну штету због повреде права личности и у случајевима када ова повреда није проузроковала физичке или душевне болове или страх".[482]

Сматрамо да би у материји заштите личних података требало прихватити објективну концепцију накнаде нематеријалне штете, где је за накнаду такве штете довољно утврдити чињеницу повреде личних података, без утврђивања штетне последице у виду страха или бола. Једноставно, правна природа личних података сужава простор за накнаду штете у садањој субјективно-објективној концепцији српског одштетног права, будући да се тешко може очекивати успешност доказивања бола или страха због повреде личног податка. При томе, сама повреда личних података може водити до бројних негативних последица по грађане. Примера ради, незаконитим објављивањем јединственог матичног броја или другог податка на интернету настаје нематеријална штета по лице чији су подаци, без потребе да се утврди и негативна последица због такве објаве.

4.5. Прекршајни поступак у вези са повредом личних података

Прекршај, на основу Закона о прекршајима,[483] представља противправно дело које је законом или другим прописом надлежног органа одређено као прекршај и за које је прописана прекршајна санкција. Дакле, прекршај представља повреду закона која слабије тангира јавне интересе него кривична дела, али опет степен угрожености јавних интереса захтева кажњавање учиниоца прекршаја.

У претходном Закону о заштити података о личности (2008) предвиђено је низ прекршаја за који је прописана новчана казна од 50.000 до 1.000.000 динара за обрађивача или корисника који има својство правног лица.[484] У случају када је

[482] Zdravko Petrović, *Naknada nematerijalne štete zbog povrede fizičkog integriteta*, Sarajevo, 1990, 162.
[483] Закон о прекршајима, *Службени гласник* РС, бр. 65/2013, 13/2016 и 98/2016.
[484] Као радње прекршаја предвиђено је: 1. Обрађивање података без пристанка, 2. Обрађивање података од стране органа власти без пристанка, 3. Прикупљање података од другог лица, 4. Пре прикупљања не упозна лице на које се подаци односе о условима прикупљања, 5. Обрада нарочито осетљивих података на неправилан начин, 6. Пропуштање обавезе чувања интегритета података, 7. Пропуштање издавања копије података у облику у коме се налази информација, 8. Пропуштање брисања података из збирке података, не извршавање решења Повереника, 10. Пропусти обавезу чувања тајне, 11. Пропуштање предузимања мера, пропуштање образовања евиденције, односно пропуштање ажурирања евиденције, 12. Пропуштање обавештења Повереника о намери успостављања збирке података, 13. Пропуштање достављања Поверенику евиденције односно промене у збирци података, 15. Изношење података из Републике Србије на незаконит начин, 16. Пропуштање поступања по налозима Повереника, 17. Спречавање овлашћеног лица у вршењу надзора. Чл. 57, Закона о заштити података о личности (2008).

прекршај извршен у вези са радом органа управе, за штетну радњу одговарало је одговорно лице у државном органу, органу територијалне аутономије или јединице локалне самоуправе. За ова лица предвиђена је блажа казна, у односу на остала лица, будући да је распон казне био предвиђен у износу од 5.000 до 50.000 динара.

Нови Закон о заштити података о личности (2018) такође предвиђа новчано кажњавање у случају прекршаја руковаоца или обрађивача података. Међутим, овај закон предвиђа знатно више прекршајних дела у односу на претходни.[485] Такође, осим повећања броја радњи прекршаја, повећана је и максимална казна на износ од 2.000.000,00 динара, када прекршај изврши правно лице.

Као прекршај предвиђена је повреда скоро сваке законске одредбе која представља одређену обавезу руковаоца или обрађивача података.[486] Као

[485] Слична је ситуација и у праву ЕУ, где су предвиђене корективне мере у циљу кажњавања руковалаца и обрађивача за прекршај, односно повреду одредби Опште уредбе ЕУ. P. Voigt, A. Bussche (2017), 208.

[486] То су ситуације када руковалац или обрађивач, односно орган управе:

1) обрађује податке о личности супротно начелима обраде,
2) обрађује податке о личности у друге сврхе, супротно закону,
3) јасно не издвоји податке о личности који су засновани на чињеничном стању од података о личности који су засновани на личној оцени,
4) ако коришћењем разумних мера не обезбеди да се нетачни, непотпуни и неажурни подаци о личности не преносе, односно да не буду доступни,
5) обрађује податке о личности без сагласности лица на које се подаци односе, а није у могућности да предочи да је лице на које се подаци односе дало пристанак за обраду својих података,
6) обрађује посебне врсте података о личности супротно закону,
7) обрађује податке о личности у вези са кривичним пресудама, кажњивим делима и мерама безбедности супротно закону,
8) лицу на које се подаци односе не пружи одговарајуће информације о подацима које се на то лице односе,
9) лицу на које се подаци односе не стави на располагање или не пружи информације када обраду врше надлежни органи у посебне сврхе,
10) не пружи тражене информације, не омогући приступ подацима, односно ако не достави копију података које обрађује,
11) ограничи делимично или у целини право на приступ подацима лицу на које се подаци односе,
12) не исправи нетачне податке или не допуни непотпуне податке,
13) не избрише податке лица на које се подаци односе без одлагања у законом предвиђеним случајевима,
14) не ограничи обраду података о личности у случајевима предвиђеним законом,
15) не избрише податке када закон то налаже,
16) не обавести примаоца у вези са исправком, брисањем и ограничењем обраде,
17) не информише лице на које се подаци односе о одлуци о одбијању исправљања, брисања, односно ограничавања обраде, као и о разлогу за одбијање,
18) не прекине са обрадом података након што је лице поднело приговор,
19) се донесе одлука која производи правне последице по лице на које се подаци односе искључиво на основу аутоматизоване обраде,

прекршај је предвиђен велики број радњи које покривају готово све законске обавезе руковаоца и обрађивача у вези са обрадом личних података. На овај начин повећава се степен правне сигурности, јер непоштовање законских одредби може да доведе до новчане санкције.

Закон о заштити података о личности (2018), попут претходног закона у овој области, предвиђа релативно благе казне за одговорна лица у органима управе. Уколико прекршај учини одговорно лице у државном органу, органу територијалне аутономије или јединице локалне самоуправе, казниће се новчаном казном од 5.000 до 150.000 динара. Сматрамо да су предвиђене казне благе у односу на значај објекта који се штити, будући да последице повреде личних података могу бити далекосежне. Наравно, осим новчане казне, треба узети у обзир и дисциплинске мере против одговорних лица у органима управе.

4.6. Судска пракса у вези са заштитом података о личности

Будући да је Закон о заштити података о личности (2018) скоро усвојен, судска пракса која се базира на овом пропису још није развијена. На основу претходног закона судови су само у одређеним сегментима пружали заштиту личним подацима. Тако, судску заштиту пружали су прекршајни судови, Управни суд и Уставни суд. Ипак, судске одлуке у овој материји су важне, јер делују *erga omnes*, штите јавни интерес и на тај начин усмеравају будућу праксу органа

20) приликом одређивања начина обраде, као и у току обраде не предузме одговарајуће техничке, организационе и кадровске мере,
21) се однос између заједничких руковаоца не уреди одговарајући законом предвиђен начин,
22) повери обраду података о личности обрађивачу,
23) се подаци обрађују без налога или супротно налогу руковаоца
24) не обавести Повереника о повреди безбедности података,
25) не обавести лице на које се подаци односе о повреди безбедности података,
26) не изврши процену утицаја на заштиту безбедности података,
27) не обавести Повереника, односно не затражи мишљење Повереника пре започињања радње обраде у законом предвиђеним ситуацијама,
28) не одреди лице за заштиту података о личности када је то обавезно,
29) не изврши своје обавезе према лицу за заштиту података о личности,
30) се пренос података о личности у друге земље и међународне организације врши супротно одредбама закона о преносу података,
31) не обезбеди примену ефективних механизама поверљивог пријављивања случајева повреде овог закона, обрађује податке о личности у сврхе архивирања у јавном интересу, у сврхе научног или историјског истраживања или у статистичке сврхе супротно закону. Вид. Чл. 95, Закона о заштити података о личности (2018).

управе у поступању са личним подацима. Сматрамо да би пракса по новом Закону о заштити података о личности (2018) требало додатно да побољша степен заштите личних података који пружају органи управе. Истраживање је обухватило важније одлуке које су пронађене у досадашњој пракси судова.

4.6.1. Пракса прекршајних судова у материји личних података

Пресуда због давања личних података неовлашћеном лицу

У пракси Прекршајног суда у Београду посебно је занимљива осуђујућа пресуда изречена Градском саобраћајном предузећу (ГСП),[487] као органу управе. Такође, осуђујућа пресуда донета је против генералног и извршног директора организационе јединице овог предузећа, као одговорних лица у правном лицу.[488]

Према изреци пресуде, ГСП (као руковалац података), генерални директор (који је пропустио дужност надзора над радом организационе јединице) и извршни директор организационе јединице (као непосредно одговорно лице) криви су јер су вршили обраду личних података супротно одредби чл. 12. Закона о заштити података о личности (2008). Ова лица су управљајући централом за саобраћајни погон, која обавља организацију трамвајског саобраћаја, дозволили и омогућили директору једног приватног правног лица, да добије снимак из трамваја који је саобраћао на линији број 13. у Београду.

На снимку се види петоро младих људи који су се возили трамвајем, од којих је један ишчупао електронски валидатор за очитавање картица за превоз, а поред њега је јасно видљив лик лица које је седело иза поменуте групе. Суд је пронашао да ГСП није имао сагласност за обраду података лица која су на снимку, нити је имао правни основ да уступи спорни снимак приватном правном лицу. Уз то, суд је нашао да није било места за изузетке у виду могућности снимања без дозволе, на основу члана 12. Закона о заштити података о личности.[489]

---

[487] Градско саобраћајно предузеће представља јавно комунално предузеће, што га сврстава у опсег органа управе. У даљем тексту уместо Градско саобраћајно предузеће биће коришћена скраћеница ГСП.

[488] Пресуда Прекршајног суда у Београду бр. 89 Пр. бр. 120316/12 од 29.01.2014. године.

[489] Диспозитив Пресуде Прекршајног суда у Београду бр. 89 Пр. бр. 120316/12 од 29.01.2014. године, 2.

На овај начин, учињен је прекршај из члана 57, став 1, тачка 3.- прикупљање података од другог лица супротно условима Закона о заштити података о личности.[490] Због тога, ГСП је обавезан да плати казну од 50.000,00 динара, док су одговорна лица, генерални директор и извршни директор организационе јединице осуђени на новчану казну у износу од 5.000,00 динара, уз обавезу плаћања трошкова прекршајног поступка. Блажа казна је изречена будући да су одговорна лица у правном лицу поступала из нехата, те су у својој одбрани истакли да разумеју последица поступка који су учинили, као и да им је жао због таквог поступка. Навели су и да је ово први случај ове врсте, због тога што само нови трамвајии имају видео надзор, као и да нису знали коме могу да учине податке доступним, а којим лицима не могу то да учине.

Ова пресуда сведочи о томе да се лични подаци који се налазе у поседу органа управе, не смеју чинити доступним неовлашћеним лицима. За свако уступање личних података грађана мора постојати одговарајући законски основ, а одговорност за бригу о законитом и правилном поступању са подацима лежи управо на одговорним лицима органа управе. Будући да је видео надзором утврђено да су одређена лица учинила штету безобзирним понашањем, њихова одговорност треба да буде утврђена у прекршајном или кривичном поступку. Међутим, то не оправдава повреду њихових личних података омогућавањем приступа неовлашћеним лицима.

Такође, ова пресуда говори о томе да код одговорних лица у органима управе није у потпуности развијена свест о важности информационо-комуникационих технологија и значају личних података. Нове технологије и системи надзора задиру директно у права грађана, те је важно да одговорна лица воде бригу да њихова приватност не буде угрожена поступцима запослених у органима управе. Због тога, ова пресуда развија свест о томе да електронска јавна управа директно производи последице у животу грађана, те да њене предности

[490] Закон прописује да се подаци прикупљају од лица на које се односе и од органа управе који су законом овлашћени за њихово прикупљање. Такође, подаци се могу прикупљати и од других лица у посебно предвиђеним случајевима, а то су: ако је то предвиђено уговором са лицем на који се подаци односе, ако је то прописано законом, ако је те неопходно с обзиром на природу посла,ако се то чини рад задовољавања нарочито важних животних интереса. Вид. чл. 14 Закона о заштити података о личности (2018).

носе и додатну одговорност запослених у органима управе, посебно у вези са заштитом личних података.

Пресуда због одавања нарочито осетљивих података

У пракси Прекршајног суда налазимо још примера осуђујућих пресуда због прекршаја у вези са личним подацима. Поменуто је да се лични подаци могу поделити у неколико категорија. Једна од најзначајнијих категорија тиче се осетљивих личних података, који уживају посебну заштиту. Ипак, повреда осетљивих личних података не представља сама по себи тежи прекршај, већ се припадност овој категорији узима у обзир приликом одређивања врсте казне. На овај начин нарочито осетљиви подаци не добијају онај степен значаја који би требали да уживају због њихове посебне природе и важне улоге.

У пракси судова повреда нарочито осетљивих података није представљала основ за строжије кажњавање учиниоца. У том смислу, индикативна је осуђујућа пресуда запосленом у Дому Здравља „Вождовац“, као лицу запосленом у јавној служби.[491] У овом случају, запослени је у просторијама Дома здравља „Вождовац“, супротно одредбама чланова 16-18 Закона о заштити података о личности (2008) обрађивао нарочито осетљиве податке грађана. Нарочито осетљиви подаци односили су се на чланство у синдикату 115 запослених у Дому здравља „Вождовац“. Такође, подаци су садржали личне матичне бројеве запослених и износ новца којим им је одбијен од плате, у висини месечног чланства у синдикату. Осуђени је нарочито осетљиве податке достављао електронским путем на једну електронску адресу, чиме је грубо повредио право личности запослених, али и регулативу у вези са обрадом личних података.

У своју одбрану, осуђени је истакао да је то учињено случајно, у вршењу свакодневних послова који се обављају у здравственој установи. Будући да у свом раду доста користи електронске начине комуникације, осуђени је навео да је предметног дана послао пуно електронских писама и да је, између осталог, наведене податке случајно доставио на погрешну адресу. У својој одбрани осуђени је обезбедио списак од 62 запослена која су дали изјаву да не сматрају да

[491] Пресуда Прекршајног суда у Београду бр. 46 Пр. бр. 35401/11, од 30.12.2011. године.

им је повређено било какво материјално или лично право. Уз то, у своју одбрану је истакао незгодну материјалну и породичну ситуацију и то да не постоје никакве мере заштите и упозорења који би представљали сигнал да крши прописе и нечија права.[492]

На основу изведених доказа суд је закључио да постоји одговорност, па га је обавезао на плаћање новчане казне у износу од 15.000,00 динара, уз обавезу да надокнади трошкове прекршајног поступка. У образложењу, суд је навео да је приликом одлуке о висини новчане казне ценио све околности, а посебно да је окривљени допринео утврђивању материјалне истине, да је прекршај учинио из нехата, као и да се окривљени налази у незгодном материјалном стању. Због тога, суд је оценио да новчани износ од 15.000 динара представља адекватну казну и да ће утицати да убудуће не дође до сличне ситуације и понављања прекршаја.

Опомена због повреде личних података

Прекршајни суд у Београду изрицао је и опомене због повреде личних података.[493] У једном случају суд је утврдио да је прекршај учинио запослени у Министарству рударства и енергетике. Запослени је у периоду од новембра 2009. године, па до новембра 2011. године, пропустио да предузме мере да се образују збирке личних података и да се о њима води евиденција. Такође, пропустио је да се Повереник за информације од јавног значаја и заштиту података о личности обавести о предузетим активностима по питању евиденција.

У поменутом случају није изречена новчана казна, већ само опомена, због тога што је Министарство рударства и енергетике истог дана када је вршен надзор Повереника, поводом чије иницијативе је и покренут овај прекршајни поступак, унело у Централни регистар три збирке података и евиденција и исте доставило Поверенику. На основу тога, суд је закључио да се може поуздано очекивати да ће Министарство и опоменуто службено лице убудуће поступати у складу са својим законским обавезама и обавештавати Повереника о збиркама и евиденцијама.

[492] Пресуда Прекршајног суда у Београду бр. 46 Пр. бр. 35401/11, 2-3.
[493] Пресуда Прекршајног суда у Београду, бр. 41 Пр. бр. 78121/10, од 27.09.2011. године.

4.6.2. Пракса Вишег суда у материји заштите података о личности

Да овлашћена лица која управљају са личним подацима некада и намерно пропусте да примене норме које уређују област личних података, сведочи пресуда Вишег суда у Београду о прихватању споразума о признању кривичног дела неовлашћеног прикупљања личних података из 2015. године.[494]

У овом предмету Виши суд је утврдио да је шеф техничке службе Факултета за специјалну едукацију и рехабилитацију у урачунљивом стању, свестан забране свог дела, у више наврата, неовлашћено саопштавао податке једној аустралијској агенцији из Мелбурна, за потребе вођења поступка пред аустралијском судом. Подаци су биле личне природе и односили су се на име, презиме, имена родитеља, годину и датум рођења, податке о студијима студената. Ово дело је учињено путем електронске поште и средствима за преношење података (УСБ меморија). Пренос је извршен без сагласности лица чији су подаци коришћени.

Окривљени је био свестан последица свог дела и прихватио споразум о признању кривице, на основу кога је осуђен на условну осуду од 6. месеци затвора и роком проверавања од 1. године, уз обавезу да надокнади трошкове кривичног поступка. У конкретном случају, јавни тужилац и суд имали су у виду све чињенице конкретном случаја, па су прихватили споразум о признању кривице и условну осуду, будући да лични подаци нису коришћени у недозвољене сврхе, већ за потребе судског поступка у Аустралији.

Ипак, условна осуда од 6 месеци затвора сведочи о томе да је важно поштовати прописе који уређују област личних података, јер њихово непоштовање може резултирати и казном затвора, због значаја приватних и јавних интереса који се овим прописима штите. Ово је један од показатеља квалитетног функционисања правосуђа у области заштите података и адекватне процене чињеничног стања конкретног случаја, када су учињене теже повреде личних података.

[494] Пресуда Вишег суда у Београду бр. К. По3-10/13-СПК-153/15 од 25.05.2015. године.

4.6.3. Пракса Управног суда у области заштите података о личности

У одређеним ситуацијама, органи управе ће сматрати да Повереник није правилно одлучивао, па да сходно томе не треба поступити по његовим налозима. У таквим ситуацијама, незадовољна страна има право да поднесе тужбу Управном суду, са циљем побијања решења Повереника, као и захтевом за одлагање извршења решења, уколико постоје оправдани разлози.

Пресуда у вези са налогом Повереника за отклањањем повреде личних података у вези са личним документима грађана

У једном од случајева,[495] јавно комунално предузеће за јавне гараже и паркиралишта „Паркинг сервис“ из Београда, поднело је тужбу Управном суду којом је тражено да се поништи решење Повереника за информације од јавног значаја и заштиту података о личности. Нападнутом пресудом, Повереник је наложио тужиоцу да отклони неправилности у обради личних података и да не тражи фотокопије личних карата и саобраћајних дозвола подносиоцима захтева, већ само да узима документа на увид. Уз то, Повереник је својим решењем наложио и да се униште све копије личних карата и саобраћајних дозвола које се чувају код тужиоца. Тужбом је тражено од суда да донесе привремену меру којом ће обуставити од извршење нападнуто решење Повереника.

Након разматрања списа предмета и чињеничних елемената случаја, Управни суд је нашао да је оваква захтев тужиоца неоснован. Наиме, да би Управни суд могао да одложи извршење, неопходно је да би се његовим извршењем нанела штета тужиоцу која би се тешко могла надокнадити, а да одлагање није противно јавном интересу нити да би се одлагањем нанела већа или ненадокнадива штета противној странци. Управни суд је нашао да се такви услови нису стекли и да се јавни интерес у овом случају остварује извршењем Повереникових мера. На овај начин, имплицитно, суд је показао да је важно примењивати и извршавати одлуке Повереника, будући да он представља орган који брани и штити првенствено јавни интерес, односно интерес грађана чији су подаци у конкретном случају били угрожени.

[495] Решење Управног суда у Београду, бр. 21 У.10163/11 од 20.10.2011 године.

Пресуда којом се одбацује тужба против Повереника због недостатака у тужби

У пракси проналазимо и случајеве у којима је одбачена тужба против Повереника, због тога што из тужбе није могло са сигурношћу да се утврди да ли се покреће управни спор због ћутања управе или због поништаја коначног управног акта. Како тужилац није прецизно означио предмет спора ни у остављеном додатном року, Управни суд је закључио да тужба садржи недостатке који спречавају рад суда по њој, па је тужбу одбацио.[496]

Пресуда у вези са вођењем јавних евиденција по службеној дужности и захтевом за брисање података из таквих евиденција

Управни суд одлучивао је и по тужбама грађана у вези са брисањем података о личности. У једном случају, тужбом је побијано решење Повереника којом је одбио жалбу на одлуку садржане у акту Епархије Пожаревачко-Браничевске из Пожаревца, којом је одбијен захтев тужиоца за брисање података о личности у Матичној књизи крштених цркве Огњене Марије у Мливи, јер би то било фалсификовање историјских података.[497] Тужилац је захтевао брисање података о чињеници крштења, будући да су подаци прикупљени без пуноважног пристанка његових родитеља. Тужени је навео да су подаци прикупљени на основу сагласности родитеља, па нема услова за брисање. Такође, будући да је чињеница крштења непроменљива, она се не може обрисати из Матичне књиге крштених, тако да се прикаже да лице никада није крштено, будући да чињеница опозива пристанка на обраду има дејство само за убудуће.

Управни суд је на основу јавне расправе и утврђеног чињеничног стања закључио да нису испуњени услову за брисање личних података тужиоца из Матичне књиге крштених. Суд је закључио да се у конкретном случају не ради о накнадно прикупљеним подацима, већ о чињеницама које су уписане у званичну евиденцију, па због тога подаци не могу бити брисани.

У овој пресуди, изложено је и значајно становиште које се може применити и на званичне евиденције које се установљавају законом, а воде их органи управе. „По налажењу суда, могуће је тражити брисање тог податка од

[496] Решење Управног суда, одељење у Новом Саду, бр. III-4 У. 7906/11, од 14.10.2011. године.
[497] Пресуда Управног суда у Београду, бр. 9 У 1581/12 од 18.05.2012. године.

сваког другог ко га користи, али не и од онога ко га је први пут евидентирао у евиденцији коју води у складу са прописима, а на основу утврђених чињеница".[498] Дакле, подаци који су уписани у званичне евиденције које се установљавају и воде законом не могу се брисати на основу захтева за брисање, будући да се њима штити јавни интерес.

На основу наведеног суд је закључио да је Повереник у конкретном случају правилно поступио, будући да је епископ наложио Управи црквене општине да обустави даљу обраду тужиочевих личних података, па није било места за реаговање Повереника, што значи да није било повреде закона на штету тужиоца.

4.6.4. Пракса Уставног суда у материји личних података

Уставни суд представља самосталан и независан државни орган који штити уставност и законитост, као и људска и мањинска права и слободе. Поменуте функције Уставни суд врши тако што, између осталог, доноси одлуке о сагласности појединих законских одредаба са Уставом. На тај начин суд спречава да постану пуноважне одредбе закона које нису у сагласности са Уставом.

Оцена уставности Закона о Војнобезбедносној и Војнообавештајној агенцији у вези са личним подацима

У пракси Уставног суда има случајева у којима је суд оцењивао да ли су одређене законске одредбе у складу са зајамченим људским правима и слободама. Таква процена вршена је на заједничку иницијативу Повереника за информације од јавног значаја и заштиту података о личности и Заштитника грађана, а у вези са одредбама којима се крши право на поштовање приватности и право на безбедност личних података.

Иницијатива се односила на одредбе Закона о Војнобезбедносној агенцији и Војнообавештајној агенцији, којима је предвиђена могућност да на основу налога директора Војнобезбедносне агенције или лица које он овласти, путем тајног електронског надзора, прикупљају подаци о телекомуникационом саобраћају и локацији корисника, без увида у њихов садржај. Такође, оспорена је

[498] Пресуда Управног суда у Београду, бр. 9 У 1581/12 од 18.05.2012. године, 4.

одредба истог закона којом је прописано да Војнобезбедносна агенција има право да од телекомуникационих оператера тражи и добије информације о корисницима њихових услуга, самостално и без било какве улоге суда.

Повереник је сматрао да се овим одредбама крши право на приватност, односно право тајности писама и других средстава комуникације, који се могу контролисати искључиво на основу судске одлуке. Предлагачи су предложили да Уставни суд обустави од извршења све појединачне акте и радње које су предузете на основу поменутих одредаба.[499]

Уставни суд је ценећи све чињеничне елементе конкретног случаја пронашао да поменуте одредбе Закона о Војнобезбедносној агенцији и Војнообавештајној агенцији нису у складу са Уставом. Суд је имао у виду системску позицију закона чије се одредбе испитују, одредбе Закона о електронским комуникацијама и дотадашњу судску праску Европског суда за људска права.[500] Како се у образложењу наводи „по оцени Суда, произлази да прописане мере тајног електронског надзора телекомуникација и информационих система ради прикупљања података о телекомуникационом саобраћају и локацији корисника, чак и без увида у њихов садржај, нарушавају неповредивост права на приватност преписке, односно тајности средстава комуницирања корисника комуникационих мрежа, с обзиром на то да надлежне службе безбедности те мере могу вршити без претходно прибављене одлуке суда, која управо треба да представља облик контроле и неопходну брану свакој могућој злоупотреби овлашћења од стране управних власти, због чега оспорена одредба Закона није у сагласности са Уставом“.[501] Суд је пронашао да Војнобезбедносна агенција, као орган управе, нема ексклузивно право на приступ информацијама од

[499] Одлука Уставног суда, бр. ИУз-1218/2010, од 24.05.2012. год.
[500] Уставни суд је у својој одлуци навео неколико пресуда Европског суда за људска права (*Одлука Klass и други против Немачке*, од 6. септембра 1978 године, *Malone против Уједињеног Краљевства* од 2. 08.1984. и *Copland против Уједињеног Краљевства* од 03.04.2007 године). Из ових одлука, суд је извукао одређене сентенце које су важне за одлучивање у конкретној ствари. Тако, наведени су ставови да је пресретање телефонских комуникација, коме прибегне неки орган јавне власти, облик мешања у право на поштовање нечије преписке, да законска овлашћења органима јавне власти да тајно пресрећу комуникације већ самом чињеницом свог постојања могу се схватити као „претња“ за право приватности, итд. Вид. Одлуку Уставног суда, бр. ИУз-1218/2010, 6.
[501] *Ibid*., 7.

телекомуникационих оператора без одговарајућег правног основа, односно судске одлуке.

Ова одлука Уставног суда важна је за поштовање права приватности у ери електронске јавне управе. Органи управе попут Војнообавештајне и Војнобезбедносне агенције, без обзира на то што обављају изузетно важне послове заштите безбедности и очувања јавног поретка, не могу вршити незаконит уплив у приватност грађана. То се односи посебно на преписку и комуникацију, као важне компоненте приватности. На тај начин, грађани се штите од арбитрерног поступања органа управе, будући да је за приступ личним средствима комуникације неопходна одговарајућа одлука суда, као независног органа.

Оцена уставности Закона о заштити података о личности по иницијативи Повереника

Једна од значајнијих иницијатива Повереника у вези са личним подацима грађана, односила се на одређене одредбе Закона о заштити података о личности.[502] Повереник, као подносилац иницијативе, сматрао је да одредбе Закона који се тичу изузетака у погледу услова за обраду података прекорачују границе које поставља Устав. Изузеци предвиђају да обрада података није дозвољена ако физичко лице чији се подаци обрађују није дало пристанак за обраду, односно ако се обрада врши без законског овлашћења. Међутим, Законом је прописано да се правни основ проширује ван уставних граница, односно да основ за обраду података може бити не само закон, већ и акт ниже правне снаге, односно подзаконски акт (конкретна формулација је прописивала да је обрада без пристанка дозвољена „у другим случајевима одређеним овим законом или другим прописом донетим у складу са овим законом“).

У својој одлуци, Суд је пошао од тога да је одредбама члана 42. Устава зајамчена заштита података о личности која представља једно од новијих права заштите приватности, па следи да се прикупљање, држање, обрада и коришћење података о личности могу уредити искључиво законом. Због тога, Уставни суд је донео одлуку о неуставности одредбе која омогућава обраду личних података без

[502] Одлука Уставног суда, бр. ИУз-41/2010, од 06.07.2012. год.

пристанака на основу правног акта нижег од закона. То се посебно односи на органе јавне управе који могу једино на основу закона, али не и на основу других прописа ниже правне снаге да обрађују личне податке без пристанка, независно од тога да ли је таква обрада неопходна за обављања послова из њихове надлежности.[503]

Ово је једна од најважнијих одлука на којима треба да се темељи систем заштите личних података грађана. Важно је имати на уму, посебно у вези са обрадама личних података које врше органи управе, да се обрада без сагласности може вршити искључиво на основу закона. Сви други нижи правни акти, било општи, било посебни не представљају ваљан основ за обраду без пристанка. Са овом праксом треба да буду упознати и грађани, како би били у могућности да заштите своја права, када се обрада података врши без њиховог пристанка.

Ова одлука Уставног суда је од великог значаја, будући да нови Закон о заштити података о личности (2018) прописује могућност обраде без пристанка, али не помиње да се то може предузети искључиво на основу закона. У члану који се односи на ограничења обраде прописано је да се права и обавезе „могу ограничити ако та ограничења не задиру у суштину основних права и слобода и ако то представља неопходну и сразмерну меру у демократском друштву“.[504]

У овој одредби недостаје формулација „на основу закона“, чиме је доведено у питање уставност одредбе, посебно што се у односу на исто питање Уставни суд већ изјашњавао. Остаје да се види да ли ће Уставни суд поново реаговати на исти начин у новом случају, и на тај начин остварити предвидљивост и законитост обрада без пристанка, као значајног елемента заштите личних података.

[503] Одлука Уставног суда, бр. ІУз-41/2010, 5.
[504] Вид. чл. 40, ст. 1, Закона о заштити података о личности (2018)

5. СУДСКА ЗАШТИТА ЛИЧНИХ ПОДАТАКА У ПРАВНОМ СИСТЕМУ ЕУ

Судска заштита личних података заузима важно место у Општој уредби ЕУ. Уредба предвиђа да повреда личних података може довести до настанка штете, па је због тога од изузетног значаја могућност да се све штетне последице исправе, односно накнаде. На значај овог питања указује се и у Преамбули Уредбе, у којој се наводи да „повреда података о личности, ако се не решава на одговарајући начин и благовремено, може да проузрокује физичку, материјалну и нематеријалну штету за физичка лица, као што су губитак контроле над њиховим подацима о личности или ограничавање њихових права, дискриминација, крађа идентитета или превара, финансијски губици, неовлашћени обрнути поступак псеудонимизације, нарушавање угледа, губитак поверљивости података и личности заштићених пословном тајном или другу значајну економску или друштвену штету за то физичко лице“.[505]

Имајући на уму претходно речено, руковалац и обрађивач су дужни да надокнаде сву штету коју грађани претрпе због повреде правила Уредбе. Значајно накнаду штете у вези са повредом личних података је и принцип по коме појам штете треба тумачити у ширем смислу, при чему мора да се има у виду пракса Суда правде ЕУ. На тај начин указано је на значај личних података и потребу да им се пружи посебна заштита у оквирима одштетног права. Штета мора бити надокнађена у потпуности и на најефикаснији начин.

5.1. Врсте судских поступака у вези са заштитом личних података у ЕУ

Уредба познаје три врсте судских поступака у вези са повредом личних података. Поступци се односе на повреду људских права у вези са личним подацима, накнаду штете и за изрицање административних казни. Разлика између поступака учињена је у односу на предмет судског поступка и сврху ради које се поступак покреће.

У случају повреде неких од људских права прописаних Општом уредбом ЕУ, грађани ЕУ имају право на (делотворно) правно средство. Под делотворним правним средством подразумева се тужба надлежном суду државе чланице у којој

[505] Тач. 85, Премабуле, Опште уредбе ЕУ.

руковалац или обрађивач имају седиште, када је повреду учинио орган управе.[506] Право ЕУ регулише и правила у вези са привременим обустављањем поступка, када је у истом предмету покренут поступак у две или више држава чланица. У том случају, судови код којих је накнадно покренут поступак, привремено ће обуставити поступке у том предмету, док први суд не донесе одлуку у односу на конкретан предмет спора.

Друга врста судске заштите тиче се права на накнаду штете због повреде личних података. Опште је правило да свако лице које претрпи неки облик штете (материјалну или нематеријалну) због неправилне примене правила Уредбе, има право да тражи накнаду. Накнада се може тражити од руковаоца или обрађивача. Да би искључили своју одговорност, руковалац и обрађивач треба да докажу да ни на који начин нису одговорни за догађај који је проузроковао штету, што значи да не сме постојати узрочна веза између руковаоца и обрађивача и последице, односно штете. За штету коју причине органи јавне власти у вези са личним подацима, надлежни су судови држава чланица у којима се налази седиште органа управе.[507] У односу на сва друга материјална и процесна питања у вези са накнадом штете, примењује се одштетно право државе чланице.

Трећа врста судске заштите односи се на поступке изрицања административних казни за повреду правила Уредбе. Предност у изрицању административних новчаних казни има надзорно тело државе чланице. Ипак, уколико правни систем неке од држава чланица не познаје концепт административних новчаних казни, поступак изрицања казни одвијаће се пред надлежним судом. У сваком случају, обавеза је држава чланица да пропишу санкције које су делотворне као и административне новчане казне. Уредба предвиђа драстичне казне за непоштовање њених правила. Казне могу ићи до износа од 20.000.000 ЕУР-а, или до 4% укупног годишњег промета у свету за претходну финансијску годину. Ипак, та правила важе када су руковаоци и обрађивачи лица приватног права.[508]

[506] У случају када руковалац или обрађивач нису органи јавне управе, предвиђена је алтернативна надлежност између седишта руковаоца или обрађивача и уобичајеног боравишта лица о чијим подацима је реч. Чл. 79, Опште уредбе ЕУ.
[507] Чл. 82, Опште уредбе ЕУ.
[508] Чл. 83, ст. 6, Опште уредбе ЕУ.

Када су руковаоци или обрађивачи лица органи јавне власти, Уредба оставља простор државама чланицама да саме пропишу правила о томе да ли ће се и на који начин органима јавне управе, односно одговорним лицима у органима управе, изрицати административне новчане санкције. Примера ради, у Хрватској је прописано да у поступцима који се воде против органа јавне власти, неће моћи да се изричу административне новчане санкције за повреде домаћег закона или Опште уредбе ЕУ.[509]

5.2. Судска пракса у вези са Општом уредбом ЕУ

Само пар дана након ступања на снагу Опште уредбе ЕУ, донета је прва судска пресуда на основу овог прописа. Пресуду је донео Регионални суд у Бону (*Bonn*) у Немачкој.[510] Овај случај остаће забележен у историји као први предмет у коме је примењено право заштите личних података предвиђено Општом уредбом ЕУ. Иако случај није уско везан за органе електронске управе, одлука служи као пример праксе за руковаоце и обрађиваче који врше послове јавне управе.

Случај се односио на Интернет корпорацију за додељивање имена и бројева (*Internet Corporation for Assigned Names and Numbers* (*ICANN*)) и на овлашћен регистар за издавање домена у Немачкој (*EPAG Domain services GmbH* (*EPAG*)). Ово тело представља непрофитну организацију одговорну за усклађивање и одржавање многих база података у вези са називима и нумерацијама домена на интернету. Са друге стране, *EPAG* представља правно лице које је добило овлашћено од *ICANN*-а да додељује домене другог нивоа заинтересованим странама.

За сваки додељени домен другог нивоа, *ICANN* захтева од регистратора (који је у овом случају *EPAG*) да прикупи одређене личне податке о лицима са којима је закључен уговор, односно којима су додељени интернет домени. Ти подаци односили су се на име и контакт податке тих лица, као и име и контакт податке лица задуженог за техничку подршку и административне послове код клијента (лица које закључује уговор са регистратором). Ови подаци су доступни

[509] Вид. чл. 47, Zakona o provedbi Opće uredbe o zaštiti podataka Hrvatske

[510] Пресуда Регионалног суда у Бону, Немачка, бр. 10 O 171/18, од 29.05.2018. год. Пресуда на немачком језику је доступна на: *https://www.icann.org/de/system/files/files/litigation-icann-v-epag-request-court-order-prelim-injunction-redacted-30may18-de.pdf*, 18. август 2018.

јавности због употребе тзв. *Who is* заштитног протокола који користи *ICANN* за базе података, ради одређивања домена, ИП адреса, и томе слично.

Због ступања на снагу Опште Уредбе ЕУ *EPAG* је одбио да достави податке *ICANN* о подацима техничког и административног особља, будући да ће ти подаци бити доступни јавности, а није постојао правни основ за обраду тих података. *ICANN* је реаговао тужбом пред Регионалним судом у Бону, тражећи да суд нареди *EPAG*-у да достави све тражене податке и да одреди привремену меру достављања података. *ICANN* је тврдио да је неопходно прикупљати и објављивати податке ради превазилажења техничких проблема, а такође и због безбедносних разлога. *EPAG* је у своју одбрану навео да сматра да се сврха прикупљања личних података може постићи и достављањем мањег броја података (само личних и контакт података клијента).

У својој одлуци, Регионални суд у Бону, одбио је тужбени захтев, сматрајући да обрада личних података техничког и административног особља није у складу са чланом 5, ставом 1, тачкама б и ц, Опште Уредбе ЕУ.[511] Укратко, суд је сматрао да су лични подаци прикупљени од клијената довољни за вршење конкретних обрада, будући да постоји једно одговорно лице за коришћење домена, те да нису неопходни лични подаци техничког и административног особља.

Важност ове одлуке огледа се не само у томе што је она прва која је донета на основу Опште уредбе ЕУ, већ и због тога што представља путоказ другим судовима на који начин треба да сагледавају опште принципе, као што је случај са „коришћењем најмањег могућег обима података".

Такође у Немачкој, први пут је постављено питање накнаде нематеријалне штете по одредбама Опште уредбе ЕУ.[512] У случају који се нашао пред Окружним судом Диез (*Diez*), тужилац је захтевао накнаду нематеријалне штете у износу од

[511] Чл. 5, ст. 1, Опште уредбе ЕУ наводи да подаци прикупљени у одређене, изричите и законске сврхе не смеју да се обрађују на начин који није у складу са тим сврхама (тач. б) и то обрада података мора да буде примерена, релевантна и ограничена на оно што је неопходно у сврхе у које се обрађују лични подаци („коришћење најмањег могућег обима података") (тач. ц.).
[512] Вид. Одлуку окружног суда Диез- *Das Amtsgericht Diez (Schlussurteil vom 07.11.18, Aktenzeichen 8 C 130/18).*

500 евра због добијања електронске пошиљке на своју електронску адресу са захтевом за пристанак за добијање нових електронских пошиљки те фирме.

Будући да је електронска адреса представља податак о личности за чију обраду је неопходан пристанак, тужилац је сматрао да је претрпео нематеријалне штету обрадом без пристанка. У међувремену, тужени је на основу правичности извршио уплату од 50 евра, како би санирао „последице“ које је имао тужилац. Суд је стао на становиште да нема места накнади нематеријалне штете у износу од 500 евра, будући да је нематеријална штета надокнађена исплатом коју је извршио тужени у износу од 50 евра.

Ова исплата покренула је дилему да ли у случају повреде личних података у електронском окружењу и коришћења електронских адреса без пристанка, руковалац, односно обрађивач могу да се „искупе“ исплатом износа од 50 евра. Сматрамо да на овај начин није установљена пракса за накнаде нематеријалне штете у вези са повредом личних података, већ је неопходно сачекати судске пресуде и ставове надзорних тела држава чланица ЕУ.

6. ОВЛАШЋЕНО ЛИЦЕ ЗА ЗАШТИТУ ЛИЧНИХ ПОДАТАКА У ОРГАНИМА УПРАВЕ

6.1. Правна природа овлашћеног лица за заштиту личних података

Један од значајних новина у систему заштите личних података грађана у поседу органа управе односи се на увођење посебног механизма заштите у облику овлашћеног лица задуженог за заштиту података.[513] Овај институт није постојао у претходним законима, већ је уведен Законом о заштити података о личности (2018). Када орган управе наступа у својству руковаоца или обрађивача података, односно уколико обрађује личне податке грађана, дужан је да одреди лице за заштиту података. Са друге стране, оваква обавеза, осим у посебним случајевима, не постоји за руковаоце и обрађиваче у сфери приватног права.

[513] У том смислу, ванвременске су и за нове области индикативне речи Stuarta Wolk-a и William Luddy-a, који наводе да „Старе правне доктрине не могу једноставно да се примене на нову технологију…Неопходне су нове концепције које се морају развијати, уз пажљиво прилагођавање старих- нови путеви правног резоновања постепено се јављају упоредно са новим законодавством и новом праксом“. Stuart Wolk, William Luddy, *Legal Aspects of Computer Use*, Engelwood Cliffs, New York 1986, 6., нав. према: С. Лилић (1989), 224, фн. 60.

Ради ефикасности и заједничког обављања послова, више органа управе може одредити једно лице које ће се старати о процедурама, пословима и актима у вези са обрадама личних података грађана. Ипак, како би ово лице могло квалитетно да обавља свој посао, приликом одређивања заједничког представника, мора се имати у виду величина органа и количина података који органи обрађују.

Обављање функције лица задуженог за заштиту података представља захтевну улогу, која подразумева стално стручно усавршавање. Овлашћено лице мора константо да води бригу о различитим аспектима обрада и личним подацима. Природа посла коју обавља ово лице не може се класификовати као стриктно правна, инжењерска или менаџерска. Ова позиција захтева разумевање основних процеса обраде података, познавање фундаменталних правних питања заштите података и разумевање функционисања организационог систем органа.[514] Због тога, лице за заштиту података умногоме олакшава вођење рачуна о безбедности податка, законито одвијање пословних обавеза и омогућава растерећивање запослених у органима управе, који у оквиру својих делатности, између осталог, рукују личним подацима. На основу изложеног, овлашћено лице сврставамо у посебан механизам заштите личних података.

Приликом одређивања лица задуженог за заштиту личних података, руководилац органа мора да води рачуна о личним и стручним квалификацијама кандидата. Кандидат мора поседовати посебно стручно знање и искуство у вези са заштитом личних података. Такође, оно мора имати карактер и интегритет, као личне квалитете, како не би дошло до компромитовања позиције и самог органа.

Са кандидатом који испуњава наведене услове руководилац органа закључује уговор. Тај уговор по својој природи може бити уговор о раду, уговор о делу или уговор о обављању привремених и повремених послова. Законодавац је оставио слободу органима да сами нађу најадекватнији начин сарадње лица и органа. За лице задужено за заштиту података може бити именовано лице у оквиру организационе структуре органа или лице изван структуре запослених.

[514] Упор. A. Diligneski, D. Prlja, D. Cerović (2018), 191.

Када одреди лице задужено за личне податке, руководилац органа о томе обавештава Повереника. Обавештавање служи ради сачињавања евиденције о лицима задуженим за заштиту података у оквиру различитих органа, које води Повереник.

6.2. Позиција овлашћеног лица за заштиту личних података у оквиру органа управе

Како би лице задужено за заштиту података могло да успешно обавља своју функцију, неопходно је да буде упознато са свим сегментима обраде података унутар органа. Руководилац органа има дужност да „уведе“ овлашћено лице у све послове и процедуре које се односе на обраду личних података унутар органа. То се чини благовремено, на начин који у потпуности омогућава све предуслове за обављање посла. Омогућавање обављања посла односи се на пружање неопходних средстава за рад, материјалних и организационих, као и на омогућавање приступа базама података и информацијама о обрадама.

Имајући у виду непрестан развој информационо-комуникационих технологија од изузетног је значаја да се овлашћено лице константно професионално усавршава. Једино на тај начин може се остварити пун потенцијал институције, тако да је спремно да одговори свакодневним изазовима по безбедност личних података. Стручно усавршавање овлашћених лица подстичу и помажу руководећа лица у органима.

Од значаја за успешно и законито обављање улоге овлашћеног лица јесте његова у оквиру органа управе. Овлашћено лице треба да ужива независан статус који му омогућава објективан приступ процени процеса у вези са личним подацима. То је посебно тешко остварити у органима управе, будући да је организациона структура запослених у овим органима постављена хијерархијски,[515] како би лакше и делотворније обављала послове из своје надлежности.[516] Независност подразумева да овлашћено лице самостално обавља послове и контролише поступке и радње запослених у вези са личним подацима. Даље, то значи да руководилац органа не може дисциплински кажњавати

[515] У оквиру хијерархијске структуре посебно се истиче дужност службеника да извршава наређења претпостављеног старешине у границама закона. Вид. С. Лилић (2013), 182.
[516] Упор. Лазо Костић, *Административно право Краљевине Југославије I*, Београд 1933, 310.

овлашћено лице или раскинути са њим сарадњу само због извршења законских обавеза овог лица, односно непоступања по (погрешном) налогу руководиоца.

То значи да независност није потпуна, управо због организационе структуре органа управе. За извршење послова у оквиру своје надлежности овлашћено лице одговара руководиоцу органа. У организационој шеми органа, овлашћено лице треба да буде самостално, тако да има само једног непосредно надређеног и то руководиоца органа.

Другачије позиционирање овог лица у организационој шеми утицало би на његову независност. Непосредна одговорност значи да руководилац мора да води рачуна о независности овлашћеног лица, али и о томе да ово лице не дође у сукоб интереса приликом извршавања својих обавеза. Забрана сукоба интереса усмерена је на то да се очува објективност. Таква забрана повезана је и са обавезом овлашћеног лица да као професионалну тајну чува све податке са којим се сусретне у вршењу своје делатности. Сматрамо да се ова обавеза не гаси ни престанком ангажовања у органу управе, већ мора трајати неограничено, будући да се једино на тај начин може очувати интегритет и поверљивост података.

6.3. Дужности овлашћеног лица за заштиту личних података

Основна дужност овлашћеног лица унутар органа управе односи се на праћење усклађености пословања са прописима који уређују област заштите личних података и пружање мишљења о стању безбедности података у оквирима органа. У том процесу улога овлашћеног лица је више саветодавна и превентивна, будући да оно нема овлашћена да предузима конкретне мере ради усклађивања пословања и поступања са законским и другим прописа.

Иако је овлашћено лице непосредно одговорно руководиоцу, оно има дужност да обавештава и даје стручна мишљења свим запосленима о законским обавезама које се односе на безбедност личних података. Због тога, оно је дужно да „прати примену одредби закона и интерних прописа руковаоца или обрађивача, који се односе на заштиту података о личности, укључујући и питања поделе одговорности, подизања свести и обуке запослених који учествују у радњама

обраде и контроле“.[517] То значи да је овлашћено лице дужно да развија свест о важности података у оквиру органа и да помаже запосленима у едукативном и професионалном усавршавању у материји личних података. Још једна од његових обавеза односи се на давање мишљења у вези са проценом утицаја одређене обраде, у случајевима када се употребљавају нове технологије за обраду или када природа обраде и података то захтева.

У вршењу својих обавеза, овлашћено лице мора свеобухватно да посматра процесе обраде података, при чему мора узети у обзир техничка, правна и организациона питања, како би његова мишљења била потпуна и адекватна. Такође, овлашћено лице представља и референтну особу за контакт у односима органа управе и Повереника. Остваривање комуникације која се односи и на обавештавање и прибављање мишљења у вези са проценама ризика и другим питањима од значаја за личне податке између Повереника и органа одвија се преко овог лица.

Дакле, дужности овлашћених лица односе се превасходно на давање мишљења, развијање свести и усмеравање ка правилним начинима обраде личних података. Ипак, законодавац је оставио широк простор код уређивања обавеза овог лица, будући да горе наведене дужности представљају „најмању обавезу“. То оставља простор да овлашћено лице добије од руковаоца или обрађивача и друге послове који могу носити више одговорности, у смислу предузимања мера безбедности по личне податке.

Сматрамо да то није добро решење, будући да се може доћи у ситуацију да овлашћена лица у различитим органима управе, имају различит степен одговорности и другачије послове. То се може одразити на управну и судску праксу, јер може доћи до дискрепанце између обавеза предвиђених прописима, интерним актима и уговорима о запослењу лица задуженог за заштиту података у оквиру различитих органа управе, па ће бити тешко створити конзистентну праксу у вези са дужностима, овлашћењима и степену одговорности ових лица. Због тога, овлашћена лица би требала да врше само дужности предвиђене законом.

[517] Чл. 58, ст. 1, тач. 2, Закона о заштити података о личности (2018).

6.4. Овлашћена лица у органима управе задужена за заштиту података у правном систему ЕУ

Право ЕУ такође предвиђа посебну позицију лица задуженог за заштиту података унутар органа јавне власти. Именовање таквог лица није представљало обавезу у правном систему ЕУ пре ступања на снагу Опште уредбе ЕУ, будући да Директива 95/46 није предвиђала обавезност именовања лица овлашћеног за заштиту података. Ипак, у пракси су се јављали случајевима у којима су приватне фирме именовале лице које се бави заштитом података.[518]

У Општој уредби ЕУ ово лице се означава као овлашћено лице за заштиту података. Органи јавне власти држава чланица имају дужност да именују овлашћено лице када врше обраду личних података грађана, било као руковаоци, било као обрађивачи. Појам органа јавне власти цениће се према унутрашњем праву држава чланица, али свакако обухвата државну управу и имаоце јавних овлашћења. Имајући у виду организациону структуру, обим и значај података, органи јавне власти могу именовати једно овлашћено лице за више органа. У том случају мора се обезбедити да овлашћено лице буде једнако укључено у процесе обраде свих организација, при чему се строго мора водити рачуна о принципу независности и поверљивости информација.

Да би лице могло бити одређено за овлашћено лице за заштиту података, оно мора поседовати стручна знања и професионалне способности које се односе на област заштите података.[519] То лице мора имати знања о европским и националним прописима из ове области, али мора имати и искуство у практичном раду са личним подацима.

За разлику од права Србије, право ЕУ омогућава само два правна облика сарадње органа и овлашћеног лица. Овлашћено лице може да буде неко од запослених у органу или треће лице које није запослено у органу, са којим се закључује уговор о делу (право Србије дозвољава било који облик уговорног односа са овлашћеним лицем). Радно место и контакт подаци овог лица морају

[518] Article 29 Data Protection Working Party, Guidelines on Data Protection Officers (‘DPOs’), 16/EN WP 243 rev.01, Brussels, 2016, 4.
[519] Erne Mraznica, „GDPR – Novi izazov zaštite podataka o ličnosti“, časopis *Bankarstvo* vol. 46, br. 4, (ur. Veroljub Dugalić), Udruženje banaka Srbije, Beograd 2017, 172.

бити транспарентни, што се остварује објављивањем података на интернет презентацији и достављањем тих информација надзорном органу државе чланице.

Примера ради, Пошта Хрватске је именовала свог „службеника за заштиту особних података“ и на свом сајту навела пропис по коме је овлашћено лице именовано, орган који је именовано то лице (одлука Управе Поште Хрватске), његов број у регистру, адресу и електронску пошту.[520]

Овлашћено лице мора да буде независно од било каквог утицаја запослених и руководилаца у оквиру органа, али и од трећих лица.[521] Ради остваривања независности, руководилац органа код кога овлашћено лице обавља функцију, мора да обезбеди финансијска и материјална средства за рад, али и одговарајуће радне услове који омогућавају приступ обрадама и личним подацима које поседује орган. Радна група која је радила на изради Опште уредбе ЕУ сматра да организација мора да обезбеди овлашћеном лицу континуирани приступ састанцима средњем и високог менаџмента (руководилаца органа), присутност код доношења одлука које се тичу личних података и брзо обавештавање код проблема и инцидената у вези са безбедношћу података.[522]

Задаци овлашћеног лица за заштиту података уређени су на истоветан начин као и у праву Србије. Лице овлашћено за заштиту података има дужност да пружа информације и даје савете запосленима и руководству руковаоца и обрађивача у вези са поштовањем и применом прописа који уређују област заштите података. Такође, овлашћено лице мора да води рачуна о прописима ЕУ и о прописима државе чланице, јер једино на тај начин може да дође до потпуне усклађености пословања.

Осим што даје савете и информације, овлашћено лице има обавезу да прати усклађеност унутрашњих поступака органа са прописима државе чланице и ЕУ. Праћење усклађености односи се и на поделу одговорности унутар органа, развијање свести и стручно оспособљавање и усавршавање запослених у вези са обрадом личних података. То значи да овлашћено лице мора континуирано да врши анализе, испитује начин опхођења у односу на права грађана у вези са

[520] Вид. Hrvatska pošta, Službenik za zaštitu osobnih podataka, *https://www.posta.hr/sluzbenik-za-zastitu-osobnih-podataka/5607*, 23. новембар 2018.
[521] P. Lambert (2018), 462.
[522] Article 29 Data Protection Working Party (2016), 13-14.

личним подацима и да прати стање информационог система у вези са личним подацима.

Значајан део обавеза овлашћеног лица тиче се одржавања сарадње са надзорним органом, ради преузимања примера добре праксе и стицања нових знања која су неопходна за обављање ове дужности. Такође, овлашћено лице је референтна контакт особа за сарадњу са надзорним органом, у случају претходних консултација или других спорних питања у вези са обрадом.[523] У обављању свих наведених дужности, овлашћено лице мора водити рачуна о природи, обиму, околностима и сврси обраде личних података грађана.[524]

[523] P. Lambert (2018), 461.
[524] Чл. 39, Опште уредбе ЕУ.

VII ИНФОРМАЦИОНА БЕЗБЕДНОСТ И ЗАШТИТА ЛИЧНИХ ПОДАТАКА У ЕЛЕКТРОНСКОЈ ЈАВНОЈ УПРАВИ

1. УВОДНА РАЗМАТРАЊА О ИНФОРМАЦИОНОЈ БЕЗБЕДНОСТИ

Систем заштите података у електронској јавној управи састоји се од низа мера и механизама које је неопходно применити како би подаци заштићени. Приликом одређивања конкретних мера мора се имати у виду зависност друштвених и пословних процеса од употребе информационо-комуникационих технологија. То значи да заштита личних података мора обухватати и техничке мере заштите. Такође, у формирању система незаобилазна су и питања организационог карактера, будући да органи управе представљају организације са великим бројем запослених, те је неопходно одредити и дефинисати улогу запослених у односу на личне податке грађана. На послетку, сва ова питања морају да буду заокружена правним нормама које на општи начин уређују систем заштите. Стога, техничке и организационе мере представљају део система правне заштите личних података.

Информациона безбедност обухвата све активности „које обезбеђују заштиту информација са циљем да буде омогућен континуитет у раду и минимизиран утицај ризика и претњи по информациони систем…Она подразумева заштиту поверљивости, интегритета и доступности података од неауторизованог приступа, промене или уништења, уз примену контролних механизама који треба да буду унапред одређени, уграђени, надгледани, проверавани и побољшани у реалном времену.“[525]

Иако постоји тесна веза између безбедности информација и заштите личних података, ова два појма се теоријски и практично разликују. Наиме, заштита података је усмерена ка појединцима и заштити њихове приватности, односно заштити њихових личних података. Са друге стране, појам безбедности информација односи се на мере којима се остварује заштита свих информација и података у оквиру неког система (органа управе или фирме). Безбедност информација чине техничке и организационе мере чији је непосредни циљ

[525] Данијела Протић, „Информациона безбедност: стандарди или правила“, *Војно дело*, пролеће/2013, Београд 2013, 135.

заштита информација, а посредни, заштита јавног интереса, интегритета и имовине органа, итд.

Дакле, систем безбедности информација односи се и на личне податке грађана који су похрањени у оквирима организације. Зато се и наводи да „свака промена целовитости или садржаја битних информација може да утиче на кредибилитет организације или изазове последице које могу привремено или трајно да зауставе њен рад. Због тога, елиминација или смањење потенцијалног ризика на минимум и квалитетна организација информационог система, обезбеђују добар основ за борбу против људских и системских грешака или малициозних напада споља“.[526]

Веза између информационе безбедности и заштите података односи на ограничење приступа информацијама и подацима, криптографију, псеудонимизацију и употребу других мера којима се штите информације и лични подаци у оквиру информационих система електронске јавне управе. То суштински значи да се мерама информационе безбедности пружа заштита и личним подацима грађана у поседу органа управе.

Како би систем безбедности информација био примењен једнако у различитим органима и како би се пружио исти степен заштите свим подацима, неопходно је правно уредити основне елементе система информационе безбедности. Уређењем основа система информационе безбедности омогућава се употреба јединствених стандарда заштите и повећава степен заштите личних података.

[526] Д. Протић, (2013), 133.

2. ИНФОРМАЦИОНА БЕЗБЕДНОСТ У ПРАВНОМ СИСТЕМУ РЕПУБЛИКЕ СРБИЈЕ

2.1. Систем информационе безбедности Србије

Правни документи ретко када у потпуности уређују организационе и техничке мере које руковаоци треба да примене у циљу заштите података. Разлог томе лежи у непрестаном усавршавању информационих система и ограничености правних норми. Такође, појављивање нових ризика захтева константно усавршавање одбрамбених механизама.[527] Због тога је неадекватно стриктно уредити одбрамбене механизме, будући да могу брзо да застаре, па пропис треба изнова мењати.

Због тога, важно је предвидети основне принципе и темеље на којима се заснива систем информационе безбедности. У Србији, основе заштите од безбедносних изазова и ризика у информационо-комуникационим системима и надлежност органа за спровођење мера заштите предвиђа Закон о информационој безбедности.[528] Ово је кровни закон у области информационе безбедности чије основе и уређује, док су поједина питања уређена другим општим актима.[529]

2.2. Основна начела информационе безбедности

Систем информационе безбедности у Србији темељи се на четири основна начела. То су начело управљања ризицима, начело свеобухватности заштите, начело стручности и добре праксе и начело свести и оспособљености.

Начело управљања ризицима значи да се сваки одбрамбени механизам заснива на анализи ризика и процени последица које могу настати по информациони систем. Како би се установила заштита, неопходно је анализирати чињенице и изазове који се појављују у пракси и на основу тих елемената

[527] „Опасности које представљају претњу пословним информационим системима и његовим објектима, посредно или непосредно, континуирано или повремено, у мањој или већој мери, толико су бројне и међусобно повезане да над целим информационим системом формирају крајње комплексну мрежу опасности“. Nikola Dragović, Mirjana Žilović, Nikola Bošković, „Definisanje adekvatnih mera u funkciji zaštite poslovnih informacionih sistema“, *Zbornik radova naučno – stručnog skupa sa međunarodnim učešćem „Informacione tehnologije, obrazovanje i preduzetništvo*“, (ur. Alempije Veljović), Fakultet tehničkih nauka u Čačku, Čačak 2017, 381.

[528] Закон о информационој безбедности, *Службени гласник* РС, бр. 6/2016, 94/2017.

[529] За више вид. Irina Rizmal, Vladimir Radunović, Đorđe Krivokapić, *Vodič kroz informacionu bezbednost u Republici Srbiji*, Centar za Atlanske studije i Misija OEBS-a u Srbiji, Beograd 2016, 33-36.

утврдити ризик и предвидети адекватну заштиту. Начело свеобухватности заштите значи да одбрамбени систем тежи да обухвати различите аспекте информационих система и да на тај начин пружи свеобухватну заштиту. То значи да није довољно предвидети само техничке мере, већ треба водити рачуна о кадровским и организационим аспектима заштите. Начело стручности и добре праксе стварају претпоставке да се систем штити квалитетним мерама које су се у пракси доказале као успешне. Начело свести и оспособљености подразумева да сва лица која учествују у активностима у вези са информационим системима морају да буду свесна ризика и непрестано да се усавршавају ради успешног превазилажења истих.[530]

2.3. Улога оператора и безбедносне мере

Информационо-комуникациони системи којима се користе органи управе представљају системе од посебног значаја, због обима и важности посла који обављају. У системе од посебног значаја сврставамо и оне системе који служе за обраду осетљивих података, независно од тога да ли обраду врши орган јавне власти или приватно лице. Посебна заштита значи да њихови оператери старају о примени одговарајућих мера које ће спречити настанак инцидената, злоупотреба и других штетних радњи по систем. Оператери могу поверити трећим лицима старање о безбедности информационих система од посебног значаја, али у том случају морају закључити уговор који ће обезбеђивати правилну примену законских одредби.[531] Сматрамо да овај уговор треба да садржи и клаузуле о поверљивости информација до којих се дође у одржавању система.

Оператор система доноси акт о безбедности система који садржи мере заштите и начине одржавања његове безбедности. Мере које оператор може применити ради повећања безбедности система могу бити техничке, организационе или кадровске природе. У техничке мере можемо сврстати

[530] Чл. 3, Закона о информационој безбедности.

[531] Уколико овај уговор закључује оператор информационих система јавне управе, сматрамо да је у том случају реч о јавно-приватном партнерству. У овом случају сматрамо да је од изузетне важности установити строги систем одговорности за повреде законских и уговорних одредби, будући да бригу о систему у области јавног права води лице приватног права. Такође, сматрамо да поменута одредба није адекватна јер не оставља гаранције безбедности и отвара питање „цурења“ информација из јавног сектора.

остваривање безбедности рада на даљину и употребе мобилних уређаја, употребу крипто заштите, заштиту носача података, ограничење приступа подацима и средствима обраде, обезбеђење интегритета рачунарских програма, мере које осигуравају континуитет у ванредним околностима. Као организационе мере предвиђене су мере успостављања организационе структуре са утврђеним пословима и одговорностима запослених, заштиту објеката, простора и просторија у којима се налазе средства информационих система и подаци који се користе у њиховом раду, мере брзог реаговања на безбедносне инциденте. Постоји и неколико кадровских мера попут подизања стручности лица која управљају информационим системима, усавршавања и унапређивања знања лица која су задужена за послове информационе безбедности, итд.[532] Поменуте мере своје пуно дејство остварују једино у интеракцији и заједничком комбиновању, будући да се тако може пружити заштита целокупном информационом систему.

2.4. Органи управе значајни за систем информационе безбедности

Посебно је значајна обавеза оператора информационо-комуникационих система да обавесте министарство надлежно за послове информационе безбедности,[533] у случају напада или угрожавања система. Уколико су инцидентом обухваћени и подаци о личности грађана, оператор ће обавестити и Повереника. Ове дужности обезбеђују транспарентност рада и укључивање важнијих државних фактора у области личних података и информационе безбедности.

Без обавештавања Повереника и надлежног министарства, изостала би узајамна акција, што би узајамност и спрегу система информационе безбедности и система безбедности личних података чинило нестабилним. Остаје да се види на који начин ће поменути органи одговорити у случајевима инцидената, будући да се пракса у овим ситуацијама још није установила.

---

[532] Чл. 7, Закона о информационој безбедности. Такође, за више о организационим и кадровским елементима заштите вид. Драган Ануцојић, *Заштита информационих система и података*, Прометеј, Нови Сад 2008, 101-155.

[533] У Србији, за послове информационе безбедности надлежно је Министарство трговине, туризма и телекомуникација које је образовало посебно тело за координацију послова информационе безбедности, *http://mtt.gov.rs/vesti/obrazovano-telo-za-koordinaciju-poslova-informacione-bezbednosti/*, 22. фебруар 2019.

Важан шраф информационе безбедности представља Национални центар за превенцију безбедносних ризика у информационо комуникационим системима (Регулаторна агенција за електронске комуникације и поштанске услуге) чији је основни циљ да координише мере заштите на националном нивоу. Национални центар има обавезу да прати стање у области информационе безбедности, да води евиденције посебних система, да пружа упозорења и развија свест о важности успостављања адекватне информационе безбедности. Такође, овај орган израђује анализе ризика и инцидената, како би се формирали примери добре праксе у предвиђању мера заштите.[534] Осим националног центра, за органе јавне управе значајан је и Центар за безбедност информационо-комуникационих система у републичким органима, који обавља истоветне послове као и национални центар, једино на нивоу државних органа.

Контролу поштовања основних елемената заштите врши Инспекција за информациону безбедност, на основу прописа којима се уређује инспекцијски надзор. У обављању својих делатности инспектор за информациону безбедност може наложити отклањање утврђених неправилности и забранити коришћење поступака и техничких средстава којима се угрожава или нарушава информациона безбедност.[535] Закон предвиђа и значајне новчане казне за правно лице и одговорно лице у правном лицу за непоштовање одредаба тог закона.

3. МЕРЕ ИНФОРМАЦИОНЕ БЕЗБЕДНОСТИ КОЈЕ СЕ ОДНОСЕ НА СИСТЕМ ЗАШТИТЕ ЛИЧНИХ ПОДАТАКА У СРБИЈИ

Систем информационе безбедности пружа заштиту и личним подацима грађана који се чувају и обрађују у дигиталном облику. Ипак, систем заштите личних података подразумева посебне мере, па се ова два система не могу поистоветити, иако постоје одређене сличности. Због тога истраживање ће пажњу усмерити на оне мере информационе безбедности које су усмерене на заштиту личних података.

Претходни Закон о заштити личних података (2008) предвиђао је да су руковалац и обрађивач дужни да предузму техничке, кадровске и организационе

[534] Чл. 15, Закона о информационој безбедности.
[535] Чл. 29, Закона о информационој безбедности.

мере, у складу са утврђеним стандардима и поступцима, а које су потребне да би се лични подаци заштитили од губитака, уништења, недопуштеног приступа, промене, објављивања и сваке друге злоупотребе, као и да утврде обавезу лица која су запослена на обради да чувају тајност података.[536] Тадашњи систем заштите указивао је на значај различитих врста мера у стварању система заштите података, али нису предвиђали конкретне начине примене, већ једино дужност усаглашености пословања са „утврђеним стандардима и поступцима".

Закон о заштити података о личности (2018) посветио је већу пажњу мерама информационе безбедности. Ради заштите личних података грађана, органи управе морају применити адекватне техничке, организационе и кадровске мере. Приликом одређивања мера које ће се применити у обради, органи управе морају обратити пажњу на два елемента. Први се тиче стања информационе технологије и трошкова примене таквих технологија. Други се односи на природу, обим, околности и сврху обраде података, као и вероватноћу ризика по безбедности система, као и права и интересе лица чији се подаци обрађују.

То значи да органи управе не морају увек применити најновије и најскупље технологије у процесу формирања система безбедности личних података. Они имају дужност да процене све чињенице случаја, односно елементе обраде и да у складу са значајем обраде процене која ће се технологија применити у конкретном случају. На тај начин, узимају се у обзир не само интереси грађана чији се подаци обрађују, већ и јавни интерес који се осликава кроз нормално одвијање друштвених токова.

Уколико би органи управе били суочени са обавезом примене најсавременијих технологија у сваком појединачном случају, трошкови обраде би били несразмерно велики у односу на сврху обраде и значај заштићеног добра. То би водило избегавању примене закона, али и онемогућавању нормалне обраде података у великом броју случајева, будући да се предвиђени стандарди не би могли остварити.

Закон о заштити података о личности (2018) наводи неколико конкретних мера заштите безбедности података. Ове мере органи управе треба да примене

[536] Чл. 47, ст. 2, Закона о заштит података о личности (2008).

према околностима конкретног случаја, уз посебно обраћање пажње на ризике обраде. Те мере подразумевају:

1. Псеудонимизацију и крипто заштиту података о личности,
2. Способност обезбеђивања трајне поверљивости, интегритета, расположивости и отпорности система и услуга обраде,
3. Обезбеђивање успостављања поновне расположивости и приступа подацима о личности у случају физичких или техничких инцидената у најкраћем року,
4. Поступак редовног тестирања, оцењивања и процењивања делотворности техничких, организационих и кадровских мера безбедности обраде.[537]

Ове мере не представљају обавезу за органе управе, али о њима мора да се води рачуна приликом обраде података. То значи да орган неће одговарати уколико није предузео одређену меру, али је обавезан да пружи разлоге због којих мере нису примењене. Употреба ових мера не искључује могућност примене осталих безбедносних мера које су руковаоци и обрађивачи применили у свом информационом систему.

3.1. Класификација мера информационе безбедности у вези са личним подацима

Мере информационе безбедности у области заштите података могу се класификовати у три основне категорије. То су техничке, организационе и кадровске мере. У пракси, ове мере су испреплетане и повезане па се најбољи резултати у пракси постижу њиховом заједничком употребом. Будући да је истраживање усмерено на правну регулативу у вези са заштитом личних података, анализа ће обухватити само значајнија питања у вези са мерама које је неопходно увести у информациони систем ради постизања квалитетне заштите личних података грађана.

[537] Чл. 50, ст. 2, Закона о заштити података о личности (2018). На исти начин су конкретизоване и мере за заштиту безбедности података у праву ЕУ. A. Diligenski, D. Prlja, D. Cerović (2018), 155.

3.2. Техничке мере безбедности у вези са заштитом личних података

3.2.1. Псеудонимизација

Псеудонимизација представља техничку меру обраде података чијом применом се лични подаци више не могу приписати одређеном лицу без употребе додатних информација, уз услов да се додатне информације чувају одвојено и да се на њих примењују мере које спречавају да се податак може приписати одређеном или одредивом лицу.[538]

Овом техничком мером омогућава се чување анонимности и задржавање приватног карактера личних података након њихове обраде. Коришћењем ове мере, подаци се не могу повезати са одређеним лицем. Ради лакшег разумевања, псеудонимизацију ћемо показати на примеру реченице са личним подацима. Пример: Марко Марковић, рођен 1. априла 1970. године у Београду. У односу на личне податке у овој реченици, псеудонимизација може бити извршена на два начина. Први је да уместо имена и презимена Марко Марковић стоји М. М., односно његови иницијали. Други начин је да се уместо личног имена, презимена и датума рођена постави одређена шифра попут неповезаних бројева и слова (НО300) чиме се додатно смањује могућност сазнавања псеудонимизираног податка. Као што се може приметити, псеудонимизација се заснива на измени личних података тако да се они не могу распознати, осим уколико руковалац обраде поседује информацију о псеудониму којим је лични податак измењен.

3.2.2. Анонимизација

Осим псеудонимизације, као мера заштите може се јавити и анонимизација.[539] Основна разлика између псеудонимизације и анонимизације је у томе што када се лични подаци анонимизирају, они више не представљају личне податке, па престаје и потреба за њиховом заштитом.

Анонимизирани су они подаци код којих су сви елементи идентификације уклоњени из збирке личних података и код којих није остао ни један елемент који

[538] Чл. 4, ст. 1, тач. 6, Закона о заштити података о личности (2018).
[539] За више о анонимизацији података у судским одлукама у Републици Србији, вид. Партнери за демократске промене, *Анализа: „Анонимизација података у судским одлукама у Србији- ка усаглашеним правилима и пракси*“ (радна верзија), Београд, 2015.

би се могао користити за поновну идентификацију конкретног лица.[540] То је случај код брисања личних података из база података. Са друге стране, када се лични подаци псеудонимизирају, остаје могућност њиховог коришћења у првобитне сврхе, за шта је потребна информација о псеудониму.

Постоје две најзначајније методе анонимизације које су у основи сличне псеудонимизацији, али се ипак разликују на наведен начин. То су генерализација и шифровање. Уколико за пример узмемо личне податке из реченице Марко Марковић, метода анонимизације путем генерализације довела заменила би Марко Марковић у М. М., само што се брише информација о генерализованом податку тако да се не може сазнати на кога се односе нови подаци. У случају шифрирања информација Марко Марковић била би замењена, на пример, са словима А. А (неповезана са основним иницијалима), при чему се првобитни лични податак на основу кога су настале шифре више не користи.[541]

3.2.3. Енкрипција

Крипто заштита представља важан технички метод који служи сигурности информационог система и личних података. Крипто заштита је позната и као метод енкрипције. Метод енкрипције представља део криптологије која представља науку о шифрама. Она се састоји од криптографије (метода енкрипције који проучава системе чувања информација и њихове безбедне размене) и криптоанализе (метода декрипције који се примењује у циљу „разбијања“ шифри, односно сазнавање правог значаја криптоване информације без кључа).[542] Криптографија представља вештину која проучава процесе чувања информација тако да они буду познати и читљиви само оним лицима којима су намењене. Појам криптографија потиче од грчких речи криптос (κριπτοσ) - тајна и графеин (γραφιεν), што значи писати.[543]

---

[540] Agencija Europske unije za temeljna prava, *Priručnik o europskom zakonodavstvu o zaštiti podataka*, Ured za publikacije EU, Luksemburg 2014, 42.
[541] Упор. Партнери за демократске промене (2015), 14-15.
[542] Даниел Дивјаковић, *Основи криптологије, ОТП и РСА алгоритам*, мастер рад (необјављено), Природно-математички факултет- Департман за математику и информатику, Нови Сад 2016, 14.
[543] Sonja Kuljanski, „Algoritam i njegova praktična primena“, *Vojnotehnički glasnik, br*. 3/10, (ur. Dragana Marković), Ministarstvo odbrane Republike Srbije, Beograd 2010, 65.

Сам метод енкрипције означава процес у коме се разумљива (смислена) порука претвара у неразумљиву поруку или шифру. У систему електронских комуникационо-информационих средстава енкрипција представља алгоритам, односно математичку операцију којом се шифрује право значење одређене поруке. У таквом систему, само онај који шаље информацију и онај који зна шифру (прималац информације), могу знати право значење криптованог текста. Трећа лица која покушају неовлашћено (без кључа) да приступе тексту неће бити у могућности да разумеју стварно значење текста.

Данашња криптологија познаје неколико различитих видова енкрипције (криптографије).[544] Да би криптографија остварила свој примарни задатак, а то је безбедност информација и њиховог преноса, она мора бити усмерена на очување поверљивости поруке.

Када говоримо о органима управе, пожељно би било да се метод енкрипције користи за слање електронске поште, посебно када таква порука садржи личне податке или друге поверљиве информације. Слање криптоване електронске поште омогућава безбедну комуникацију у коме само орган управе и лице коме је порука упућена, знају стварну садржину поруке.

Увођење обавезне енкрипције електронских порука које шаљу органи управе, а које садрже личне податке повећало би степен безбедности информација и створило би веће поверење грађана у електронску управу. Такође, нове електронске методе достављања одлука у управним поступцима захтевају уређивање овог питања интерним актима органа. Због тога, сматрамо да би било целисходно предвидети ову обавезу подзаконским актима који уређују пословање са електронском поштом и начину поступања са подацима у органима управе.

3.2.4. Ризици и могућа решења у вези са информационим системима у јавној управи

Будући да су сви информациони системи производи људског рада, њихова природа није савршена, па увек постоји могућност квара или грешке у одређеном елементу. Грешке и кварови могу бити физичке или техничке природе и могу

[544] За више о видовима енкрипције података вид. Ilija Apostolov, Risto Hristov, „Izbor optimalne tehnike za enkripciju i dekripciju podataka“, *Informacione tehnologije- sadašnjost i budućnost*, (ur. Božo Krstajić), Podgorica 2014, 125.

утицати на правилан рад хардвера и софтвера, чиме се угрожава функционисање целог рачунарског система, а тиме и података који се чувају или обрађују у таквом систему. Како информациони системи представљају основно средство преко кога се обавља рад органа електронске управе, грешке се могу јавити и у вези са обрадом личних података грађана.

Зато, опасност од грешака и кварова на рачунарским системима мора бити узета у обзир приликом установљавања целокупне заштите података у електронској управи. Посебно треба обратити пажњу на обезбеђивање способности трајне поверљивости, интегритета, расположивости и отпорности система и услуга обраде, као и могућност успостављања, у што краћем року, поновне расположивости и приступа подацима након физичких и техничких инцидената.[545] У случају квара одређеног сегмента информационог система, долази до могућности прекорачења рокова за органе управе, што може имати негативне последице по права грађана и поштовање закона. Примера ради, „хаковање“ система може блокирати рад органа управе на рачунарима, који не могу приступити базама података и предметима које обрађују.

Како би предупредили штетне последице, органи управе морају извршити детаљну анализу ризика који прете целовитости, доступности и интегритету система и података. Технички посматрано, ризике можемо поделити на две велике групе, према месту настанка могућих последица. У том смислу постоје ризици хардверских компоненти и ризици софтвера.[546]

Ризици прве групе испољавају се у виду грешки и кварова на хардверу. Могу се јавити у односу на све делове хардвера на информатичким уређајима (овде можемо сврстати излазне и улазне уређаје, процесоре, меморије и уређаје за складиштење информација). Такође, ови ризици обухватају и грешке које могу настати на хардверу из спољног извора (неадекватна повезаност са изворима енергије, дотрајалост уређаја и механичка оштећења хардверских компоненти).

---

[545] Чл. 50, ст. 2, тач. 2 и 3., Закона о заштити података о личности (2018).

[546] Одређени аутори врше поделу хардверско-софтверских недостатака на више елемената, па наводе: кварове на информатичким уређајима, техничке грешке инфраструктуре, грешке у контролним или управљачким програмима и грешке у апликативним програмима. Вид. Д. Ануцојић (2008), 41. Наравно, ове поделе су пре свега теоријске природе, док у практичном смислу подразумевају холистички приступ који се заснива на интеракцији више врста ризика и предузимању заједничких мера ради њихове заштите.

Друга врста ризика у односу на информационе системе односи се на програмске, односно софтверске компоненте. У ову групу грешака спадају грешке у контролним или управљачким програмима и грешке у апликативним програмима. Грешка у алгоритму или неповезаност функција доводе до тога да програм није у могућности да обавља своју функцију или није у могућности да је обавља на правилан начин. Ови ризици могу настати као последица грешке унутар самог програма или помоћу људског фактора („хаковање“). Зато је неопходно водити рачуна о квалитету рачунарског програма и начинима његове заштите приликом програма увођења у систем, али и током коришћења програма.

Како би се подаци у поседу органа управе заштитили од поменутих ризика, неопходна је вишестепена заштита. Функционални рачунарски програми подразумевају правилну примену техничких норми, редовну контролу и усавршавање система. Зато је потребно прецизно одредити обавезе лица која уводе и одржавају рачунарске програме у јавној управи.

На пословима одржавања рачунарских система морају радити савесна и стручна лица чије су обавезе детаљно регулисане интерним прописима или уговорима, како би се остварили предвиђени принципи заштите података. Сматрамо да је пожељно интерним и подзаконским прописима предвидети мере које могу превентивно утицати на појаву техничких ризика. У том смислу, може се предвидети прављење копија база података, физичко обезбеђење рачунара од нежељеног спољног утицаја, редовно одржавање и ажурирање рачунарских програма, итд.

Као пример добре праксе заштите од ризика у вези са техничким елементима информационих система наводимо Правилник о чувању, заштити и сигурности података у оквиру информационог система Централног регистра обавезног социјалног осигурања.[547] Овај правилник уређује физичку заштиту података информационог система помоћу две мере безбедности.

Прва мера се односи на стварање безбедносних копија података, како би се спречиле опасности од техничких кварова рачунарских система. Таква заштита се

[547] Правилник о чувању, заштити и сигурности података у оквиру информационог система Централног регистра обавезног социјалног осигурања, *Службени гласник* РС, бр. 29/2013. Овај Правилник је донет на основу чл. 26, став 4, Закона о Централном регистру обавезног социјалног осигурања, *Службени гласник* РС, бр. 30/2010.

остварује стварањем секундарне базе података и секундарног рачунарског система.[548] Секундарна база података и секундарни рачунарски систем представљају копије оригиналних база и система. Стварањем копија обезбеђује се непрекидно функционисање информационог система и побољшава систем заштите података. Копије се не смеју чувати на истом месту где и оригинали, при чему место на коме се налазе копије мора бити адекватно заштићено од спољних ризичних фактора (примера ради од пожара и поплава).[549] Приступ секундарним базама и системима могу имати само овлашћена лица.

Друга мера заштите односи се на одржавање, поправку и повлачење из употребе опреме информационог система. Централни регистар обезбеђује одржавање рачунарске опреме информационог система, а у случају ажурирања или поправљања опреме, неопходно је сачинити безбедносне копије података како би се спречио њихов губитак.[550] Мере оправке и одржавања рачунарског система треба да буду под надзором овлашћеног лица како би подаци о личности остали заштићени. Предвиђене су и мере за случај потпуног повлачења из употребе информационог система. Ту је и обавеза да се сви подаци трајно и сигурно избришу са конкретних уређаја који се повлаче из употребе.[551]

Поменуте мере су превентивне природе. Оне иду за тим да осигурају резервну копију у случају грешке или квара техничких компоненти уређаја за обраду. На овај начин, чак и повлачење информационог система или одређеног рачунара не доводи у питање сигурност и интегритет података. Наравно, од изузетне важности је питање је ко ће контролисати примену мера безбедности. Зато је важно установити систем одговорности овлашћених и надлежних лица, како би предвиђене мере заживеле у пракси.

Треба имати у виду да се одредбе Правилника односе искључиво на информациони систем Централног регистра обавезног социјалног осигурања. Сматрамо да би било адекватно и пожељно да и остали органи управе донесу

[548] Чл. 6. Правилника о чувању, заштити и сигурности података у оквиру информационог система Централног регистра обавезног социјалног осигурања.
[549] Чл. 6., став 3. Правилника о чувању, заштити и сигурности података у оквиру информационог система Централног регистра обавезног социјалног осигурања.
[550] Чл. 7., став 1. Правилника о чувању, заштити и сигурности података у оквиру информационог система Централног регистра обавезног социјалног осигурања.
[551] Чл. 7., став 3. Правилника о чувању, заштити и сигурности података у оквиру информационог система Централног регистра обавезног социјалног осигурања.

правилнике или друге унутрашње акте по угледу на поменути Правилник. Тиме се може очекивати већа сигурност система од различитих ризика у органима управе. Доношењем правилника на нивоу свих органа управе који на сличан начин уређује мере безбедности, остварио би се виши степен безбедности личних података, као и стандарди заштите које предвиђа Закон о заштити података о личности (2018).

3.2.5. Начин чувања података као значајно техничко питање

- Чување личних података у дигиталном облику

Једно од основних питања у вези са техничким мерама заштите личних података тиче се њиховог чувања. Начин чувања података зависи од облика у коме се они налазе. Подаци се могу чувати у материјалном (папирном) облику који се похрањују у архивама органа. Са друге стране, све већа употреба информационо-комуникационих технологија избацује папирне документе из употребе, па се подаци све више чувају у дигиталном облику, на меморијама рачунара, других техничких уређаја за складиштење и у виртуелним базама података, које се користе уз помоћ интернета.

Како се јавна управа састоји од великог броја органа, ради лакше комуникације и бржег приступа подацима, образују се и велики (информациони) центри који се користе као база података у виртуелном облику. У Србији, у Београду је крајем 2017. године отворен први велики центар са подацима под покровитељством Владе Србије и Канцеларије за информационе технологије и електронску управу.[552] У центру су обједињени подаци које чувају сви органи који се налазе у систему јавне управе. На овај начин ствара се централизовано управљање електронским подацима, што олакшава успостављање система безбедности и омогућава контролу приступа, чиме се смањује могућност за преварне радње, неовлашћен приступ и друге злоупотребе. Пракса изградње великих центара у којима ће се чувати подаци у поседу јавне управе биће

[552] Блиц бизнис, Ана Брнабић отворила први државни Data centar, *https://www.blic.rs/biznis/ana-brnabic-otvorila-prvi-drzavni-data-centar-evo-sta-ce-se-sve-u-njemu-nalaziti/9wqwge1,* 05. фебруар 2019.

настављена и наредних година, будући да је предвиђена изградња још једног великог резервног центра у Крагујевцу.

У центрима налази се велики број сервера на којима су похрањени подаци. Ови сервери подржавају „облаке“ (*eng. clouds*),[553] који представљају дигиталне базе података. Ове базе података заснивају се на виртуелним (дигиталним) складишним капацитетима који су повезани рачунарским програмима који дозвољавају приступ овлашћеним лицима. Подацима се може приступити преко интернета и посебних информационо-комуникационих система који захтевају верификацију корисника помоћу шифре или других идентификационих елемената.

Виртуелне базе података дозвољавају похрањивање великог броја различитих података на централну мрежу којој могу приступити овлашћена лица. Тиме се олакшава праћење субјеката, времена и других елемената приступа базама података и преузимање података. То је од посебног значаја за органе управе који имају потребу за приступом подацима у поседу различитих органа, па би прибављање података од сваког појединачно одузимало доста времена. Бележење приступа повећава и степен одговорности за евентуалне повреде личних података.

У центрима се морају применити све техничке и организационе мере ради успостављања безбедности информационог система и личних података, што посебно подразумева континуирано испитивање стабилности и делотворности информационо-техничких мера заштите рачунарских програма.

- *Чување личних података у материјалном облику*

Иако дигитални начин чувања података у поседу органа управе постаје примарни, мора се водити рачуна и о подацима у материјалном (физичком) облику. Грешке у рачунарским програмима или тврдим елементима рачунара и система могу водити трајном губитку података, што може угрозити функционисање органа управе и приватност грађана чији се подаци чувају.

[553] За више о *clouds*-у вид. Preston de Guise, *Data protection – Ensuring Data Availability*, Auerbach Publication, New York 2017, 7-8.

Због тога, као један од могућих начина чувања копија података јесте на магнетним дисковима којима се може лако и брзо приступити. На њима се може похранити велика количина података. Сличну функцију магнетним дисковима, обављају магнетне траке,[554] само у знатно мањој мери. Магнетни диск представља облик трајне меморије са великим складишним могућностима и опцијом за брзим приступом подацима. Дискови се састоје од површинског магнетског слоја, који може меморисати електронске информације и податке. Погон диска уписује и очитава податка са диска и извлачи информације из било ког дела диска изузетно лако и брзи, независно од редоследа снимљених података.[555] Међутим, код ових дискова јавља се опасност од размагнетисања и ризици који прете од других спољних појава, као што је случај са високим температурама или течностима. Због тога, приликом чувања копија података на дисковима мора се водити рачуна о њиховој физичкој безбедности.

Питања физичке заштите копија података и носача на којима се подаци чувају требало би да представља предмет подзаконских аката. Како се у органима управе користе различите врсте рачунарских система и података, адекватно би било донети правилник о поступању са носачима података, јер се једино на тај начин може спречити остваривање ризика.

Важно питање у вези са безбедношћу копија јесте брисање података са носача. Наиме, шта се дешава када се јави потреба за њиховим избацивањем из употребе (зато што су дискови дотрајали или постоји потреба за изменом носача због мањка меморије) и потребно их је заменити? На таквим носачима и дисковима увек може остати податак који је поверљив или који не би смео да буде доступан јавности.

У циљу решавања таквих проблема постоји неколико могућности. Прва, да се постојећи подаци на диску измене, односно препишу новим и небитним садржајем. Друго, да се изврши контакт електромагнета и диска прелажењем магнета преко плоча диска, како се садржају носача не би могло никако

[554] Код магнетних трака, подаци се снимају и репродукују са слоја намагнетисаних честица на пластичном носачу – траци. Магнетна трака може ускладиштити велику количину података, међутим приступ тим подацима је знатно успорен, те се данас обично користе као алтернативна опција или опција за сачињавање безбедносних копија. Milan Milosavljević, Mladen Veinović, Gojko Grubor, *Informatika*, Univerzitet Singidunum, Beograd 2009, 93.
[555] *Ibid*.

приступити. Трећа опција је физичко уништење магнетног диска, које се може извршити на различите начине (спаљивање диска, потапање у киселине или течности, итд.).[556]

Ово питање није уређено законским и подзаконским прописима на јединствен начин. Због тога, потребно је прописати правила о руковању са дотрајалим и неупотребљивим носачима података, на нивоу свих органа управе. На тај начин ће заштита података бити квалитетнија и потпунија.

3.3. Кадровске мере у вези са заштитом личних података

Један од важних елемената информационе безбедности, а тиме и система заштите података односи се на кадровске мере. Значај тих мера препознаје и Закон о заштити података о личности (2018), сврставајући их у једне од три основних врста мера којима се достиже одговарајући ниво безбедности личних података. Ове мере су од посебног значаја код обраде коју врше органи управе, због сложене и масовне кадровске структуре јавне управе.

Квалитетно обављање послова органа управе, примарно зависи од квалитетног и ваљаног вршења дужности запослених у јавној управи, односно од јавних службеника (у домаћој правној терминологија тренутно постоји искључиво појам државних службеника).[557] Како би јавна управа квалитетно обављала своје дужности и одговарала савременим изазовима са којима се сусрећу грађани, неопходан услов је да се службеници константно усавршавају и развијају своја знања и способности. То посебно долази до изражаја у модерном, информатичком друштву, и будући да се њихови задаци и послови дигитализују и самим тим, усложњавају.

---

[556] Д. Ануцојић (2008), 83.

[557] У позитивном праву Републике Србије не користи се термин јавни службеник. Са друге стране, право Републике Србије познаје термин „државни службеник“. Државни службеник је лице чије се радно место састоји од послова из делокруга органа државне управе, судова, јавних тужилаштава, Републичког јавног правобранилаштва, служби Народне скупштине, председника Републике, Владе, Уставног суда и служби органа чије чланове бира Народна скупштина или са њима повезаних општих правних, информатичких, материјално-финансијских, рачуноводствених и административних послова. Чл. 2. Закона о државним службеницима, *Службени гласник* РС, бр. 79/2005, 64/2007, 116/2008, 104/2009, 99/2014 и 94/2017. У складу са дефиницијом државних службеника, јавни службеници су сва лица која обављају исте делатности као и државни службеници, било да раде у органима државне управе, било у органима недржавне јавне управе.

3.3.1. Усавршавање и оспособљавање јавних службеника у вези са заштитом личних података

Данас више није довољно да јавни службеник познаје искључиво управну материју којом се бави, већ је важно да поседује и додатна знања рада на рачунару како би могао да обавља послове који спадају у надлежност органа управе. Такође, неопходно је да јавни службеници поштују и примењују принципе интегритета и искрености и да поштују грађане.[558]

Због тога, важан елемент развоја електронске јавне управе и заштите података јесте усавршавање и оспособљавање јавних службеника.[559] Усавршавање и оспособљавање јавних службеника огледају се у прикупљању нових знања, информација и начина обављања послова и комуникације са грађанима. Стицање нових стручних знања мора бити континуирано и заступљено на свим нивоима, од најнижих звања до највишег менаџмента. Како обрада личних података грађана и заштита података представљају нове делатности које су од великог значаја за управу и друштво, усавршавање у овим областима треба да буде један од приоритета обука.

У Србији је усвојена Стратегија стручног усавршавања државних службеника,[560] у којој су промовисани општи и посебни циљеви усавршавања. Општи циљ усавршавања тиче се доприноса повећању ефикасности и економичности рада државне управе и њене делотворности у погледу остваривања права и интереса грађана, субјеката привређивања и других носилаца права и обавеза, кроз остваривање услова за континуирано и свеобухватно повећање нивоа компетенција државних службеника.[561] Конкретни начини остваривања циљева из Стратегије су предвиђени Уредбом о стручном усавршавању државних службеника.

---

[558] Rodney Erakovich, Dragoljub Kavran, Sherman Wyman, „Public administration and ethics training strategy“ , *Legal life*, 9/2003, Belgrade 2003, 907.

[559] Детаљно о усавршавању и оспособљавању државних службеника у Добросав Миловановић, Јован Ничић, Марко Давинић, *Стручно усавршавање државних службеника у Републици Србији*, Удружење за јавну управу, Београд 2011.

[560] Стратегија стручног усавршавања државних службеника у Републици Србији, *Службени гласник* РС, бр. 56/2011 и 51/2013. Ова Стратегија испитује досадашње стање ствари у правном оквиру и пракси, анализирања упоредна решења и даје смернице и стратешке принципе на којима би требало развијати систем усавршавања државних службеника.

[561] Стратегија стручног усавршавања државних службеника у Републици Србији, 11-12.

Стручно усавршавање је право и дужност државног службеника.[562] Руководилац органа је дужан да државном службенику омогући стручно усавршавање за извршавање послова радног места у складу са програмима стручног усавршавања.[563] Службеник може да се усавршава на различите начине, у зависности од посебних потреба појединог органа, ресурса и стратешке усмерености. Закон о државним службеницима познаје општи програм обуке, програм обуке руководилаца и посебни програми обуке.

Посебну улогу усавршавању има Национална академија за јавну управу. Национална академија за јавну управу представља посебну организацију и централну институцију система стручног усавршавања у јавној управи Србије са статусом јавно признатог организатора активности неформалног образовања одраслих.[564] Ова институција управља развојем начина и методама којима се одржава сталан и флексибилан систем усавршавања службеника јавне управе, у складу са потребама и циљевима тих органа и целокупне јавне управе.

3.3.2. Посебни програми обуке и усавршавања у области заштите личних података

Када говоримо о области заштите података, усавршавање у овој области може бити засновано на посебним програмима обуке. Посебни програми обуке припремају се и спроводе ради стручног усавршавања државних службеника запослених у појединим државним органима, а у складу са специфичним потребама из њиховог делокруга и надлежности, односно потребама везаним за поједина радна места, врсте послова или посебне групе корисника.[565] То значи да област заштите података и уопште начина поступања са личним подацима, представља једну од важних тема посебних програма стручног усавршавања.

Програми посебног стручног усавршавања државних службеника морају се утврдити за сваку годину у односу на специфичне потребе органа, што оцењује и доноси руководилац органа.[566] Будући да су у данашње време изузетно активне промене и иновације у информационо-комуникационим технологијама, а уз то се

[562] Чл. 96, став 1., Закона о државним службеницима.
[563] Чл. 96, став 2., Закона о државним службеницима.
[564] Чл. 3. Закона о Националној академији за јавну управу, *Службени гласник* РС, бр. 94/2017.
[565] Чл. 97г, став 1., Закона о државним службеницима.
[566] Уредба о стручном усавршавању државних службеника, *Службени гласник* РС, бр. 25/2015.

јављају и нови ризици по личне податке, можемо закључити да су посебни програми обуке адекватни за усавршавање у области заштите личних података.

Осим посебних програма, службеници се могу усавршавати и стицати нова знања у форми додатног образовања[567] и усавршавања као што су присуствовање предавањима, тренинзима, семинарима, конференцијама, студијским посетама и другим.[568] У пракси Националне академије повремено се јављају посебни програми стручног усавршавања у вези са управним поступком, инспекцијским надзором, управним споровима, итд. Такође, међу поменутим програмима, област заштите личних података добија на значају.

У том смислу, Национална академија за јавну управу организује обуке у области заштите података о личности. Основни циљ ових обука је да се повећа капацитет државних службеника за примену Закона о заштити података о личности. Обуке су намењена државним службеницима који раде на пословима података о личности.[569] Овакве типове обука треба додатно промовисати и отворити простор за све службенике који раде на пословима у вези са обрадом и заштитом личних података. Зато можемо рећи да усавршавање државних (јавних) службеника доприноси квалитетнијем раду органа управе.

У области личних података то значи правилну и ефикасну примену регулативе у вези са заштитом података. Последично, то води заштити приватности грађана и остварењу њихових права и интереса.

***

Повећањем свести о изазовима у електронској јавној управи и упознавањем са принципима и правима на којима се заснива систем заштите података, грађани ће бити сигурнији у правне могућности у вези са личним подацима. Напомињемо да би било корисно проширити обавезу усавршавања на све запослене у јавној управи, а не искључиво у државној управи, јер како смо навели, јавна управа представља систем повезаних елемената који морају бити у

[567] Д. Миловановић, Ј. Ничић, М. Давинић (2011), 63.
[568] Чл. 97е Закона о државним службеницима.
[569] Служба за управљање кадровима, Пријава на обуке у организацији Националне академије за јавну управу, доступно на: *http://www.suk.gov.rs/sr/strucno_usavrsavanje/obuke_po_temama.dot?id_obuke_oblast=106*, 29. новембар 2018.

складу, што подразумева и државну и недржавну јавну управу. Многи подаци грађана налазе се у поседу недржавних органа којима су поверена јавна овлашћења, па је корисно да и тај део јавне управе води бригу о заштити и тајности података.

3.4. Организационе мере које се односе на заштиту личних података

И поред квалитетних прописа и јасно прописаних правила поступања за запослене, у органима управе јављају се организациони ризици. Организациони ризици тичу се алокације људских ресурса у органима и квалитетно распоређене радне обавеза, дужности и овлашћења јавних службеника. Због тога, организациона питања представљају важан елемент система заштите података.

Односи запослених у органима управе обично су уређени према принципу хијерархије. Овај принцип омогућава квалитетно и ефикасно обављање управних послова, будући гломазни системи, попут јавне управе, захтевају јасну организациону структуру надређених и подређених, брзо деловање и руководиоца који ће усмеравати правац деловања органа и доносити одлуке. Хијерархија значи да се на челу органа налази једно лице (или група лица) које усмерава и води орган и представља га у односу са другим лицима. Запослени који се на хијерархијској лествици налазе испод руководиоца имају дужност да поступају према његовим наредбама и инструкцијама.

Дакле, запослени су према руководиоцу у односу субординације, односно правно организационе подређености. Доношење одлука обично се делегира и лицима које руководилац одреди, за поједину област деловања органа, па се тако хијерархија формира и на „нижим лествицама“ власти унутар органа. На тај начин у оквиру органа настаје неколико пирамидално надређених и подређених односа.

Инструкције и наредбе руководећег морају бити засноване на закону и у складу са околностима случаја. Како једно лице има већу и значајнију улогу на хијерархијској лествици, тако расте и одговорност коју то лице сноси у доношењу својих одлука. У том смислу, руководеће лице органа сноси највећу одговорност за функционисање целог органа.

Управо због хијерархијске организације и односа субординације, важно је да се рад унутар органа одвија према унапред утврђеним правилима и на

предвиђеним пословима. Тако и одређена радна места могу бити формирана само за одређену групу важних послова.

3.4.1. Да ли би требало одредити посебно лице које се стара о личним подацима у органима управе ?

У односу на област заштите података, сматрамо да је добро решење обавеза именовања лица које ће надгледати процес обраде података и старати се о њиховој безбедности. Једино на тај начин могу се ускладити различити послови унутар органа који се односе на личне податке, а који обухватају правне, административне, информатичке и друге врсте послова.

Закон о заштити података о личности (2018) предвиђа овлашћено лице за заштиту личних података које треба да контролише обраде и коришћење личних података у вези са радом органа управе. Одређивањем лица које врши надзор над обрадом и правилношћу примене норми у вези са заштитом личних података, грађани су добили додатну гаранцију сигурности у вези са њиховом приватношћу и личним подацима. Грађани који сматрају да се њихови подаци не користе у законом прописане сврхе или сумњају у правилност обраде, имају на располагању могућност обраћања лицу које је директно упућено у рад органа у вези са личним подацима, што доприноси степену заштите личних података.

3.4.2. Приступ запослених у органима управе личним подацима грађана

Због великог броја запослених у органима управе неопходно је ограничити круг лица која имају приступ личним подацима грађана. Круг треба ограничити на ужи круг запослених којима је приступ неопходан ради решавања конкретног предмета или обављања другог, законом предвиђеног посла. Сваки приступ подацима који није у вези са пословима органа управе је неовлашћен и представља повреду личних података, те због тога приступ треба двоструко ограничити, у односу на овлашћена лица и у односу на разлоге због којих се подацима приступа. Једино се на тај начин може очувати интегритет података и приватност грађана.

У зависности од облика у коме се чувају подаци, приступ може бити ограничен мерама физичког обезбеђења за податке који се налазе у материјалном

облику, односно техничким (рачунарским) мерама када се подаци чувају у дигиталном облику. Ове мере представљају баријере неовлашћеном коришћењу података и приступу од стране неовлашћених лица. То значи да су усмерене ка спречавању злоупотреба и квалитетнијем раду органа управе.

Физичке мере обезбеђења представљају организационо питање које спада у предмет чувања материјалних средстава у оквиру органа управе. Физичко обезбеђење, картица за улазак у посебне просторије, записници о приступу, само су неке од мера које се могу обезбедити.

Од већег значаја за органе управе јесу техничке мере које се успостављају за приступ базама података у дигиталном облику. Постоје две основне техничке мере. То су идентификација и верификација. Оне су међусобно повезане и представљају дигиталне методе „препознавања“ корисника. Метафорички речено, идентификација и верификација представљају дигитални кључ за улазак рачунарске базе података. Идентификацијом се врши препознавање корисника од стране рачунарског система. Корисник пружа одређене улазне информације и податке који морају бити препознати од стране рачунара (система) како би корисник добио приступ. Овај процес је стандардизован и врши се на основу истих улазних параметара које уноси овлашћени корисник. Методом верификације, корисник потврђује да је баш он то лице које тражи приступ. Уношењем података који су познати само кориснику и систему, програм допушта овлашћеном лицу да приступи електронској бази података.

Поменуте методе могу контролисати субјекте који приступају подацима, као и разлоге због којих се приступа одређеној бази података. Рачунарски програм поседују могућност чување информација о месту и времену приступа подацима, што је од изузетног значаја за целокупни систем заштите личних података и систем информационе безбедности. Информација о лицу, времену и разлогу приступа мора бити позната лицима чији се подаци користе. На тај начин се омогућава да лице чији се подаци користе буде упознато са обрадом његових личних података. Такође, остварује се већа повезаност управе и грађана и до изражаја долази начело транспарентности.

3.5. Контрола квалитета прописа и примењених мера у вези са личним подацима

Сматрамо да контрола квалитета прописа представља посебан начин заштите личних података у органима управе, јер „регулатива лошег квалитета је скупа за друштво и ограничава привредни раст“.[570] Ову меру посредно предвиђа и Закон о заштити података о личности (2018) који наводи да је један од начина заштите информационог система редовно тестирање, оцењивање и процењивање делотворности организационих и кадровских мера безбедности и обраде.

Посматрано из правне перспективе, потребно је пратити начине и квалитет примене прописа (како закона, тако и подзаконских аката) у материји заштите личних података, будући да се информационо-комуникационе технологије константно развијају. Њихов развој подстиче и стварање нових изазова и ризика по безбедност личних података, те је неопходно проверавати делотворност прописа у овој области.

Контрола квалитета заштите података у јавној управи обухвата две компоненте које се односе на примењене мере и прописе. Прва компонента тиче се контроле техничких, организационих и кадровских мера којима се пружа заштита личним подацима. Она подразумева периодично испитивање функционалности предузетих системских мера заштите личних података. Овде можемо сврстати контролу квалитета рачунарских програма и информационих система у погледу нових изазова и опасности по податке, као и контролу ефикасности мера. Њу врше лица са посебним знањима из области заштите рачунарских система и програма, која су посебно овлашћена да се баве заштитом података у органу управе. Овај начин контроле може обухватити и претходна истраживања код увођења рачунарских система и рачунарских програма у органе јавне управе. Тестирање које претходи увођењу система и програма представља технички посао, који зависи од лица која праве програме, па се може рећи да ово

[570] D. Milovanović, „Analiza efekata regulative kao moderna tehnika javnog menadžmenta“, *Pravni život*, br. 9/2003, Beograd 2003, 1013.

техничко питање, иако важно за функционисање правног система, оно се решава на стручном нивоу информатичке струке.[571]

Друга компонента тиче се контроле квалитета прописа који уређују област заштите података. Приликом доношења прописа мора се водити рачуна о практичној примени њихових одредби. У супротном, предвиђени циљеви прописа остају само слово на папиру. Циљ закона служи, не само као основни разлог доношења и примене правних норми, већ и као референтна тачка за упоређивање предвиђеног и оствареног у датој друштвеној области. Ово је посебно од значаја у областима у којима инофмрационо-комуникационе технологије имају значајну улогу, због њиховог непрестаног усавршавања и измене са техничке стране.

Анализа ефеката које један пропис треба да произведе у друштву подразумева претходну и накнадну анализу. Накнадна анализа (*ex post*) има исту важност као и анализа основних елемената приликом доношења прописа. Накнадном анализом ефеката прописа анализирају се промене у друштву које је пропис донео, позитивни и негативни ефекти и степен примене прописа.

У Србији, обавеза праћења стања из свог делокруга је прописана као један од основних послова органа управе. Органи управе имају дужност да прате и утврђују стање у областима из свог делокруга, да анализирају последице утврђеног стања, и да у зависности од својих могућности и надлежности предузму мере или предложе Влади доношење прописа.[572]

Сматрамо да би ове одредбе требало поновити и у посебним законима, односно другим прописима, прецизирањем начина и времена вршења анализе ефеката њихових одредби. Анализа ефеката које закон или други пропис остварује у свакодневном животу треба да обухвати различите елементе. Скуп елемената које треба истражити, анализирати и упоредити обично је доста широк и зависи од предмета прописа.

Када је реч о заштити података у органима управе анализа може обухватити број и врсту штета и повреда личних података, изворе штете и повреда и пропусте у пружању заштите. Осим тога, анализа ефеката треба да

[571] За начине и теорију мерења проблема у вези са рачунарским програмима вид. Cem Kaner, *Measurement Issues and Software Testing*, online 2001, *file:///C:/Users/Win/Downloads/Measurement_Issues_and_Software_Testing_1.pdf*, 13. јануар 2019.
[572] Чл. 13. Закона о државној управи.

обухвати и став јавног мњења, односно друштва у вези са начином и квалитетом примене прописа. Став запослених у јавној управи о квалитету прописа би требало да буде један од елемената анализе ефеката. Финансијски елемент је још један важан параметар у анализи ефеката прописа. Примена једног прописа може да буде неадекватно скупа у зависности од метода које се користе, па је могуће изменити или рачунарски програм или начин заштите како би се постигао склад између заштите и финансијских могућности.

Учесталост повреде личних података, велике штете, спорост или неадекватност у примени, могу бити индикатори да су норме закона неадекватне и да је потребно изменити их. Због тога, сматрамо да је важно повремено анализирати стања у области заштите података у електронској јавној управи. Органи би требали да врше периодично испитивање о врстама напада и угрожавања података, проблемима који су настали у вези са обрадама, последицама донетих одлука и да на основу тих параметара примењују одредбе прописа или предузму нове мере у циљу побољшања заштите. Као што се наводи, „имајући у виду да се квалитет закона првенствено процењује на основу његових ефеката и степена примене, а не на основу квалитета правног текста или саме чињенице усвајања и ступања на снагу, предуслов правилне оцене квалитета јесте евиденција тих ефеката“.[573]

4. БЕЗБЕДНОСТ ИНФОРМАЦИЈА И ЗАШТИТА ЛИЧНИХ ПОДАТАКА У ПРАВНОМ СИСТЕМУ ЕУ

Правни систем ЕУ препознаје значај информационе безбедности за стварање квалитетне правне заштите личних података. Елементи информационе безбедности односе се на технолошке, организационе и управљачке мере које се предвиђају правним нормама ради успостављања минимума јединствене правне заштите.[574] У ери информационог друштва, где се већина комуникације одвија путем информационо-комуникационих технологија, неопходно је правним

[573] Dobrosav Milovanović, Nemanja Nenadić, Vladimir Todorić, *Studija o unapređenju zakonodavnog procesa u Republici Srbiji*, GIZ, Beograd 2012, 182.

[574] Саму информациону безбедност можемо одредити као систем мера унутар фирме, односно органа, које се уводе са циљем пружања заштите информацијама од неовлашћене употребе, неовлашћеног приступа, недозвољене измене, брисања или објављивања.

нормама обухватити, у основним цртама, и мере које служе сигурној комуникацији и трансакцијама, уз очување приватности свих учесника правних односа.

Ово се посебно односи на државе чланице ЕУ које теже дигитализацији јединственог тржишта, олакшавању размене добара и услуга преко интернета, оснаживању дигиталних мрежа и дигиталној трансформацији свих учесника на тржишту.[575] Да би се остварили поменути циљеви, неопходно је предвидети квалитетну правну инфраструктуру која покривају различите аспекте безбедности информација и података.

Општа уредба ЕУ предвиђа обавезу руковалаца и обрађивача да приликом установљавања система заштите личних података посебну пажњу обрате на нове технолошке облике и мере заштите као и трошкове увођења нових технологија у систем заштите. Адекватност увођења нових технологија и трошкова њиховог увођења треба сагледати кроз природу, опсег, друштвени контекст и разлоге обраде података који се уобичајено врше. Уз то, руковалац и обрађивач морају водити рачуна о ризицима који прете да угрозе основна права и интересе грађана у вези са њиховим личним подацима који се обрађују. У односу на такву процену, руковаоци и обрађивачи примењују одговарајуће техничке и организационе мере, како би се остварили циљеви уредбе. Дакле, руковаоци и обрађивачи морају извршити процену значаја података и процену ризика који се могу јавити у односу на такве податке.

Можемо рећи да систем информационе безбедности који се осликава у техничким и организационим мерама није изолован систем, већ треба да функционише у складу са осталим сегментима система заштите података. Зато, систем информационе безбедности представља важан подсистем система заштите података у оквиру општих правила о заштити података ЕУ. Општа уредба ЕУ предвиђа неке од основних мера техничке и организационе природе које се могу имплементирати у сврху заштите информационог система и личних података. Те мере се односе на:

[575] European Union Agency for Network and Information Security, *Guidelines for SMEs on the security of personal data processing*, Athens office (online) 2016, 5, *file:///C:/Users/Win/Downloads/WP2016%203-2%206%20Data%20Controllers%20Risk.pdf*, 05. децембар 2018.

1. Псеудонимизацију и енкрипцију личних података који се обрађују,
2. Обезбеђивање континуиране поверљивости, целовитости, доступности и отпорности система и услуга обраде личних података,
3. Могућност брзог приступа подацима и успостављања система након физичких или техничких проблема у систему (менаџмент кризних ситуација)
4. Редовне контроле и континуирани процес усавршавања и побољшавања система заштите (менаџмент развоја).[576]

Поменуте мере претежно су техничког карактера. Њих треба применити увек када то налаже конкретна обрада и ризици који је прате. Осим поменутих мера, Општа Уредба ЕУ предвиђа и дужност ангажовања лица овлашћеног за заштиту података у оквиру органа (фирме), као и ограничење приступа запослених у односу на податке. Ове мере су организационог карактера и имају за циљ да се уреди однос запослених према личним подацима грађана са којима се сусрећу у обављању свакодневних пословних делатности.

У тренутку израде истраживања, неколико независних надзорних тела надлежних за заштиту података држава чланица ЕУ, предвидело је списак потенцијалних техничких и кадровских мера које руковаоци и обрађивачи могу предузети приликом вршења обраде, како би се ускладили са европским и домаћим прописима. Ове мере односе се на информациону безбедност у оквиру система заштите података.

4.1. Препоруке независног надзорног тела Француске

Француска Национална комисија за информатику и слободе промовисала је неколико мера које су од помоћи руковаоцима и обрађивачима, између осталог и целокупној јавној управи, приликом вршења обраде. Мере се односе на очување информационе безбедности личних података.

Приликом предузимања радњи обраде, у сврхе информационе безбедности, руковалац или обрађивач треба да предузму четири корака. Први корак се састоји у евидентирању врсте личних података и носача на којима се ти подаци налазе.

[576] Чл. 32, ст. 1, Опште уредбе ЕУ.

Након тога, други корак се састоји у процењивању ризика. Процењује се евентуалне последице које могу настати по права и слободе појединаца, извори ризика и начин на који они делују. Такође, евидентирају се и постојеће и могуће мере које смањују ниво ризика на одговарајућу меру. Неке од ових мера су предвиђене Општом уредбом ЕУ, док су друге предложене као додатна заштита. Примера ради, те мере се односе на прављење копија података, ограничење приступа, енкрипција и анонимизација. Трећи корак се односи на имплементацију и проверу планираних мера, док је четврти корак засебан и односи се на периодична испитивања сигурности целокупног информационог система.[577]

Француско тело предвидело је низ мера које треба предузети, али и које треба избегавати приликом обраде како би се очувао систем безбедности. У односу на приступ информационом систему треба избегавати одавање приступне лозинке систему трећим лицима, чување лозинке у незаштићеним електронским документима или лако доступним документима у папирном облику, коришћење лозинке са личним подацима запосленог, коришћење лозинке дате од система, коришћење лозинке у електронској комуникацији.[578] Такође, треба избегавати додељивање једне лозинке свим или одређеном броју запослених, као и могућност приступа администратора систему више него што техничке потребе то захтевају. То значи да за приступ информационом систему и личним подацима треба користи „јаке“ лозинке које се тешко отварају и које се разликују у зависности од врсте уређаја. Сваки запослени треба да има појединачну лозинку за свој приступ, будући да се на тај начин индивидуализује одговорност.

Пожељно је забранити преузимање неовлашћених апликација, редовно одржавање система и рачунарских програма, онемогућавање приступа са неовлашћених уређаја и оперативних система, што се може остварити постављањем филтера приватности и лимита преузимања података. Такође, треба избегавати удаљене интернет конекције за приступ, омогућавање непознатог интернет приступа и подешавање бежичног интернета коришћењем јавних

577 CNIL**,** *A new guide regarding security of personal data*, online 2018, *https://www.cnil.fr/en/new-guide-regarding-security-personal-data#,*: 05. децембар 2018.

578 CNIL, Security of Personal Data-The CNILs Guides-2018 Edition, online 2018, 8, *https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle_gb_web.pdf*, 05. децембар 2018.

приступних тачака. Уместо тога, пажњу треба усмерити на коришћење приватних мрежа као и рачунарских програма који ће „контролисати“ нападе.[579] Предвиђене су и мере за одржавање сервера, интернет презентације, архивирање података, одржавање, итд.[580]

Применом поменутих мера, руковаоци и обрађивачи постају усклађени са одредбама Опште уредбе ЕУ (из перспективе француског независног тела). Наравно, није целисходно применити све мере уколико те не захтева природа обраде или података, односно ако ризици нису толико високи или једноставно висина уложених материјалних средстава није пропорционална степену заштите. Због тога, улога руковаоца и обрађивача је осетљива и захтева холистичку анализу свих елемената обраде.

4.2. Препоруке независног надзорног тела Немачке

Конкретизација техничких и организационих мера које предвиђа Општа уредба ЕУ учињена је и у немачком законодавству. Немачки закон прописује техничке и организационе мере које треба предузети приликом аутоматске обраде података (обраде података која се врши коришћењем рачунарских система и програма). У таквим случајевима, руковаоци и обрађивачи морају водити рачуна о функционалности рачунарских система, приступу подацима, разврставању података прикупљених у различите сврхе итд. Осим тога, они морају предузети неколико „контролних мера“. Код аутоматске обраде мора се забранити (одбити) сваки неовлашћени приступ средствима обраде (контрола приступа средствима обраде), мора се спречити неовлашћено стављање, читање, копирање, измена и брисање података (контрола смештања и интегритета података). Неопходно је осигурати да лица која раде на аутоматским обрадама података имају приступ само подацима који се односе на њихове случајеве у раду. Такође, важно је омогућити верификацију и евиденцију размене података између органа, када се подаци размењују електронским путем.[581]

[579] *Ibid.*, 13.
[580] *Ibid.*, 14-23.
[581] Одељак 64, ст. 3, Федералног закона о заштити података Немачке.

Када се примењују норме Федералног закона о заштити података Немачке, руковаоци и обрађивачи морају водити рачуна о препорукама и ставовима Федералне канцеларије за информациону безбедности.[582] Канцеларија је издала техничке смернице са циљем да се установе стандарди техничке заштите информационих система, као и да се примери добре праксе примене у различитим органима и фирмама. Ове смернице нису обавезне, али то могу постати уколико се имплементирају у подзаконске акте органа јавне управе. Такође, примена ових смерница може бити поуздан знак да су руковалац или обрађивач ускладили своје пословање и предузели све могуће мере да не дође до злоупотреба и повреда личних података, што процењује надзорни орган.

Препоруке у вези са имплементацијом техничких мера односе се на механизме криптографске заштите, тестове усклађености званичних електронских докумената са правилима заштите, питања безбедности приступа, управљања биометријским подацима у јавном сектору, итд.[583] Такође, Федерална канцеларија израђује редовне годишње извештаје о стању безбедности информационих система у Немачкој, што омогућава указивање на нове облике ризика и изазове који се појављују у вези са информационо-комуникационим технологијама. Извештаји се темеље на анализи постојећих ризика, слабости и пропуста у коришћењу информационих технологијама, што доприноси развоју одбрамбених система које органи јавне управе могу употребити у својим системима ради заштите личних података.

***

Информациона безбедност представља важан део система заштите личних података у електронској јавној управи. Иако је заштита непосредно усмерена на заштиту свих информација, података и информационог система у целини, она штити приватност грађана. Техничке и организационе мере су неопходни елементи заштите личних података, будући да правне норме могу само да забране и санкционишу поједина понашања, али не могу ефективно да их спрече у пракси.

[582] Одељак 64, Федералног закона о заштити података Немачке.

[583] За више вид. Federal Office for Information Security, Technical Guidelines, *https://www.bsi.bund.de/EN/Publications/TechnicalGuidelines/TechnicalGuidelines_node.html*, 06. децембар 2018.

Због тога, ова питања постају предмет интересовања правне науке и праксе, у оном сегменту који се односи на правилно увођење техничких и организационих норми, како би се омогућила њихова примена и санкционисало њихово непоштовање. Такав је случај и са регулативом у Србији, у вези са којом једино остаје питање практичне примене и одговора на нове ризике који ће се неминовно појавити у пракси.

VIII ЗАКЉУЧАК

Кроз историју, нове појаве су утицале на различите друштвене концепте. Међутим, ретко које су имале толики утицај попут појаве интернета и информационо-комуникационих технологија. Ове појаве су из корена промениле друштвену реалност и извршиле су толики утицај на редовне друштвене токове, да се без њих не може замислити било која област друштвеног живота. Отвориле су неслућене могућности напретка човечанства, измениле начине комуникације и односа између људи, утицале на измену традиционалних друштвених и пословних образаца и отвориле бројна неистражена поља људске радозналости. Уплив ових појава у све друштвене области дозвољава да савремено друштво означимо као информационо друштво.

Информационо друштво подразумева развој електронске писмености и дигитализацију свакодневних активности. Наравно, привредни субјекти први су прихватили нове појаве и применили их у циљу развоја својих пословних делатности и повећања квалитета и квантитета производа и услуга које нуде на тржишту. Захваљујући таквим околностима, грађани временом прихватају тржишне трендове и сами почињу да усклађују свој живот према новим технолошким појавама. Пратећи привреду и грађане, утицај интернета и информационо-комуникационих технологија проширио се и на јавни сектор.

Преиспитивањем традиционалних вредности и начина обављања послова, уочена је нестабилна улога државе у новом технолошком поретку. Застарели и историјски надмашени начини обављања државних послова нису могли да опстану у савременом друштву, које је усмерено на иновације, развој и ближи контакт свих друштвених чинилаца. Због тога, долази до промена у државама широм света, које покушавају да одрже контакт са грађанима и друштвом, будући да њих усмеравају и да им уједно служе. Тако се дошло у ситуацију да су развој друштва и технологије подстакле технолошку револуцију државе и њених органа.

Дигитализација и информационо-комуникационе технологије у јавном сектору најширу примену су нашле у области јавне управе, великог државног апарата који је у односу на друге државне чиниоце, у најближем односу са грађанима. Прихватањем нових трендова долази до измењене улоге и начина обављања послова органа управе. Нова улога утицала је и на промену правне

природе јавне управе. Поменути фактори утицали су на практично остварење потреба грађана и државе, које су се теоријски и практично остварили у појму електронске јавне управе.

Електронска јавна управа представља концепт измењене и савремене јавне управе који је изменио начин и сврху обављања државних послова. У техничком смислу, она се заснива на коришћењу интернета и информационо-комуникационих технологија за извршавање редовних државних послова и предвиђања стања у различитим друштвеним областима. Технички елементи утицали су и на њену правну природу. Они су омогућили органима управе да брже и квалитетније обављају послове, уз ближи контакт грађана са својом државом, која им сада даје могућност увида у државне послове, који утичу на њихова права и интересе. На тај начин остварује се трансформација правне природе јавне управе ка јавној служби, чији је основни циљ пружање квалитетних јавних услуга и задовољство грађана. Због тога, развој електронске јавне управе омогућава боље испуњавање задатака, обавеза и дужности према грађанима.

Осим што је допринела развоју односа грађана и органа управе, употреба информационо-комуникационих технологија и интернета отворила је значајна правна питања. Наиме, информационо-комуникационе технологије, осим небројених предности, носе са собом одређене изазове и ризике. Како је основно средство рада у данашњем свету информација, односно податак, јасно је да се главни изазови односе управо на њихову сигурност у дигиталном окружењу. Информације и подаци представљају главно оруђе рада информационих технологија, које се захваљујући интернету и могућностима које он пружа, могу брзо и лако делити са широким аудиторијумом. У таквом стању ствари, информације постају значајно средство утицаја и моћи, па онај ко поседује већи број информација и података, може лакше и брже обавити своје задатке.

Коришћење бројних информација и личних података у корелацији је са бројним задацима електронске јавне управе и њеном измењеном природом. Како би могла да обавља своје послове коришћењем нових технолошких средстава, јавној управи су неопходне велике количине личних података и информација у вези са грађанима. Сама та чињеница отвара питање безбедности података у поседу органа управе.

Због тога, можда и најзначајније и најактуелније правно питање електронске јавне управе односи се на механизме правне заштите личних података грађана у поседу органа управе. Коришћењем великог броја личних података употребом информационо-комуникационих технологија, отварају се питања заштите приватности и других права грађана у вези са њиховим личним подацима. Зато је неопходно установити адекватну правну регулативу која предвиђа одговарајуће начине заштите личних података.

Сва ова питања важе и у правном систему Србије, где су појавни облици електронске јавне управе у настајању и свакодневно се развијају. На том плану, у Србији је усвојен Закон о електронској управи и у пракси се појављују пројекти који остварују принципе електронске јавне управе. Ипак, нове друштвене трендове неопходно је ускладити и са другим законским текстовима који уређују поступање органа управе, што је превасходно случај са Законом о општем управном поступку. Ништа мањи значај немају ни закони који уређују посебне управне области и посебне управне поступке. Њиховом дигитализацијом ствара се дигитално управно окружење, усмерено на техничка и организациона питања која доводе до даљег напретка и развоја електронске јавне управе.

У истраживању смо дошли до закључка да се пројекти дигитализације јавне управе заснивају на личним подацима грађана. Лични подаци грађана носе информације о различитим аспектима идентитета одређеног или одредивог лица. Они се односе на физичке и психичке карактеристике, филозофска и верска убеђења, здравствено стање, количину новца на банковним рачунима, итд. Сви ти подаци свакодневно се користе и стварају потребу за установљавањем правне заштите која ће омогућавати слободно остваривање приватности, без бојазни да ће се неовлашћена лица упознати са њиховим подацима или да ће ти подаци бити злоупотребљени.

Приметан је и узајамни подстицај развијања информационо-комуникационих технологија и употребе личних података. Значај личних података доводи до идеја о новим концептима, попут *big data* и вештачке интелигенције. Ови појмови представљају новину о којима ће се у будућности више говорити и писати. Ови концепти захтевају стабилну правну инфраструктуру како би могли да остваре свој пун потенцијал и спрече

злоупотребе личних података. Можемо закључити да постојање квалитетне правне регулативе у вези са деловањем органа електронске јавне управе представља један од услова безбедности личних података.

Област личних података је толико широка да је створен посебан систем заштите личних података. У Србији традиција уређења области заштите личних података постоји од 2008. године, уколико изузмемо парцијалну регулативу која је постојала у претходним државама које су настајале на овим просторима. Чини се да претходна регулатива није дубље залазила у многа значајна питања система заштите личних података, већ је само уређивала основне појмове система заштите. Таква регулатива није била спремна да одговори новим изазовима који се свакодневно повећавају.

Због тога, приступило се свеобухватном уређивању система заштите личних података. Заинтересованости за формирање квалитетног и свеобухватног система заштите можда је у највишем делу допринела регулатива ЕУ. Наиме, ЕУ је 2016. године усвојила Уредба о заштити физичких лица у односу на обраду податка о личности и о слободном кретању таквих података (Општа уредба о заштити података ЕУ), која је ступила на снагу две године касније. Уредба представља један од ретких прописа који је у већем делу стао на страну грађана и заштите њихове приватности, као слабије стране у односу на све оне који обрађују и користе личне податке. Значајну улогу у доношењу овог прописа имали су грађани и невладине организације. Грађани и заинтересоване организације за заштиту људских права и слобода изборили су се за своје право на приватност, које је постало незаштићено у новоствореним друштвено-информатичким околностима.

На таласу европске револуције у вези са заштитом личних података и на територији Србије формирана је идеја о потреби за системским уређењем заштите података. На жалост, делује да је таква идеја настала под окриљем међународних дешавања и спољно - политичких циљева, од којих је најважнији прикључивање Србије ЕУ, него што је у друштву сазрела потреба за заштитом права у вези са личним подацима.

Међутим, на формирање квалитетног правног оквира у вези са заштитом података значајну улогу имали су и поједини домаћи фактори. Овде истичемо

Повереника за информације од јавног значаја и заштиту података о личности и запослене у овој институцији, који су својим радом и праксом указивали на недостатке и практичним примерима попуњавали празнине у области заштите личних података. Такође, управна и судска пракса су у мањој мери допринеле новим концептима у систему заштите података.

На таласу нових дешавања и дејством више фактора, у Србији усвојен Закон о заштити података о личности 2018. године, који представља закон који на системски начин уређује питање заштите личних података. Важна улога овог закона је велика, будући да су у њему препозната посебна људска права у вези са личним подацима у савременим околностима. Установљени су и нови механизми правне заштите који обезбеђују грађанима одређени степен сигурности у односу на њихове личне податке које обрађују друга лица.

Посебна права грађана у вези са личним подацима представљају важно средство у борби за очување приватности и заштите личних података. Као тековина европске и домаће судске и управне праксе, створени су основни принципи на којима почива систем заштите личних података. У систем правне заштите личних података Србије, као и у праву ЕУ, утемељена су основна начела заштите која се осликавају кроз начело најмањег могућег обима података, начело ограничене сврхе обраде, начело тачности, начело интегритета и поверљивости, начело ограниченог временског чувања података и начело одговорности руковаоца.

Иако ова начела представљају само полазишне тачке и оквире правне заштите личних података, она служе и као основ даље разраде конкретних права и механизама заштите. Начела сведоче о развоју свести о значају личних података у ери нових технологија и ризицима које оне носе. Посредни објекат заштите јесу посебна права грађана у вези са личним подацима. Захваљујући новим начелима, поред централног права на заштиту личних података које је загарантовано Уставом, заживела су и посебна права, попут права на обавештеност, права на приступ личним подацима, права на заборав, права на исправку и допуну личних података, права на ограничење обраде, права на преносивост података, права грађана у вези са аутоматским обрадама података и права на правно средство у случају незаконите обраде.

Поменута начела и права у области личних података имају скоро револуционаран значај. Она говоре о значају заштите приватности и растућој потреби заштите података у савременом свету. У овом контексту посебно радује чињеница да загарантована људска права и слободе не би требало да буду на нижој лествици од тренутне, већ да њихова улога и значај додатно расте временом, што би требало да се осликава и у све квалитетнијој регулативи и правној пракси.

Поред несумњивог напретка у области заштите приватности и личних података, у истраживању смо дошли до закључка да систем заштите података ипак садржи одређене недостатке које је неопходно исправити, како би се остварила сврха заштите личних података и приватности. Ти недостаци посебно су уочљиви у односу на личне податке који чувају и обрађују органи (електронске) јавне управе.

Кроз истраживање смо дошли до закључка да установљен општи систем заштите личних података није једнако применљив, процесно и материјално, у односу на све руковаоце и обрађиваче података. Најважнија разлика јавља у односу на руковаоце и обрађиваче приватног и јавног сектора. Многа решења и концепти не могу се у потпуности и доследно применити када је реч о личним подацима које обрађују органи јавне управе. Бројне специфичности произлазе из природе и улоге управе у животу грађана, која понекад подразумева и веће задирање у приватност грађана.

У Србији није предвиђен посебан управни поступак у вези са обрадом и коришћењем личних података грађана, па је неопходно да органи управе примењују одредбе општег управног поступка, уз вођење рачуна о посебним процесним елементима система заштите података. Јавља се потреба и за доношењем подзаконских аката којима се уређује чување и поступање са личним подацима у оквиру органа управе, будући да управни органи користе како материјалне, тако и дигиталне податке. Поједини концепти општег система заштите личних података могу, уз одређене модификације, да буду примењени и на заштиту података у електронској јавној управи.

Установили смо да се систем заштите података у електронској јавној управи заснива на три одвојена механизма заштите права грађана. Реч је о

механизмима управне заштите, судске заштите и заштите коју пружају независна надзорна тела (у Србији то је Повереник за информације од јавног значаја и заштиту података о личности). Узајамним деловањем, механизми стварају заокружен систем заштите који подразумева учешће управне и судске гране власти, али и тзв. „независне гране власти“.

Већи број механизама сматрамо као адекватно решење, будући да систем подразумева различите аспекте посматрања и механизме заштите. Управни механизми заштите делују у току самог управног поступка и након његовог завршетка, а односе се на заштиту личних података који се користе у таквом поступку. Уколико изостане адекватна заштита управног механизма, на снагу ступа судски систем заштите. Судски механизам заштите података пружа заштиту од сваког неправилног поступања органа управе са личним подацима грађана. У оквиру овог механизма заштите остварује се и накнада причињене материјалне и нематеријалне штете у односу на личне податке грађана.

Можда и најзначајнији механизам заштите личних података остварује се пред Повереником за информације од јавног значаја и заштиту података о личности. Повереник вршењем посебних овлашћења прати стање личних података, утиче на правну регулативу у вези са личним подацима и одлучује о притужбама грађана у вези са повредом њихових личних података. Уз то, Повереник кроз посебан поступак притужби, контролише рад органа управе у вези са личним подацима грађана. Као један од предлога, истичемо да би за област информација од јавног значаја, са једне стране и заштите личних података, са друге, требало предвидети различите надзорне органе, како би та тела била у могућности да свој рад у потпуности посвете једној посебној области. И поред заједничког именитеља у подацима, ове области се разликују према правима која у њиховим оквирима штите и начину остваривања тих права.

На основу истраживања дошли смо до закључка да је регулатива ЕУ у вези са механизмима заштите истоветна регулативи у Србији, што је позитивна ствар за српско законодавство, које тежи усаглашавању са европским. Такође, то нас води закључку да постоји општа потреба свих физичких лица за вишестепеном заштитом личних података, што представља законитост упоредно-правног посматрања.

Осим механизма правне заштите, систем заштите личних података чини и заштита која је усмерена на безбедност самих података, односно информација који се налазе у поседу органа управе. Будући да се ради о великом броју личних података, у правном систему Србије предвиђено је неколико мера које су управљене да пружају безбедност подацима, како у материјалном, тако и у електронском облику. Ове заштите представљају део информационе безбедности, али и део система заштите података, Реч је о техничким, организационим и кадровским мерама. Иако је реч о мерама која превазилазе оквире правне науке и уређују се посебним техничким нормама, ове мере представљају предмет законске регулативе. Квалитетна заштита личних података у електронској јавној управи подразумева вишедимензионални приступ, који подразумева и информационе мере заштите, усавршавање кадрова, ограничавање приступа свим запосленима, и томе сл.

Као посебно важан институт у оквиру кадровских мера истиче се постојање лица овлашћеног за заштиту података унутар органа. Овај нови институт помаже усклађивању правила поступка и других интерних правила са регулативом у вези са заштитом личних података. Предвиђање обавезе постојања овог лица умногоме ће допринети сигурности грађана у вези са њиховим личним подацима, али и олакшати остваривање заштитних механизама.

Сматрамо да је вишедимензионални приступ једини исправан и да га треба усавршавати и унапређивати кроз подзаконске акте, како би одговорио захтевима праксе и потребама грађана. У том погледу, може да буде индикативна пракса држава чланица ЕУ, која је са правне тачке гледишта, на истом степену развоја као и регулатива у Србији.

Истраживање је посветило пажњу и анализи квалитета прописа која је у области података о личности од изузетног значаја, јер говори о односу предвиђеног и оствареног, што у „новим областима“ информационо-комуникационих технологија представља неопходност. Без сагледавања резултата и ефеката примене прописа нема ни напретка у области заштите података. Зато, у пракси, пажњу треба ставити и на овај механизам заштите.

Информационо-комуникационе технологије ће свакако наставити да се развијају и побољшавају, што ће имати утицаја и на развој електронске јавне

управе. Са друге стране, појавиће се и бројни нови ризици по информације и податке грађана које користе органи управе. Зато, неопходно је наставити са истраживањем заштите података о личности у поседу електронске јавне управе. Ова материја захтева темељан теоријски и практични правни приступ, који не изоставља из вида ни значајна средства заштите која се налазе ван сфере права.

Аутор је имао за циљ да испита „анатомију“ електронске јавне управе и њен однос са личним подацима грађана, као основним средством рада. Напомене и размишљања о евентуалним решењима појединих празнина у овој области резултат су тежње аутора да пружи подршку развоју заштите података. На овај начин, аутор је покушао да укаже на основе нове и слабо истражене научне и практичне области у Србији и шире. Такође, истраживање представља тежњу аутора да пружи скромни допринос теорији и пракси у циљу поштовања права грађана и њихових личних података у савременом свету.

ЛИТЕРАТУРА

СПИСАК КОРИШЋЕЊЕ ЛИТЕРАТУРЕ НА СПРСКОМ ЈЕЗИКУ И НА ЈЕЗИЦИМА БИВШЕ ЈУГОСЛАВИЈЕ

1. АВРАМОВИЋ Драгутин, „Електронска демократија – пут ка непосредној демократији“, *Правни живот*, 12/2012, Београд 2012,
2. Agencija Europske unije za temeljna prava, *Priručnik o europskom zakonodavstvu o zaštiti podataka*, Ured za publikacije EU, Luksemburg 2014,
3. АДАМОВИЋ Анђелија, „Поступак у парницама за објављивање исправке неистините, непотпуне или нетачно пренете информације“, *Зборник радова Правног факултета у Нишу* (ур. Милан Петровић), LXI, Правни факултет у Нишу, Ниш 2012,
4. АНУЦОЈИЋ Драган, *Заштита информационих система и података*, Прометеј, Нови Сад 2008,
5. APOSTOLOV Ilija, HRISTOV Risto, „Izbor optimalne tehnike za enkripciju i dekripciju podataka“, *Informacione tehnologije- sadašnjost i budućnost*, (ur. Božo Krstajić), Podgorica 2014,
6. АРСЕНИН Александар, *Приватност у 21. веку – Заштита приватности и података о личности у информатичком добу*, Београд 2012,
7. БАЧАНИН Невенка, *Управно право, књига I – Уводна и организациона питања*, Крагујевац 2011,
8. BOBAN Marija, „Pravo na privatnost i pristup informacijama u suvremenom informacijskom društvu“, *Zbornik radova Pravnog fakulteta u Splitu* 3/2012, god. 49, Split 2012,
9. БОРИЈАНИШЕВИЋ Владимир, „Поступак у парницама за објављивање исправке“, *Зборник радова „Владавина права и правна држава у региону“* (ур. Горан Марковић), Правни факултет у Источном Сарајеву, Источно Сарајево 2014,
10. BUBANJA Branislav, Google koristi AI za kontrolu hlađenja u data centrima, *PC Press*, online 2018, https://pcpress.rs/google-koristi-ai-za-kontrolu-hladenja-u-data-centrima,
11. BUKOVAC PUVAČA Marijana, „Deset godina nove koncepcije naknade neimovinske štete“, *Zbornik Pravnog fakulteta Sveučilišta u Rijeci* (ur. Dionis Jurić), br. 1/2015, Rijeka 2015,
12. BUBALOVIĆ Tadija, „Pravo na pravni lijek protiv odluka tijela državne vlasti prema domaćem i međunarodnom pravu“, Zbornik sveučilišta Libertas, br.3/2018, Libertas međunarodno sveučilište, Zagreb 2018,
13. ВАСИЉЕВИЋ Драган, *Управно право*, Криминалистичко-полицијска академија, Београд 2015,
14. ВАСИЉЕВИЋ Драган, *Законитост управе и дискрециона оцена*, Криминалистичко-полицијска академија, Београд 2012,

15. VELJOVIĆ Alempije, RADOJČIĆ Miroslav, VESIĆ Jasmina, *Menadžment-informacioni sistemi*, Tehnički fakultet u Čačku, Čačak 2008,
16. ВЛАТКОВИЋ Милан, ЈОВАНОВИЋ Зоран, *Управни надзор*, Правни факултет у Крагујевцу, Крагујевац 2016,
17. VODINELIĆ Vladimir, „Pravo na slobodan pristup informacijama od javnog značaja kao ustavno pravo“, u: *Slobodan pristup informacijama – ustavno jemstvo i zakonske garancije*, Fond za otvoreno društvo, Beograd 2004,
18. VODINELIĆ Vladimir, „Sloboda medija kao granica zaštite podataka (medijska privilegija)“, *Zaštita podataka o ličnosti i poverljivi podaci – pravni standardi*, Fond za otvoreno društvo, Beograd 2005,
19. VRČEK Neven, MUSA Antonio, „E-uprava u Hrvatskoj: Izazovi transformacije uprave u digitalnom društvu“, *Forum za javnu upravu- Uprava u digitalno doba*, Friedrich Ebert Stiftung, Zagreb 2016,
20. ВУЧКОВИЋ Јелена, „Право на слободан приступ информацијама од јавног значаја“, *Зборник радова правног факултета у Нишу*, LIV, (ур. Радмила Ковачевић-Куштримовић), Правни факултет Универзитета у Нишу, Ниш 2009,
21. VUCHETICH Laurenz, „Pravednost i pravičnost u filozofiji prava“, *Pravnik: časopis za pravna i društvena pitanja*, 41 br. 2 (85), Pravni fakultet u Zagrebu (ur. Jerko Bulić), Zagreb 2007,
22. GDPR Informer, Službene smjernice o prenosivosti podataka, online 2018,
23. ДАВИНИЋ Марко, *Европски омбудсман и лоша управа*, Заштитник грађана, Београд 2013,
24. ДАВИНИЋ Марко, Независна контролна тела у Републици Србији, Досије студио, Београд 2018,
25. ДИВЈАКОВИЋ Даниел, *Основи криптологије, ОТП и РСА алгоритам*, мастер рад, Природно-математички факултет - Департман за математику и информатику, Нови Сад 2016,
26. DRAGOVIĆ Nikola, ŽILOVIĆ Mirjana, BOŠKOVIĆ Nikola, „Definisanje adekvatnih mera u funkciji zaštite poslovnih informacionih sistema“, *Zbornik radova naučno – stručnog skupa sa međunarodnim učešćem „Informacione tehnologije, obrazovanje i preduzetništvo*“, (ur. Alempije Veljović), Fakultet tehničkih nauka u Čačku, Čačak 2017,
27. DRAKULIĆ Mirjana, DRAKULIĆ Ratimir, „Elektronska upotreba i zloupotrebe“, *Pravni život*, br. 9/2003, god. LII, Beograd 2003,
28. ДРЕНОВАК-ИВАНОВИЋ Мирјана, *Дискрециона оцена у управном праву Србије са освртом на упоредно право и европске стандарде*, Правни факултет Универзитета у Београду, Београд 2011,
29. DILIGENSKI Andrej, PRLJA Dragan, CEROVIĆ Dražen, *Pravo zaštite podataka-GDPR*, Institut za uporedno pravo, Beograd 2018,
30. ДИМИТРИЈЕВИЋ Предраг, „Електронска управа и информационо друштво“, *Модерна управа- часопис за управно-правну теорију и праксу* (ур. Драгомир Кутлија), Агенција за државну управу Републике Српске, Бања Лука 2009,

31. ДИМИТРИЈЕВИЋ Предраг, „Организација државне управе у Републици Србији“, *Зборник радова Правног факултета у Нишу* LXII (ур. Предраг Димитријевић), Ниш 2012,
32. ДИМИТРИЈЕВИЋ Предраг, „Правна регулација електронске комуникације и право на приватност, *Зборник радова Правног факултета Универзитета у Источном Сарајеву* (ур. Горан Марковић), Правни факултет у Источном Сарајеву, Источно Сарајево 2011,
33. ĐURIĆ Sanja, „Monteskjeova teorija podele vlasti“, *Poslovne studije*, god. 1, br. 1-2, Banja Luka 2010,
34. ZVONAREVIĆ Mladen, *Socijalna psihologija*, Školska knjiga, Zagreb 1985,
35. ZIROJEVIĆ Mina, IVANOVIĆ Zvonimir, *Zaštita prava intelektualne svojine u sektoru informaciono-komunikacionih tehnologija*, Institut za uporedno pravo, Beograd 2016
36. ИЛИЋ ПЕТКОВИЋ Александра, ИЛИЋ Миле, „Одговорност државних службеника и заштита њихових права“, *Годишњак Педагошког факултета у Врању*, књига VIII, 1/2017, (ур. Сунчица Денић), Врање 2017,
37. ЈАКШИЋ Александар, *Европска конвенција о људским правима – коментар*, Правни факултет Универзитета у Београду, Београд 2006,
38. ЈАНЧИЋ Предраг, НИКОЛИЋ Младен, *Вештачка интелигенција*, електронско издање 2016,
39. JERINIĆ Jelena, *Sudska kontrola uprave*, Pravni fakultete Univerziteta Union, Beograd
40. ЈОВИЧИЋ Јелена, „Уставно регулисање права на јавно информисање“, *Зборник радова правног факултета у Нишу*, LXI (ур. П. Димитријевић), Правни факултет Универзитета у Нишу, Ниш 2012,
41. KAVRAN Dragoljub, *Javna uprava – reforma, trening, efikasnost*, Savet za državnu upravu vlade Srbije – Udruženje za javnu upravu – Centar za javnu upravu FON-a u saradnji sa Fondom za unapređenje kapaciteta Programa za razvoj Ujedinjenih nacija, Beograd 2005,
42. КАНДИЋ Татјана, *Судска власт у уставном и законодавном развоју Републике Србије*, докторска дисертација, Правни факултет Универзитета у Београду, Београд 2012,
43. КАТЈЕЗ Илија, „Личност и живот друштвене заједнице“, *Соколски зборник Infinitas,* Српско лекарско друштво, Београд 2012,
44. КОСТИЋ Лазо, *Административно право Краљевине Југославије I*, Београд 1933,
45. KRNETA Slavica, „Lična prava pravnih lica“, *Godišnjak Pravnog fakulteta u Sarajevu*, br. XXV, Sarajevo 1977,
46. КРИВОКАПИЋ Данило, КРИВОКАПИЋ Ђорђе, ТОДОРОВИЋ Иван, КОМАЗЕЦ Стефан, ПЕТРОВСКИ Андреј, ЕРЦЕГОВИЋ Катарина, *Водич за органе власти – Заштита података о личности*, Share фондација, Београд 2016,

47. KRIVOKAPIĆ Danilo, KRIVOKAPIĆ Đorđe, JOVANOVIĆ Milica, PERKOV Bojan, PETROVSKI Andrej, *Moji podaci, moja prava,* Share fondacija, Београд, 2018,
48. KRIVOKAPIĆ Đorđe, ADAMOVIĆ Jelena, KALEZIĆ Petar, KRIVOKAPIĆ Danilo, KRIVOKAPIĆ Nevena, MALINOVIĆ Sonja, PERKOV Bojan, PETROVSKI Andrej, *Share@Work 2016: Monitoring digitalnih prava i sloboda u Srbiji, Share fondacija*, Beograd 2017,
49. KULJANSKI Sonja, „Algoritam i njegova praktična primena“, *Vojnotehnički glasnik, br.* 3/10, (ur. Dragana Marković), Ministarstvo odbrane Republike Srbije, Beograd 2010,
50. LILIĆ Stevan, *Evropsko upravno pravo – sa osvrtom na upravno pravo Srbije u kontekstu evropskih integracija*, Beograd 2011,
51. LILIĆ Stevan, „Organizacioni pojam uprave“, Pravni zbornik – časopis za pravnu teoriju i praksu br. 2-3/95, Podgorica 1995
52. ЛИЛИЋ Стеван, „Право, информатичка технологија и заштита података“, *Анали Правног факултета у Београду*, бр. 2-3/1989, Београд 1989,
53. ЛИЛИЋ Стеван, *Управно право и Управно процесно право*, Београд 2013,
54. LOZINA Duško, KLARIĆ Mirko, „Javna uprava suvremene države u promijenjenim okolnostima“, *Zbornik radova Pravnog fakulteta u Splitu,* god. 49, br. 1, Split 2012,
55. МАЉКОВИЋ Небојша, *Политичко-извршна функција у друштвенополитичком систему Југославије*, докторска дисертација, Правни факултет Универзитета у Београду, Београд 1985,
56. МАРКОВИЋ Данило, *Општа социологија*, Савремена администрација, Београд 1993,
57. МАРКОВИЋ Ратко, *Управно право*, Слово АД, Београд 2002,
58. MEDIĆ Duško, „O naknadi nematerijalne štete“, u: Odgovornost za štetu, naknada štete i osiguranje, (ur. Zdravko Petrović, Vladimir Čolović), Institut za uporedno pravo, Udruženje za odštetno pravo, Pravosudna akademija, Valjevo-Beograd 2018,
59. MILENKOVIĆ Dejan, *Pristup informacijama, zaštita podataka o ličnosti i tajnost informacija – Aktuelna pitanja zakonodavstva u Srbiji*, Komitet pravnika za ljudska prava, Beograd 2009,
60. MILENKOVIĆ Dejan, „Upravno-procesni i drugi slični oblici zaštite prava na pristup informacijama u komparativnom pravu“, *Strani pravni život,* 3/2015, Beograd 2015,
61. MILENKOVIĆ Dejan, „Zašto je Srbiji potreban zakon o klasifikaciji tajnih podataka“, *Zaštita podataka o ličnosti i poverljivi podaci- Pravni standardi*, Fond za otvoreno društvo, Beograd 2005,
62. МИЛКОВ Драган, *Управно право I – уводна и организациона питања*, Правни факултет у Новом Саду, Нови Сад 2016,
63. МИЛКОВ Драган, *Управно право II- Управна делатности*, Универзитет у Новом Саду- Правни факултет, Нови Сад 2017,

64. МИЛКОВ Драган, „Инспекцијски надзор и заштита животне средине“, *Зборник радова Правног факултета у Новом Саду*, 4/2015, Нови Сад 2015,
65. MILOVANOVIĆ Dobrosav, „Odnos opšt(ij)eg i posebn(ij)ih, *Polis- časopis za javnu politiku*, br. 11, Stalna konferencija gradova i opština i Centar za javnu i lokalnu upravu, Beograd 2016,
66. MILOVANOVIĆ Dobrosav, NENADIĆ Nemanja, TODORIĆ Vladimir, *Studija o unapređenju zakonodavnog procesa u Republici Srbiji*, GIZ, Beograd 2012,
67. MILOVANOVIĆ Dobrosav, „Analiza efekata regulative kao moderna tehnika javnog menadžmenta“, Pravni život, br. 9/2003, god. LLI, Beograd 2003,
68. МИЛОВАНОВИЋ, Добросав, „Визионарска мисао професора Славољуба Поповића о управним уговорима, *Зборник радова правног факултета у Нишу – Тематски број посвећен Славољубу Поповићу*, Правни факултет Универзитета у Нишу, Ниш 2011,
69. МИЛОВАНОВИЋ Добросав, ЦУЦИЋ Вук, „Унапређење пословног окружења у Србији у светлу нових решења Нацрта закона о општем управном поступку“, Усклађивање пословног права Србије са правом ЕУ (ур. В. Радовић), Правни факултет Универзитета у Београду, Београд 2015,
70. МИЛОВАНОВИЋ Добросав, НИЧИЋ Јован, ДАВИНИЋ Марко, *Стручно усавршавање државних службеника у Републици Србији*, Удружење за јавну управу, Београд 2011,
71. MILOSAVLJEVIĆ Bogoljub, „Načelo podele vlasti u Ustavu i ustavnoj praksi Republike Srbije“, *Pravni zapisi*, god. III, br. 1, Beograd 2012,
72. MILOSAVLJEVIĆ Milan, MIŠKOVIC Vladislav, *Elektronska trgovina*, Univerzitet Singidunum, Beograd 2016,
73. MILOSAVLJEVIĆ Milan, VEINOVIĆ Mladen, GRUBOR Gojko, *Informatika*, Univerzitet Singidunum, Beograd 2009,
74. МИТРОВИЋ Драган, *Увод у право*, Правни факултет Универзитета у Београду, Београд 2010,
75. MONTESKJE Šarl, *O duhu zakona*, tom I, knjiga XI, Filip Višnjić, Beograd 1989,
76. MRAZNICA Erne, „GDPR – Novi izazov zaštite podataka o ličnosti“, časopis *Bankarstvo* vol. 46, br. 4, (ur. Veroljub Dugalić), Udruženje banaka Srbije, Beograd 2017,
77. NAISBITT John, *Megatrendovi- Deset novih smejrova razvoja koji mijenjaju naš život*, Globus, Zagreb 1985,
78. ОРЛОВИЋ Славиша, „Независна тела- четврта грана власти или контролор власти“, у *Савремена држава: структура и социјалне функције* (ур. Чедомир Чупић), Konrad Adenauer Stiftung, Факултет Политичких наука и Центар за демократију, Београд 2010,
79. Партнери за демократске промене, *Анализа: „Анонимизација података у судским одлукама у Србији- ка усаглашеним правилима и пракси*“ (радна верзија), Београд, 2015,

80. PAUNOVIĆ Milan, KRIVOKAPIĆ Boris, KRSTIĆ Ivana, *Međunarodna ljudska prava*, Pravni fakultet Univerziteta u Beogradu, Beograd 2013,
81. ПЕТРОВИЋ Далибор, „Друштвена конструкција интерперсоналних медија – од телеграфа до интернета“, у *Интернет и друштво*, (ур. Д. Тодоровић, Д. Петровић, Д. Прља), Српско социолошко друштво, Универзитет у Нишу – Филозофски факултет, Институт за упоредно право, Ниш – Београд 2014,
82. PETROVIĆ Zdravko, *Naknada nematerijalne štete zbog povrede fizičkog integriteta*, Sarajevo, 1990,
83. ПЕТРОВИЋ Миодраг, *О појму јавне управе у савременој теорији*, Зборник радова Правно-економског факултета у Нишу, II, Ниш 1963,
84. ПОПОВИЋ Славољуб, МАРКОВИЋ Бранислав, ПЕТРОВИЋ Милан, *Управно право - Општи део*, Београд 2002,
85. POSAVEC Mirjana, „Višestruke inteligencije u nastavi“, *Život i škola*, br. 24, 2/2010, (ur. Anđelka Peko), Učiteljski fakultet u Osijeku, Osijek 2010,
86. PRLJA Dragan, ANDONOVIĆ Stefan, „Naknada štete kod povrede ličnih podataka“, u: Odgovornost za štetu, naknada štete i osiguranje (ur. Zdravko Petrović, Vladimir Čolović), Institut za uporedno pravo, Udruženje za odštetno pravo, Pravosudna akademija, Valjevo-Beograd 2018
87. ПРЉА Драган, АНДОНОВИЋ Стефан, „Дигитализација рада Управног суда“, Савремена управа, бр. 1, Регула, Београд 2019
88. PRLJA Dragan, DILIGENSKI Andrej, *Fejsbuk i pravo*, Institut za uporedno pravo, Beograd 2014,
89. PRLJA Dragan, RELJANOVIĆ Mario, *Pravna informatika*, Službeni glasnik, Beograd 2010,
90. PUSIĆ Eugen, *Nauka o upravi – knjiga I – Uvodna pitanja, uprava u društvu, uprava kao ljudska djelatnost*, Narodne novine Zagreb, 1989,
91. ПРОТИЋ Данијела, „Информациона безбедност: стандарди или правила“, *Војно дело*, пролеће/2013, Београд
92. RADBRUH Gustav, *Filozofija prava*, Nolit, Beograd 1980,
93. РАДЕНКОВИЋ Божидар, ДЕСПОТОВИЋ-ЗРАКИЋ Маријана, БОГДАНОВИЋ Зорица, БАРАЋ Душан, ЛАБУС Александра, *Електронско пословање*, Факултет организационих наука, Београд 2015,
94. RADOJKOVIĆ Miroljub, „Za slobodan pristup informacijama“, *Prizma* br.4/2002, Centar za liberalno-demokratske studije, Beograd 2002,
95. RADOLOVIĆ Antonio, „Pravo osobnosti u novom Zakonu o obaveznim odnosima“, *Zbornik Pravnog fakulteta Sveučilišta u Rijeci*, br. 1/2006, (ur. Velinka Grozdanić), Rijeka 2006,
96. РАДОШЕВИЋ Ратко, „Управни спор због ћутања управе“, *Зборник радова Правног факултета у Новом Саду* бр. 4/2015 (ур. Слободан Орловић), Нови Сад 2015,

97. РЕНДУЛИЋ Илија Дарио, *ITdesk.info – пројекат рачунарске е-едукације са слободним приступом – Приручник за дигиталну писменост*, Отворено друштво за размену идеја, Загреб 2013,
98. RESANOVIĆ Aleksandar, „Zaštita podataka o ličnosti u Srbiji i Crnoj Gori, odnosno u SR Jugoslaviji“, u: *Zaštita podataka o ličnosti i poverljivi podaci – pravni aspekti*, Fond za otvoreno društvo, Beograd 2005,
99. RIZMAL Irina, RADUNOVIĆ Vladimir, KRIVOKAPIĆ Đorđe, *Vodič kroz informacionu bezbednost u Republici Srbiji*, Centar za Atlanske studije i Misija OEBS-a u Srbiji, Beograd 2016,
100. СИМОВИЋ Ивана, ЛАЗИЋ Мирослав, „Грађанско правна заштита права личности“, *Зборник радова Правног факултета у Нишу*, бр. 68, год. LIII, (ур. Ирена Пејић) Ниш 2014,
101. SIMONOVIĆ Branislav, JOVANOVIĆ Zoran, „Elektronska uprava i prevencija korupcije“, *Pravni život*, br. 10/2017, god. LXVI, Beograd 2017,
102. СТАНКОВИЋ Обрен, ВОДИНЕЛИЋ Владимир, *Увод у грађанско право*, Номос, Београд 2007,
103. СТЕФАНОВИЋ Милан, РАДОВАНОВИЋ Душан, ЈОЛОВИЋ Даница, *Водич за примену Закона о инспекцијском надзору*, Представништво Cardno Emerging Markets USA Ltd, Београд 2017,
104. STJEPANOVIĆ Nikola, *Upravno pravo u SFRJ – opšti deo, knjiga II*, Prosvetni pregled, Beograd 1973,
105. ТОМИЋ Зоран, МИЛОВАНОВИЋ Добросав, ЦУЦИЋ Вук, *Практикум за примену Закона о општем управном поступку*, Службени гласник, Београд, 2017,
106. ТОМИЋ Зоран, *Опште управно право*, Правни факултет у Београду, Београд, 2012,
107. TOPALOVIĆ Darko, *Kako veštačka inteligencija transformiše bankarski sektor*?, *PC Press*, online 2018, https://pcpress.rs/kako-vestacka-inteligencija-transformise-bankarski-sektor/,
108. УРОШЕВИЋ Зорица, „Положај и улога јавних агенција у нашем правном систему“, *Правни живот*, бр. 10, Београд 2005,
109. FINŽGAR Alojzije, *Pravo ličnosti*, Službeni list SFRJ, Beograd 1988,
110. HARDING Luk, *Dosije Snouden*, Evrogiunti, Beograd 2014,
111. ЦВЕТИЋ Раденка, „Правна способност и биомедицина – биомедицинска дискриминација“, *Зборник радова Правног факултета у Новом Саду*, 3/2011, (ур. Драгиша Дакић), Нови Сад 2011,
112. ЦУЦИЋ Вук, *Управни спор пуне јурисдикције*, Правни факултет Универзитета у Београду, Београд 2016,
113. ČOLAKOVIĆ Maja, BUBALO Lana, „Pravo na zaborav kao instrument zaštite prava ličnosti u Evropskoj Uniji“, *Zbornik radova Pravnog fakulteta u Tuzli*, god. 3, br. 2, (ur. Vedad Gurda), Pravni fakultet u Tuzli, Tuzla 2017.

КОРИШЋЕНА ЛИТЕРАТУРА НА СТРАНИМ ЈЕЗИЦИМА

1. ABRAMSON Jeffrey, „Searching for Reputation: Reconciling Free Speech and the „Right to be Forgotten““, *North Carolina Journal of Law & Technology*, vol. 17, issue 1, online 2015,
2. AGRAWAL Pallavi, „Public Administration Challenges in the World of AI and Bots“, *Public Administration Review*, vol. 78, issue 6, (ed. Paul Battaglio), American Society for Public Administration, Washington 2018,
3. AMBROSE Meg Leta, AUSLOOS Jef, „The Right to Be Forgotten Across the Pond“, *Journal of Information Policy*, vol. 3, Pennsylvania State University Press, Penssylvania 2013,
4. Article 29 Data Protection Working Party, *Guidlines on the right to data portability, 16/EN WP 242 rev.01*, online 2017,
5. BAHR Kanzlei, *Kein Recht auf Einschränkung der Datenverarbeitung nach Art. 18*, DSGVO, online 2018, https://www.datenschutz.eu/urteile/Kein-Recht-auf-Einschraenkung-der-Datenverarbeitung-nach-Art-18-DSGVO-Verwaltungsgericht-Stade-20181009/#,
6. BURKERT Herbert, „Privacy - Data Protection a German/European Perspective“, *in Governance of Global Networks in the Light of Differing Local Values, (eds. E. Christoph, K. Keeneth), Nomos: Baden-Baden 2000,*
7. CASTELLS Manuel, *THE Internet Galaxy - Reflections on the Internet, Business, and Society*, Oxford University Press, Oxford 2001,
8. CERULUS Laurens, *E-Democracy entrepreneur: Online voting will boom in coming years*, Euractiv, online 2014, https://www.euractiv.com/section/elections/interview/e-democracy-entrepreneur-online-voting-will-boom-in-coming-years,
9. CNIL, *A new guide regarding security of personal data*, online 2018, https://www.cnil.fr/en/new-guide-regarding-security-personal-data#,
10. CNIL, Security of Personal Data-The CNILs Guides-2018 edition, online 2018, https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle_gb_web.pdf,
11. COLONNA Liane, „Europe versus Facebook: An Imbroglio of EU Data Protection Issues“, *Data protection on the move – Current Developments in ICT and Privacy/Data Protection*, (eds. S. Gutwirth, R. Leenes, P. de Hert), vol. 24, Springer, Dordrecht – Heidelberg – New York 2016,
12. COX James, *Canada and the Five Eyes Intelligence Community*, Strategic Studies Working Group Papers, 2012, https://www.opencanada.org/features/canada-and-the-five-eyes-intelligence-community/,
13. CULIK Nicolai, „Brussels Calling: Big Data and Privacy”, y *Big Data in Context-Legal, Social and Technological Insights*, (eds. T. Hoeren, B. Kolany-Raiser), Springer, online 2018,

14. CULIK Nicolai, DOPKE Christian, „About Forgetting and Being Forgotten“, y *Big Data in Context- Legal, Social and Technological Insights,* (eds. T. Hoeren, B. Kolany-Raiser), Springer, online 2018,
15. DAVISON Mark, *The Legal Protection of Databases*, Cambridge University Press, Cambridge – New York – Melbourne 2003
16. DE BAETS Antoon, „A historian's view on the right to be forgotten“, *International Review of Law, Computers & Technology*, Vol. 30, Nos. 1-2, Routledge- Taylor & Francis group, online 2016,
17. DE BRUIN Hugo, PRAKKEN Henry, SVENSSON Jorgen, „The Use of Legal Knowledge-Based Systems in Public Administration: What Can ¨ Go Wrong?“, *Legal Knowledge and Information Systems*, (eds. T.J.M. Bench-Capon, A. Daskalopulu and R.G.F. Winkels), Jurix, Amsterdam: IOS Press, Amsterdam 2002,
18. DE GUISE Preston, *Data protection – Ensuring Data Availability*, Auerbach Publication, New York 2017,
19. DE HERT Paul, PAPAKONSTANTINOU Vagelis, MALGIERI Gianclaudio, Laurent Beslay, SANCHEZ Ignacio, „The right to data portability in the GDPR: Towards user-centric interoperability of digital services“, *Computer law & security review* (ed. Steve Saxby), Amsterdam – Boston - London 2018,
20. Department of Finance and Administration, Australian Government, *Automated Assistance in Administrative Decision-Making Better Practice Guide*, Australian Government Information Management Office, Canbera 2007,
21. DESOUZA Kevin, *Delivering Artificial Intelligence in Government: Challenges and Opportunities*, IBM Center for The Business of Government, Washington 2018,
22. DE TERWANGNE Cécile, „Internet Privacy and the Right to Be Forgotten/Right to Oblivion“, Monograph "VII International Conference on Internet, Law & Politics-Net Neutrality and other challenges for the future of the Internet", *Revista de internet, derecho y politica,* Universitat Oberta de Catalunya, Barcelona 2012,
23. DOPKE Christian, „The Importance of Big Data for Jurisprudence and Legal Practice“, y *Big Data in Context- legal, Social and Technological Insights*, (eds. T. Hoeren, B. Kolany-Raiser), Springer, online 2018,
24. DUPUIS Georges, GUEDON Marie-Jose, *Institutions administratives – Droit administratif*, Armand Colin, Paris 1988,
25. ELMASTI Ramez, NAVATHE Shamkant, *Fundamentals of Database Systems*, Addison-Wesely Publishing Company, Boston – Columbus - ets. 2010,
26. ERAKOVICH Rodney, KAVRAN Dragoljub, WYMAN Sherman, „Public administration and ethics training strategy“ , *Legal life*, no. 9/2003, Belgrade 2003,
27. European Group on Tort Law, Principles of European Tort Law, Text and Commentary, Springer, New York - Wien 2005,
28. European Union Agency for Network and Information Security, *Guidelines for SMEs on the security of personal data processing*, Athens 2016.
29. GODSMITH Stephen, CRAWFORD Susan, *The Responsive city*, Jossey-Bass: A Wiley Brand, San Francisco 2014,

30. GELLMAN Barton, POITRAS Laura, „U.S. British intelligence mining data from nine U.S. Internet companies in broad secret program“, *The Washington Post*, online 2013, https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html?noredirect=on&utm_term=.712646f40b06,
31. HANOLD Stefanie, SCHUTZE Benjamin, „The Principle of Purpose Limitation and Big Data“, *New techonolgy, Big Data and the Law* (ed. Marcelo Corrales, Mark Fenwick, Nikolaus Forgó), Springer, Singapore 2017,
32. HENMAN Paul, *Governing Electronically, E-Government and the Reconfiguration of Public Administration, Policy and Power*, Palgrave Macmillan, UK 2010,
33. KANER Cem, *Measurement Issues and Software Testing*, online 2001, *file:///C:/Users/Win/Downloads/Measurement_Issues_and_Software_Testing_1.pdf,*
34. KARVALICS László, *Information Society – what is it exactly? (The meaning, history and conceptual framework of an expression*), online coursbook, Budapest 2007,
35. LAMBERT Paul, *Understanding the New European Protection Rules*, CRC Press-Taylor and Francis Group, New York 2017,
36. LILIC Stevan, „Legal Framework of E-Government in Europe of Knowledge“, *Legal, Political and Economic Initiatives Towards Europe of Knowledge* (ed. Kestutis Kriščiunas), Kaunas University of Technology, Kaunas 2006,
37. MOLNAR Szilárd, *E- Government in the European Union*, (online), Budapest 2007, https://s3.amazonaws.com/academia.edu.documents/8057421/09_molnar_final.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1535474281&Signature=7O6qeJ8biz965HTNVDM%2F%2FkA2PA8%3D&response-content-disposition=inline%3B%20filename%3DeGovernment_in_the_European_Union.pdf,
38. Organization for Economic Co-operation and Development, *European Principles for Public Administration*, Sigma Papers No. 27, online 1999, http://unpan1.un.org/intradoc/groups/public/documents/nispacee/unpan006804.pdf.
39. Organization for Economic Co-operation and Development, *Policy Brief - The e-government imperative: main findings*, online 2003, http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN015120.pdf,
40. PANZARDI Roberto, CALCOPIETRO Carlos, FANTA IVANOVIC Enrique, *New-Economy Sector- Study Electronic Government and Governance: Lessons for Argentina*, The World Bank, Washington DC, July 2002,
41. PERRI P. 6, E-governance *Styles of Political Judgment in the Information Age Polity*, Palgrave Macmillan, UK 2004,
42. SCHWARTZ Paul, „Property, Privacy and Personal Data“, *Harvard Law Review*, vol. 117, University of Harvard, Harvard 2003,

43. SCHIMDL Matthias, „100 Tage DSGVO aus Sicht der Datenschutzbehörde, Keine freiwillige Einwilligung zur Verwendung eines „GPS-Trackers““, *Firmenfahrzeugen newsletter*, 3/2018, online 2018, https://www.dsb.gv.at/documents/22758/115212/Newsletter_DSB_4-18.pdf/8d475c88-615c-4a1f-a014-464e0018a9c0,
44. SICULAR Svetlana, *Gartner's Big Data Definition Consists of Three Parts, Not to Be Confused with Three 'V's*, Forbes, online 2013, http://www.forbes.com/sites/gartnergroup/2013/03/27/gartners-big-data-definition-consists-of-threeparts-not-to-be-confused-with-three-vs,
45. VOIGT Paul, VON DEM BUSSCHE Axel, *The EU General Data Protection Regulation (GDPR)- A Practical Guide*, Springer, eBook, online 2017,
46. WACHTER Sandra Wachter, MITTELSTADT Brent, FLORIDI Luciano, „Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation“, *International Data Privacy Law*, Vol. 7, No. 2, (ed. Nora Ni Loideain), Oxford 2017,
47. WATSON Hugh, "Tutorial: Big Data Analytics: Concepts", *Technologies and Application, Communications of the Associations for Information Systems*, vol. 34, art. 65, The Berkeley Electronic Press, Berkeley 2014, https://pdfs.semanticscholar.org/d392/0f02dbb15da19b04d782fc0546ef113e0bf7.pdf,
48. WEBER Max, *Economy and Society: An Outline of Interpretative Sociology*, University of California Press, Berkeley - Los Angeles - London 1978,
49. WEINTRAUB Joseph, „Expert Systems in Government Administration“, *AI Magayine*, Vol. 10, online 1989, file:///C:/Users/Win/Downloads/730-Article%20Text-727-1-10-20080129.pdf,
50. WOLK Stuart, LUDDY William, *Legal Aspects of Computer Use*, Engelwood Cliffs, New York 1986,
51. United Nations, UN Global E-government Readiness Report 2005 - From Egovernment to E-inclusion, UN Department of Economic and Social Affairs, Division for Public Administration and Development Management, New York 2005,
52. European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions EU, E-government Action Plan 2016-2020, Accelerating the digital transformation of governments, European Commission, Brussels 2016.

КОРИШЋЕНИ ИНТЕРНЕТ ИЗВОРИ

1. Блиц бизнис, Ана Брнабић отворила први државни Data centar, https://www.blic.rs/biznis/ana-brnabic-otvorila-prvi-drzavni-data-centar-evo-sta-ce-se-sve-u-njemu-nalaziti/9wqwge1,
2. Град Суботица, Услужни центар Суботице претеча јединственог управног места, http://www.subotica.rs/index/page/lg/cp/id/11862,
3. ГеоСрбија, Систем Националне инфраструктуре геопросторних података доступан је на: http://www.geosrbija.rs/,
4. GDPR Informer, Službene smjernice o prenosivosti podataka, online 2018, dostupno na: https://gdprinformer.com/hr/gdpr-clanci/sluzbene-smjernice-o-prenosivosti-podataka,
5. EDGE expert system, *https://www.anao.gov.au/work/performance-audit/edge-project*,
6. Enerprivacy Consulting Group, Categories of Personal Information, *https://enterprivacy.com/2017/03/01/categories-of-personal-information/*,
7. Internet world stats, World Internet Users and 2018 Population Stats, https://www.internetworldstats.com/stats.htm,
8. Интегрисани здравствени информациони систем Републике Србије, Министарство здравља, https://www.mojdoktor.gov.rs/about,
9. Повереник за информације од јавног значаја и заштиту података о личности, Питања и одговори, доступно на: https://www.poverenik.rs/sr/%D0%B7%D0%B0%D1%88%D1%82%D0%B8%D1%82%D0%B0-%D0%BF%D0%BE%D0%B4%D0%B0%D1%82%D0%B0%D0%BA%D0%B0/%D0%BF%D0%B8%D1%82%D0%B0%D1%9A%D0%B0-%D0%B8-%D0%BE%D0%B4%D0%B3%D0%BE%D0%B2%D0%BE%D1%80%D0%B84/1600-%D0%BF%D0%B8%D1%82%D0%B0%D1%9A%D0%B0-%D0%B8-%D0%BE%D0%B4%D0%B3%D0%BE%D0%B2%D0%BE%D1%80%D0%B8.html,
10. Портал еуправе Републике Србије, http://www.euprava.gov.rs/eusluge/opis_usluge?generatedServiceId=2888&title=Upis-u-bira%C4%8Dki-spisak&alphabet=lat,
11. Портал отворених података, Отворени подаци, доступно на: https://data.gov.rs/sr/discover/,
12. Privacy matters, *Austria: Data protection for personal data of legal entities under the GDPR*?, online 2018, https://blogs.dlapiper.com/privacymatters/austria-data-protection-for-personal-data-of-legal-entities-under-the-gdpr/,
13. Пројекат „Бебо добродошла на свет“, http://gakfront.org/A3d2HmiN/assets/files/OBAVESTENJA/Prezentacija_bebo_dobrodosla.pdf,

14. Република Србија, Министарство трговине, туризма и телекомуникација, Образовано тело за координацију послова информационе безбедности, http://mtt.gov.rs/vesti/obrazovano-telo-za-koordinaciju-poslova-informacione-bezbednosti/
15. Републички геодетски завод, Статистика Републичког геодетског завода, http://www.rgz.gov.rs/,
16. РТС, Систем „Бебо добро дошла на свет“ усклађен са изменама закона, доступно на: http://www.rts.rs/page/stories/sr/story/125/drustvo/3186661/bebo-dobrodosla-na-svet-uskladjeno-za-izmenama-zakona.html,
17. Служба за управљање кадровима, Пријава на обуке у организацији Националне академије за јавну управу, доступно на: http://www.suk.gov.rs/sr/strucno_usavrsavanje/obuke_po_temama.dot?id_obuke_oblast=106,
18. UK Information Commissioner's Office, Principle (c): Data minimisation, https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/,
19. UK Information Commissioner's Office, Principle (d): Accuracy, https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/,
20. UK Information Commissioner's Office, Principle (e): Storage limitation, https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/,
21. Federal Office for Information Security, Technical Guidelines, https://www.bsi.bund.de/EN/Publications/TechnicalGuidelines/TechnicalGuidelines_node.html,
22. Hrvatska pošta, Službenik za zaštitu osobnih podataka, https://www.posta.hr/sluzbenik-za-zastitu-osobnih-podataka/5607.

КОРИШЋЕНИ ПРОПИСИ И ОДЛУКЕ ОРГАНА РЕПУБЛИКЕ СРБИЈЕ

1. Закон о безбедносно-информативној агенцији, *Службени гласник* РС, бр. 42/2002, 111/2009, 65/2014-одлука УС и 66/2014,
2. Закон о библиотичко-информационој делатности, *Службени гласник* РС ,бр. 52/2011,
3. Закон о државним службеницима, *Службени гласник* РС, бр. 79/2005, 64/2007, 116/2008, 104/2009, 99/2014 и 94/2017,
4. Закон о државној управи, *Службени гласник* РС, бр. 79/2005, 101/2007,95/2010 и 99/2014,
5. Закон о државном премеру и катастру, *Службени гласник* РС, бр. 72/2009, 65/2013, 15/2015 – одлука УС, 96/2015, 47/2017 и 41/2018 – др. закон,
6. Закон о заштити података о личности, *Службени гласник* РС, бр. 87/2018,
7. Закон о заштити података о личности, *Службени лист* СРЈ, бр. 24/98 и 26/98,

8. Закон о инспекцијском надзору, *Службени гласник* РС, бр. 36/2015,
9. Закон о информационом систему Републике Србије, *Службени гласник* РС, бр. 12/96,
10. Закон о јавним агенцијама, *Службени гласник* РС, бр. 18/2005 и 81/2005,
11. Закон о јавним предузећима, *Службени гласник* РС, бр. 15/2016,
12. Закон о јавном бележништву, *Службени гласник* РС, бр. 31/2011, 85/2012, 19/2013, 55/2014- др. закон, 93/2014- др. закон, 121/2014, 6/2015, 106/2015,
13. Закон о јединственом матичном броју грађана, *Службени гласник* РС, бр. 24/2018,
14. Закон о локалној самоуправи, *Службени гласник* РС, бр. 129/2007 и 83/2014- др. закон,
15. Закон о матичним књигама, *Службени гласник* РС, бр. 20/2009, 145/2014 и 47/2018,
16. Закон о министарствима, *Службени гласник* РС, бр. 44/2014, 14/2015, 54/2015, 96/2015- др. закон и 62/2017,
17. Закон о наслеђивању, *Службени гласник* РС, бр. 46/95, 101/2003,
18. Закон о Националној академији за јавну управу, *Службени гласник* РС, бр. 94/2017,
19. Закон о Националној корпорацији за осигурање стамбених кредита, *Службени гласник* РС, бр. 55/2004
20. Закон о облигационим односима, *Службени лист* СФРЈ, бр. 29/78, 39/85, 45/89 – одлука УСЈ и 57/89, *Службени лист* СРЈ, бр. 31/93 и *Службени лист* СЦГ, бр. 1/2003- Уставна повеља,
21. Закон о општем управном поступку, *Службени лист* СРЈ, бр. 33/97 и 31/2001, *Службени гласник* РС , бр. 30/2010,
22. Закон о основама друштвеног система информисања и о информационом систему Федерације, *Службени лист* СФРЈ, бр. 68/81,
23. Закон о пацијентима, *Службени гласник* РС, бр. 45/2013,
24. Закон о пореском поступку и пореској администрацији, *Службени гласник* РС, бр. 80/2002 и 30/2018,
25. Закон о пребивалишту и боравишту грађана, *Службени гласник* РС, бр. 87/2011,
26. Закон о прекршајима, *Службени гласник* РС, бр. 65/2013, 13/2016 и 98/2016
27. Закон о раду, *Службени гласник* РС, бр. 24/2005, 113/2017,
28. Закон о слободном приступу информацијама од јавног значаја, *Службени гласник* РС, бр. 120/2004, 54/2007, 104/2009, 36/2010,
29. Закон о тајности података, *Службени гласник* РС, бр. 104/2009,
30. Закон о управним споровима, *Службени гласник* РС, бр. 111/2009,
31. Закон о уређењу судова, *Службени гласник* РС, бр. 116/2008, 65/2018,
32. Закон о утврђивању надлежности аутономне покрајине Војводине, *Службени гласник* РС, бр. 99/2009 и 67/2012- одлука УС,

33. Кривични законик Републике Србије, *Службени гласник* РС, бр. 85/2005, 94/2016.
34. Међународни пакт о грађанским и политичким правима,, Сл. лист СФРЈ (Међународни уговори), бр. 7/1971,
35. Повеља о људским и мањинским правима и грађанским слободама, *Службени лист* СЦГ, бр. 6/2003
36. Породични закон, *Службени гласник* РС, бр. 18/2005, 72/2011,
37. Правилник о чувању, заштити и сигурности података у оквиру информационог система Централног регистра обавезног социјалног осигурања, *Службени гласник* РС, бр. 29/2013,
38. Стратегија стручног усавршавања државних службеника у Републици Србији, *Службени гласник* РС, бр. 56/2011 и 51/2013,
39. Стратегија развоја електронске управе у Републици Србији за период од 2015-2018. године,
40. Стратегија развоја Републичког геодетског завода 2020, Београд 2017,
41. Стратегија реформе јавне управе у Републици Србији, *Службени гласник* РС, бр. 9/14 и 42/14,
42. Устав Републике Србије, *Службени гласник* РС, бр. 98/2006,
43. Устав СФРЈ, *Службени лист* СФРЈ, бр. 9/74.
44. Царински закон, *Службени гласник* РС, бр. 18/2010, 111/2012 и 113/2017- др. закон.
45. Мишљење Повереника бр. 011-00-00607/2013-05, од 16.10.2013. год,
46. Мишљење Повереника бр. 011-00-00548/2010-05, од 01.09.2010. год,

Мишљење Повереника бр. 011-00-00223/2011-05, од 30.05.2011. год,

47. Мишљење Повереника бр. 011-00-00292/2010-05, од 22.07.2010. год,
48. Мишљење Повереника бр. 011-00-00181/2011-05 од 23.05.2011. год,
49. Одлука Уставног суда, бр. ІУз-1218/2010, од 24.05.2012. год
50. Одлука Уставног суда, бр. ІУз-41/2010, од 06.07.2012. год
51. Одлука Уставног суда ІУз-252/2002, од 27.02.2014. год
52. Пресуда Апелационог суда у Београду, Гж 8976/12 од 10.01.2013. год,
53. Пресуда Вишег суда у Београду бр. К. По3-10/13-СПК-153/15 од 25.05.2015. год,
54. Пресуда Прекршајног суда у Београду бр. 89 Пр. бр. 120316/12 од 29.01.2014. год,
55. Пресуда Прекршајног суда у Београду бр. 46 Пр. бр. 35401/11, од 30.12.2011. год,
56. Пресуда Прекршајног суда у Београду, бр. 41 Пр. бр. 78121/10, од 27.09.2011. год,
57. Пресуда Управног суда у Београду, бр. 9 У 1581/12 од 18.05.2012. године
58. Решење Повереника у вршењу инспекцијског надзора, бр. 07-00-01090/2010-05, од 27.07.2010. год,
59. Решење Повереника бр. 011-00-00102/2009-05, од 08.03.2011. год,

60. Решење Управног суда у Београду, бр. 21 У.10163/11 од 20.10.2011 год,
61. Решење Управног суда, одељење у Новом Саду, бр. III-4 У. 7906/11, од 14.10.2011. год,
62. Упозорење Повереника бр. 164-00-00193/20110-07 од 22.09.2011. год,
63. Упозорење Повереника бр. 164-00-00030/2011-07, од 31.03.2011. год.

КОРИШЋЕНИ ПРОПИСИ СТРАНИХ ДРЖАВА И ОДЛУКЕ УПРАВНИХ И СУДСКИХ ОРГАНА СТРАНИХ ДРЖАВА

1. Аустријски закон којим се олакшава електронска комуникација између органа јавне власти - Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen (E-Government-Gesetz – E-GovG) StF: BGBl. I Nr. 10/2004, https://www.ris.bka.gv.at/Dokumente/Erv/ERV_2004_1_10/ERV_2004_1_10.pdf,
2. Аустријски закон о заштити личних података - *Bundesgesetz über den Schutz personenbezogener Daten*, од 31.07.2017. год., https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2017_I_120/BGBLA_2017_I_120.pdfsig,
3. Директива ЕУ о заштити појединаца у односу на обраду личних података и слободан промет таквих података - Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data , *Official Journal L 281 , 23/11/1995 P. 0031 – 0050*, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN,
4. Европска конвенција за заштиту људских права и основних слобода, Савет Европе, Рим 1950, https://www.echr.coe.int/Documents/Convention_ENG.pdf,
5. Закон о електронској управи Немачке- Gesetz zur Förderung der elektronischen Verwaltung (E-Government-Gesetz - EGovG), vom 25. Juli 2013 (BGBl. I S. 2749), доступно на: https://www.gesetze-im-internet.de/egovg/EGovG.pdf,
6. Закон о електронској управи Црне Горе, *Службени лист* ЦГ, бр. 32, од 30. 07. 2014. год,
7. Zakon o provedbi Opće uredbe o zaštiti podataka, Narodne novine Hrvatske 42/12, do 25.05.2018. год,
8. Конвенција Савета Европе о заштити лица у односу на аутоматску обраду података, бр. 108, Стразбур, 1981. год, https://rm.coe.int/1680078b37,
9. Немачки закон о унапређењу електронске управе - Gesetz zur Förderung der elektronischen Verwaltung (E-Government-Gesetz - EGovG), (BGBl. I S. 2749), од 25.07.2013,https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl113s2749.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl113s2749.pdf%27%5D__1551773912035,

10. Одлука Француске комисије за информатику и слободе, Délibération n°SAN-2019-001 од 21.01.2019, https://www.legifrance.gouv.fr/affichCnil.do?&id=CNILTEXT000038032552
11. Одлука суда Рајнланд-Пфлаца, *Das Amtsgericht Diez (Schlussurteil vom 07.11.18, Aktenzeichen 8 C 130/18), https://openjur.de/u/2116788.html*,
12. Пресуда Европског суда за људска права *Mikhaylyuk and Petrov v. Ukraine*, app no. 11932/02, 2009,
13. Пресуда Европског суда за људска права, *Y.Y. v. Russia*, app. no. 40378/06, 2016,
14. Пресуда Европског суда за људска права, *Rotaru v. Romania*, app. no. 28341/95, 2000,
15. Пресуда Европског суда за људска права, *Peck v. the United Kingdom*, app no. 44647/98, 2003,
16. Пресуда Европског суда за људска права, *Halford*, RJD, 1997 – III, бр. 44, од 25.06.1997. год.
17. Пресуда Европског суда за људска права, *Amman*, бр. 69, од 16.02.2000. год
18. Пресуда Европског суда за људска права, *Silver*, Series A, no. 61, бр.83, од 25.03.1983. год.
19. Пресуда Регионалног суда у Бону, Немачка, бр. 10 O 171/18, од 29.05.2018. год.,
20. Пресуда Суда правде Европске уније, *Google Spain SL, Google Inc. Vs. Agencia Espanola de Protecction de Datos (Google v. Costeja)*, case no. C-131/12, 2014,
21. Пресуда Управног суда Стаде, бр. Az. 1 B 1918/18, од 09.10.2018. год.
22. Пресуда уставног суда федералне државе *Rheinlnad-Pfalz*, case no. B0035/12, од 13.05.2014,
23. Старатегија вештачке интелигенције Уједињених арапских емирата, UAE Artificial Inteligence Strategy 2031, https://government.ae/en/about-the-uae/strategies-initiatives-and-awards/federal-governments-strategies-and-plans/uae-strategy-for-artificial-intelligence,
24. Статут Агенције за заштиту особних података Хрватске- Statut Hrvatske Agencije za zaštitu osobnih podataka од 04.07.2004. год, https://azop.hr/images/dokumenti/159/statut_agencije_za_zastitu_osobnih_podataka.pdf,
25. Уговор из Лисабона ЕУ, Lisbon EU Treaty, *https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:C:2007:306:FULL&from=HR*,
26. Уговор о функционисању Европске уније, Official EN Journal of the European Union C 326/49, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN,
27. Универзална декларација Уједињених нација о људским правима, Организација Уједињених Нација, 217 (III) , од 10. децембра 1948 год., Париз, http://www.sostelefon.org.rs/zakoni/12.%20Univerzalna%20deklaracija%20o%20ljudskim%20pravima.pdf,

28. Уредба ЕУ о заштити физичких лица у погледу обраде личних података и слободног кретања таквих података и укадњу Директиве 95&46- Regulation 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95&46EC (General Data Protection Regulation), of 27.04.2016, https://publications.europa.eu/en/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1/language-en,
29. Француски закон о информатици, документима и слободама - Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, http://www.congreso.es/docu/docum/ddocum/dosieres/sleg/legislatura_12/spl_13/pdfs/46.pdf,
30. Француски закон о заштити података о личности - Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, https://www.legifrance.gouv.fr/eli/loi/2018/6/20/JUSC1732261L/jo/texte
31. Француски декрет бр. 2005-1309 о примени Закона бр. 78-17 о обради података, документима и индивидуалним слободама, Decree No. 2005-1309 од 20.10.2005, file:///C:/Users/Win/Downloads/Decree_enacted_for_application_of_Act_No_78_17_on_data_processing_2005_am_2007_en%20(1).pdf.

Биографија аутора

Стефан (Небојша) Андоновић је рођен 13. маја 1991. године у Београду, где је завршио Основну школу „Радоје Домановић" и Спортску гимназију завршио је у Београду. Правни факултет Универзитета у Београду уписао је у школске 2010/11. године, на којем је и дипломирао 25. августа 2014. године са општим успехом 9,37.

На матичном факултету школске 2014/15. године уписао је мастер академске студије, Јавно-правни модул, управно-правни под модул, где је све испите положио са оценом 10, да би септембра 2015. године одбранио мастер рад под насловом *Усмени управни акти*. На докторске академске студије на Правном факултету Универзитета у Београду (управно-правна ужа научна област) уписао се у школској 2015/16. години.

Пословну каријеру започео је у септембру 2014. године као адвокатски приправник у адвокатској канцеларији адвоката Небојше Андоновића. Након завршетка приправничког стажа у адвокатској канцеларији, фебруара 2017. године положио је правосудни испит у Београду. Од маја 2018. године ангажован је на Институту за упоредно право у Београду у својству истраживача сарадника. На Институту бави се научним истраживањима у области дигитализације, права заштите података, управног права и спортског права. За арбитра пред Сталном спортском арбитражом Олимпијског комитета Србије именован је 2018. године.

Говори енглески, а служи се и француским језиком

У току свог школовања на докторским академским студијама, кандидат Стефан Андоновић је сачинио и објавио је неколико научних радова, од којих се истичу *Правна природа националних олимпијских комитета – упоредно-правна анализа, Право на спорт као људско право, Правна класификација електронског спорта као врсте спорта*, *Отворени подаци као посебна услуга јавне управе* и други.

Изјава о ауторству

Име и презиме аутора: Стефан Андоновић

Број индекса: ДС 11/2015

Изјављујем

да је докторска дисертација под насловом:

„Заштита података у електронској јавној управи у Републици Србији - правни аспекти“

- резултат сопственог истраживачког рада;
- да дисертација у целини ни у деловима није била предложена за стицање друге дипломе према студијским програмима других високошколских установа;
- да су резултати коректно наведени и
- да нисам кршио/ла ауторска права и користио/ла интелектуалну својину других лица.

Потпис аутора

У Београду, 10.09.2019. год. _____

Изјава о истоветности штампане и електронске верзије докторског рада

Име и презиме аутора: Стефан Андоновић

Број индекса: ДС 11/2015

Студијски програм: докторске студије

Наслов рада: „Заштита података у електронској јавној управи у Републици Србији – правни аспекти“

Ментор: проф. др Добросав Миловановић

Изјављујем да је штампана верзија мог докторског рада истоветна електронској верзији коју сам предао/ла ради похрањена у **Дигиталном репозиторијуму Универзитета у Београду.**

Дозвољавам да се објаве моји лични подаци везани за добијање академског назива доктора наука, као што су име и презиме, година и место рођења и датум одбране рада.

Ови лични подаци могу се објавити на мрежним страницама дигиталне библиотеке, у електронском каталогу и у публикацијама Универзитета у Београду.

Потпис аутора

У Београду, 10.09.2019. год. _____

Изјава о коришћењу

Овлашћујем Универзитетску библиотеку „Светозар Марковић“ да у Дигитални репозиторијум Универзитета у Београду унесе моју докторску дисертацију под насловом:

„Заштита података у електронској јавној управи у Републици Србији – правни аспекти“

која је моје ауторско дело.

Дисертацију са свим прилозима предао/ла сам у електронском формату погодном за трајно архивирање.

Моју докторску дисертацију похрањену у Дигиталном репозиторијуму Универзитета у Београду и доступну у отвореном приступу могу да користе сви који поштују одредбе садржане у одабраном типу лиценце Креативне заједнице (Creative Commons) за коју сам се одлучио/ла.

1. Ауторство (CC BY)
2. Ауторство – некомерцијално (CC BY-NC)
3. **Ауторство – некомерцијално – без прерада (CC BY-NC-ND)**
4. Ауторство – некомерцијално – делити под истим условима (CC BY-NC-SA)
5. Ауторство – без прерада (CC BY-ND)
6. Ауторство – делити под истим условима (CC BY-SA)

(Молимо да заокружите само једну од шест понуђених лиценци.
Кратак опис лиценци је саставни део ове изјаве).

Потпис аутора

У Београду, 10.09.2019. год. _____