

**УНИВЕРЗИТЕТ У НИШУ**  
**ПРАВНИ ФАКУЛТЕТ**

**Обрада података о личности**  
**(мастер рад)**

**Ментор:**

**Проф. др Милош Прица**

**Студент:**

**Петровић Марина**

**M001/21 – ИТ**

**Ниш, 2022. године**

## САДРЖАЈ:

УВОД .....	1
<b>1. ОДРЕЂЕЊЕ ПОЈМА ПОДАТАКА О ЛИЧНОСТИ .....</b>	<b>2</b>
<b>2. ВРСТЕ ПОДАТАКА О ЛИЧНОСТИ .....</b>	<b>3</b>
2.1. Подаци о личности у приватној, јавној и професионалној сфери појединца ..	3
2.2. Обични и осетљиви подаци о личности.....	4
2.3. Подаци о личности који не уживају правну заштиту.....	5
2.4. Метаподаци као подаци о личности.....	6
<b>3. ОБРАДА ПОДАТАКА О ЛИЧНОСТИ.....</b>	<b>7</b>
<b>4. ЗАКОНОДАВНИ ОКВИР.....</b>	<b>9</b>
4.1. Међународно право .....	9
4.2. Национално законодавство .....	11
<b>5. ОСНОВНА НАЧЕЛА ОБРАДЕ ПОДАТАКА О ЛИЧНОСТИ .....</b>	<b>13</b>
<b>6. ЗАКОНИТОСТ ОБРАДЕ ПОДАТАКА О ЛИЧНОСТИ .....</b>	<b>16</b>
6.1. Пристанак .....	17
6.2. Закључење и извршење уговора.....	21
6.3. Поштовање правних обавеза.....	22
6.4. Заштита животно важних интереса.....	23
6.5. Јавни интерес.....	24
6.6. Легитимни интерес .....	25
<b>7. ОБРАДА ПОСЕБНИХ ВРСТА ПОДАТАКА О ЛИЧНОСТИ.....</b>	<b>28</b>
<b>8. ПОСЕБНИ СЛУЧАЈЕВИ ОБРАДЕ ПОДАТАКА О ЛИЧНОСТИ.....</b>	<b>31</b>
<b>9. ЗАШТИТА И НАДЗОР НАД ОБРАДОМ ПОДАТАКА О ЛИЧНОСТИ.....</b>	<b>34</b>
<b>10. ПРИМЕРИ ИЗ ПРАКСЕ МЕЂУНАРОДНИХ СУДОВА.....</b>	<b>38</b>
10.1. Case of Peck v. The United Kingdom - Application no. 44647/98 (28/01/2003) .	38
10.2. Case of Big brother watch and others v. the United Kingdom [GC] - Application no. 58170/13, 62322/14 and 24960/15 .....	39
10.3. CJEU - C-673/17 - Planet49 (01/10/2019) .....	42
10.4. CJEU - C-61/19 - Orange Romania SA v Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) (11/11/2020).....	43
10.5. Case no. 20-CIV-03346 - Kelly Whalen and others v. Facebook, (07/08/2020), Superior Court of California.....	45
10.6. Case 10 O 84/20 - LG Itzehoe (Germany) (11/06/2020).....	46
<b>11. ПРИМЕРИ ИЗ ПРАКСЕ ДОМАЋИХ СУДОВА .....</b>	<b>47</b>
<b>12. ЗАКЉУЧНА РАЗМАТРАЊА .....</b>	<b>50</b>
<b>13. ЛИТЕРАТУРА .....</b>	<b>52</b>
<b>14. ИСТРАЖИВАЧКА ГРАЂА.....</b>	<b>53</b>
<b>Сажетак и кључне речи .....</b>	<b>56</b>
<b>Summary and key words .....</b>	<b>58</b>
<b>Биографија ауторке .....</b>	<b>60</b>

## УВОД

Право на заштиту података о личности није таксативно наведено као једно од основних људских права у међународним правним актима који су представљали темељ универзалних људских права. У Универзалној декларацији о људским правима из 1948. године, Европској конвенцији о људским правима из 1950. године и Пакту о грађанским и политичким правима из 1966. године наводи се право на поштовање приватног живота, али се не наводи право на заштиту података о личности. Наравно таксативно наведена права нису била ограничавајућег карактера, па је примена и остваривање заштите појединих универзалних права показала да се у оквиру права на поштовање приватног живота мора штитити и право на заштиту података о личности. Касније, током времена, право заштите података се издвојило из оквира права на поштовање приватног живота и развило се као посебно фундаментално људско право. Право на заштиту података о личности далеко је шире од права на поштовање приватног живота. Оно се односи на све врсте података о личности које се обрађују, без обзира у којој мери ти подаци могу утицати на право на приватан живот. Као одговор на све убрзанији развој технологије и све чешће злоупотребе података о личности јавила се потреба за стварањем правила која детаљније регулишу прикупљање, обраду и коришћење података о личности. Најзначајнији документ којим се регулише област заштите података о личности представља Општа уредба о заштити података - ГДПР, док на националној основи то јесте Закон о заштити података о личности из 2019. године. Управо наведена акта одређују појам података о личности, обраде података, прописују начела која се морају поштовати приликом обраде података о личности, који субјекти учествују у овом процесу, који су то законити основи обраде, која су права лица чији се подаци обрађују, које обавезе имају руковооци и обрађивачи података о личности, колико подаци могу да се чувају, када може доћи до злоупотребе података, која су правна средства доступна и друга важна питања. У овом раду ће се најпре ауторка осврнути на појам дефинисања личних података, различитих подела, дефинисања обраде података и законских правила којима се то регулише, док ће се касније усредсредити детаљније на начела и законом дозвољене основе обраде података о личности, али и примере такве обраде, на обраду посебних врста података о личности, затим ће бити обрађени неки интересантни случајеви из праксе међународних и националних органа и на крају ће бити изнета закључна разматрања.

## 1. ОДРЕЂЕЊЕ ПОЈМА ПОДАТАКА О ЛИЧНОСТИ

Подаци о личности представљају карактеристичну особину одређеног лица. Они се користе у свакодневним животним ситуацијама, служећи као средство конкретизације и остваривања правних односа. Међутим, подаци о личности не представљају само средство идентификације. Заправо, они представљају појавни облик одређене личности у правном животу који служи за остваривање различитих права и интереса.<sup>1</sup> Члан 4 ст. 1 тач. 1 Закона о заштити података о личности даје следећу дефиницију: „Податак о личности је 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.“<sup>2</sup> Податак о личности је дакле сваки податак који се односи на неко физичко лице, уз помоћ којег је идентитет тог физичког лица одређен или одредив, посредно или непосредно. Податак о личности може бити свака информација која нас, као физичка лица, ближе одређује и која се може довести у везу са конкретном особом. То могу бити име и презиме, адреса, ЈМБГ, број телефона, број рачуна у банци, списак омиљених књига, укупна потрошња мобилног саобраћаја и слично, али и сваки други податак који нешто говори о нама. Велики број наших личних података се налази на интернету, попут ИП адресе, ИМЕИ броја уређаја којим приступамо мрежи, лозинки, наших налога за електронску пошту и друштвене мреже, историје активности са таквих налога (шерови, лајкови, кликови), историје претраге интернета и слично. Иако многи дигитално генерисани подаци на први поглед не делују као подаци о личности, уз помоћ њих се неко лице може посредно идентификовати, у неким случајевима чак и само на основу таквих података или у комбинацији са још неким подацима. Управо могућност идентификације физичког лица и те податке чини личним подацима. Због тога категоризација одређеног податка као податка о личности понекад захтева да се у обзир узме целокупан контекст конкретног случаја, па је и правна дефиниција податка о личности довољно широка да би се у примени тестирала у односу на различите ситуације и неке још непредвидљиве догађаје који могу утицати на основна права и слободе. Подаци који су препознатљиви, неодређени или на неки други начин

---

<sup>1</sup> Стефан Андоновић, Драган Прља, *Основи права заштите података о личности*, Институт за упоредно право, Београд 2020. године, стр. 14;

<sup>2</sup> члан 4, Закон о заштити података о личности ("Сл. гласник РС", бр. 87/2018);

измењени, не могу се сматрати подацима о личности уколико на основу њих није могуће конкретизовати неку особу. 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 података о личности.<sup>3</sup>

## 2. ВРСТЕ ПОДАТАКА О ЛИЧНОСТИ

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.<sup>4</sup> Међутим, подела личних података се може још упростити тако да личне податке поделимо у три основне области живота појединца, а то су приватна, јавна и професионална област живота појединца. Сваки појединац има своју личну сферу, коју обично не дели са јавношћу, јавну сферу која се дели са трећим лицима и са којом је обично упознат већи број људи или сви заинтересовани и последњу, професионалну сферу у коју се убрајају подаци у вези са пословним активностима неког лица. Ове области неретко се поклапају, па подаци о личности који се употребљавају у једној области друштвеног живота имају велики значај и у остале две.

### 2.1. Подаци о личности у приватној, јавној и професионалној сфери 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),
- 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),
- лични ставови и наклоност лица према стварима, лицима и појавама (омиљена врста хране, омиљена боја, песма).

---

<sup>3</sup>Op.cit., Стефан Андоновић, Драган Прља., стр. 16;

<sup>4</sup><https://enterprivacy.com/2017/03/01/categories-of-personal-information/> приступљено дана 27.09.2022. године;

У ову групу можемо сврстати и друге идентификационе податке личне природе, као што су подаци о етничком и социјалном пореклу лица, подаци о сексуалности, медицински подаци и подаци о здрављу.

У личне податке који се тичу јавног живота појединца убрајају се они подаци о личности који се односе на сегменте живота појединца у друштвеној заједници и то:

- подаци о породичном животу (да ли лице има породицу, величина породице, односи у породици)
- податке о социјалном окружењу (пријатељи, конекције, припадност у формалним и неформалним организацијама),
- податке о криминалној прошлости лица (да ли је осуђивано, да ли се воде поступци против њега).

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),
- пословни подаци (да ли је лице запослено, на ком радном месту, оцене о резултатима рада, подаци о одсуству са посла),
- финансијски подаци (бројеви рачуна, банке у којима су ускладиштена средства тог лица, подаци о личној имовини лица, кредитни статус лица),
- радна историја (подаци о фирмама у којима је радило лице, подаци о запосленима у фирми тог лица, подаци о новчаним примањима и трансакцијама).

## **2.2. Обични и осетљиви подаци о личности**

Могуће је извршити поделу на „обичне“ личне податке и „осетљиве“ личне податке, који се још називају и „посебна категорија“ података о личности. Ова подела прави разлику података о личности у зависности од степена поверљивости и значаја који лични податак има за физичко лице. „Обични“ подаци о личности носе уобичајену информацију о физичком лицу, док „осетљиви“ подаци о личности носе посебно значајну информацију о личном идентитету физичког лица. Повреда осетљивих података о личности, по правилу, производи значајнију последицу за физичко лице од повреде обичних података о личности. Сходно овој подели, осетљиви подаци о

личности уживају већи степен правне заштите у односу на друге врсте података о личности.<sup>5</sup> У групу осетљивих података о личности убрајају се подаци о верским и филозофским уверењима, расно и етничко порекло, политичко мишљење, генетски подаци, биометријски подаци, подаци о сексуалном животу и сексуалној оријентацији физичког лица и подаци о здравственом стању.<sup>6</sup> 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 података о личности може имати утицаја на друштвену позицију, углед и статус одређеног лица. Остали подаци о личности спадају у групу „обичних“ података о личности.

### **2.3. Подаци о личности који не уживају правну заштиту**

Правни систем којим се штити област заштите података о личности тежи ка томе да заштита приватности појединца буде што свеобухватнија, али ипак је то често недостижно, те постоји одређена група личних података која изостаје из оквира правне заштите. То је случај са оним личним подацима који су мање важни, који су доступни јавности или који се не могу злоупотребити. У позитивно-правном законодавству Републике Србије обично се наводе категорије података о личности који уживају заштиту и оне категорије код којих правна заштита изостаје. У чл. 3 ст. 2 Закона о заштити података о личности Републике Србија прописано је да изван сфере правне заштите података о личности остају они подаци који се обрађују од стране физичких лица за личне потребе или потребе њиховог домаћинства.<sup>7</sup> У овој ситуацији степен опасности од пропуста и злоупотреба није превише изражен, па самим тим изостаје и заштита државе. Ово је једина група података о личности којима Закон о заштити података о личности ускраћује правну заштиту. Одличан пример јесу лични адресари, телефонски именик, фото албуми и слично, у случају да их власник користи искључиво у личне, непословне сврхе тј. уколико нису доступни трећим лицима они остају у оквирима породице, па заштита државе у овом случају изостаје. У овим ситуацијама изостаје реакција државе из разлога јер не постоји потреба за упливом државе у строго личну сферу појединца. Самим тим, претпоставља се да је обрада података о личности

---

<sup>5</sup>Д. Кривокапић, Ј. Адамовић, Д. Тасић, А. Петровски, П. Калезић, Ђ. Кривокапић, *Водич кроз Закон о заштити података о личности и ГДПР, тумачење новог правног оквира, 2019. године, стр. 14;*

<sup>6</sup>Ор. Сит. Чл. 17, *Закон о заштити података о личности;*

<sup>7</sup>Ор. Сит. Чл. 3 ст. 2, *Закон о заштити података о личности;*

у личне или породичне сврхе приватна ствар о којој превасходно мора да води рачуна лице чији су подаци.

#### **2.4. Метаподаци као подаци о личности**

Метаподаци су саставни део података генерално и заједно творе јединствену целину. Метаподатке треба евидентирати приликом прикупљања личних података и потребно их је ажурирати када се подаци мењају. Односно, важније радње над личним подацима треба забележити кроз метаподатке. Метаподаци дају одговоре на питања повезана с извором података као што су: Ко је створио извор податка? Шта је садржај извора? Када је створен извор података? Које подручје обухватају подаци? Зашто су прикупљани? Како су подаци прикупљани?<sup>8</sup> У теорији и пракси, најраспрострањенија дефиниција је да метаподаци представљају податке о подацима. Свакако велики обрађивачи метаподатака јесу државне односно службе које брину о јавној безбедности, којима закон даје могућности да податке прикупљају и обрађују и без сагласности физичких лица, али уз поштовање унапред одређених сврха и у случају поштовања легитимних интереса за ту обраду. Такође, данашње највеће светске компаније попут Google-а или Facebook-а модел свог пословања заснивају управо на прикупљању и коришћењу мета податка корисника. Исти случај је и са многим другим платформама за бесплатну размену порука, блоговање, размену слика, видеа итд. Иако наизглед бесплатни сервиси, своје услуге наплаћују управо приватним подацима.<sup>9</sup> Примера ради, у мејл комуникацији метаподатком би се сматрала адреса пошиљаоца, адреса примаоца, наслов мејла, мејл сервис који је коришћен за размену мејла, али не и сама садржина мејла. Метаподаци нам такође говоре о датуму креирања податка, намени, значењу, аутору односно креатору, локацији рачунара на ком је креиран податак, коришћеним стандардима, величини фајла, квалитета, извора податка и процеса и метода коришћених код његове производње.

Све претходно наведене врсте података по својој правној природи представљају податке о личности. 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 кога се односе, док су у одређеним случајевима доступни повезаним лицима или широј друштвеној заједници.

---

<sup>8</sup>Жељко Хећимовић, *Метаподаци*, Свеучилиште у Сплиту, Факултет грађевинарства, архитектуре и геодезије, Катедра за геодезију и геоинформатику, Сплит, 2016. године, стр. 7;

<sup>9</sup><https://www.milic.rs/zastita-podataka-o-licnosti/> приступљено 27.09.2022. године;

### 3. ОБРАДА ПОДАТАКА О ЛИЧНОСТИ

Обрада података о личности је свака (аутоматизована или неаутоматизована) радња која се предузима у вези са подацима о личности, као што су прикупљање, бележење, чување, разврставање, увид, брисање, уништавање, похрањивање података и многе друге.<sup>10</sup> Аутоматизована обрада подразумева коришћење рачунара или других дигиталних уређаја који преко одговарајућег програма (софтвера) обрађују податке – обрада података у Microsoft Word-у на рачунару. Неаутоматизована обрада у ствари представља ручну обраду – преписивање података у свеску хемијском оловком. Иако реч „обрада“ асоцира на активно понашање, под обрадом података се могу подвести и пасивне радње, попут чувања и складиштења података. Намера законодавца је, дакле, да не затвара списак радњи које се могу сматрати радњама обраде података о личности, док набраја само најчешће и типичне радње обраде. Стога је потребно имати на уму да свако активно или пасивно понашање у вези са подацима о личности представља њихову обраду, па је тешко замислити ситуацију да је неко дошао у додир са подацима о личности, а да се то не сматра обрадом. Дакле, свака употреба или сваки додир са подацима о личности, без обзира на то колико је таква обрада трајала и какве је врсте била (активна или пасивна) се може сматрати обрадом података о личности у смислу Закона.

Главни актери у обради података о личности су свакако руковалац и обрађивач. Руковалац је физичко или правно лице, односно орган власти који самостално или заједно са другима одређује сврху и начин обраде, а обрађивач је физичко или правно лице, односно орган власти који обрађује податке о личности у име руковаоца.<sup>11</sup> Свако ко обрађује податке о личности, мора најпре да утврди да ли се у односу на конкретну обраду јавља у улози руковаоца, заједничког руковаоца или обрађивача. У пракси се често дешава да се исти ентитет у односу на једну групу података јавља као руковалац, а у односу на другу као обрађивач. Због тога је потребно испитати улоге у односу на сваку конкретну обраду и категорију података о личности који се обрађују. Током утврђивања улога, у обзир се узимају све околности конкретног случаја, али се најпре утврђује ко одређује сврху обраде података - одговор на питање “Зашто се подаци обрађују?” - и начин обраде података.<sup>12</sup> Примера ради, комунално предузеће ангажује предузеће које управља позивним центром, да у име и за рачун комуналног предузећа

---

<sup>10</sup>Ор. Cit. Чл. 4 ст. 1 тач. 3, Закон о заштити података о личности;

<sup>11</sup>Ibid. Чл. 4 ст. 1 тач. 8 и 9;

<sup>12</sup>Ор. Cit., Д. Кривокапић, Ј. Адамовић, Д. Тасић, А. Петровски, П. Калезић, Ђ. Кривокапић, стр. 27;

обавља многе функције његове корисничке службе. Запослени у позивном центру имају приступ евиденцијама о корисницима услуга комуналног предузећа за потребе пружања услуга за које су ангажовани, али те податке могу да користе само у конкретне сврхе и у складу са строгим уговорним аранжманима. Комунално предузеће је и даље руковалац података. Предузеће које управља позивним центром је обрађивач података.<sup>13</sup> Руковалац је, дакле, главно одговорно лице за обраду података о личности. Ова одговорност осликава се и у односу руковоаца и обрађивача, где обрађивач мора да поступа у свему према налозима руковоаца, што треба да буде уређено обавезним уговором између ових лица. Одговорност руковоаца подразумева и обавезу сношења последица у случају злоупотребе података о личности или повреде одредаба Закона о заштити података о личности, путем прекршаја, кривичних дела или института накнаде штете. Наравно, уколико је за штету крив обрађивач, руковалац ће моћи да се регресира по правилима одштетног права.

Примери руковалаца: привредно друштво или предузетници који обрађују податке о својим радницима, финансијске организације које обрађују податке о личности својих радника, странака и клијената, школе или факултети који обрађују податке о личности ученика, студената или наставника и других радника, болнице које обрађују податке о личности својих пацијената, државни органи који обрађују податке о личности грађана, итд.

Примери обрађивача: служба рачуноводства која обрађује податке о платама радника за друго привредно друштво или предузетника, привредна друштва овлашћена за обављање послова безбедности, сервиси за наплату потраживања, пружаоци неких информатичких услуга, итд.

Не треба заборавити још једног важног актера у процесу обраде података о личности, а то је лице чији се подаци прикупљају и обрађују. Дакле, Да би један податак представљао податак о личности, он се мора односити на физичко лице. Уз то, није довољно да се ради о било ком лицу, већ подаци морају упућивати на тачно одређено или одредиво физичко лице. Овим лицима Закон о заштити података о личности приписује широк корпус права када је у питању заштита личних података и процес обраде истих међу којима су право на обавештеност, право на приступ, право на

---

<sup>13</sup>Клеменч Мишич, Маја Лубарда, *Заштита података – приручник за руковоаце, Повереник за информације од јавног значаја и заштиту података о личности Републике Србије, Београд 2012. године, стр.12.*

исправку, право на заборав, право на ограничење обраде, право на пренос, право на приговор и права у вези са аутоматском обрадом података.<sup>14</sup> 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). Правним лицима се гарантује правни субјективитет, али им није омогућена заштита података о личности у поменутих прописима.

## 4. ЗАКОНОДАВНИ ОКВИР

### 4.1. Међународно право

Када говоримо о законодавној регулативи на међународном плану, оно што је вредно помена јесте најпре Европска конвенција за заштиту људских права и основних слобода<sup>15</sup> а коју је Република Србија ратификовала 2003. године<sup>16</sup>, која чланом 8 прописује да сва лица уживају заштиту у погледу обраде података о личности у оквиру заштите права на приватни и породични живот, као и права на неповредивост приватности и тајност личне комуникације. Дакле, област заштите података о личности није експлицитно регулисана Конвенцијом, већ се установљеном судском праксом посредно штити кроз право на приватност. Даљи допринос успостављању правног оквира заштите података о личности дала је Конвенција о заштити лица у односу на аутоматску обраду личних података Савета Европе из 1981. године (ратификована у Србији 2005. године)<sup>17</sup>. Ова је Конвенција у међувремену значајно осавремењена Протоколом о допуни Конвенције из 2018. (ратификована је 5. марта 2020. године), а који је ускладио вредности Конвенције са модерним концептима и појмовима права

---

<sup>14</sup>Ор. Cit. Чл. 21-41, Закон о заштити података о личности;

<sup>15</sup>[https://www.echr.coe.int/Documents/Convention\\_MNE.pdf](https://www.echr.coe.int/Documents/Convention_MNE.pdf) приступљено 28.09.2022.. године;

<sup>16</sup>Закон о ратификацији Европске конвенције за заштиту људских права и основних слобода, измењене у складу са протоколом број 11, протокола уз Конвенцију за заштиту људских права и основних слобода, протокола број 4 уз Конвенцију за заштиту људских права и основних слобода којим се обезбеђују извесна права и слободе који нису укључени у конвенцију и први протокол уз њу, протокола број 6 уз Конвенцију за заштиту људских права и основних слобода о укидању смртне казне, протокола број 7 уз Конвенцију за заштиту људских права и основних слобода, протокола број 12 уз Конвенцију за заштиту људских права и основних слобода и протокола број 13 уз Конвенцију за заштиту људских права и основних слобода о укидању смртне казне у свим околностима ("Сл. лист СЦГ - међународни уговори", бр. 9/2003, 5/2005 и 7/2005 - испр. и "Сл. гласник РС - међународни уговори", бр. 12/2010 и 10/2015);

<sup>17</sup>Закон о потврђивању Конвенције о заштити лица у односу на аутоматску обраду личних података ("Сл. лист СРЈ - међународни уговори", бр. 1/92, "Сл. лист СЦГ - међународни уговори", бр. 11/2005 - др. закон и "Сл. гласник РС - међународни уговори", бр. 98/2008 - др. закон и 12/2010);

заштите података о личности, посебно под утицајем новог законодавства Европске уније.<sup>18</sup> У праву Европске уније заштита података о личности је препозната и као посебно основно право, регулисано чланом 8. Повеље Европске уније о основним правима (ПОПЕУ), којим је уређено да се подаци о личности морају обрађивати на поштен начин, у за то утврђене сврхе и на темељу законитог основа.<sup>19</sup> ПОПЕУ предвиђа да се лицима чији се подаци обрађују морају гарантовати право на приступ прикупљеним подацима који се на њих односе и право на исправку података, док подаци морају бити обрађени у складу са законом за тачно одређене сврхе и на основу пристанка лица чији се подаци обрађују или неког другог легитимног основа утврђеног законом, као и да надзор над поштовањем тих права има независно надзорно тело. Уз право на заштиту података о личности, Повеља предвиђа и право на приватност и породичног живота (члан 7).

Заштита података о личности на међународном нивоу је експлицитно регулисана 1995. године путем тзв. Data Protection Directive, односно Директивом о заштити података о личности 95/46/ЕЦ.<sup>20</sup> Директива 95/46/ЕЦ о заштити појединаца у погледу обраде личних података и о слободном кретању таквих података донета је од стране Европског парламента и Савета и усвојена је 24. октобра 1995. године. Основни циљ доношења овог документа био је да се обезбеди заштита личних података у државама чланицама како би могао да се осигура слободан проток информација. Већ се у члану 6 Директиве помињу начела обраде података о личности и наводе се значајна ограничења, јер је између осталог, прописано да лични подаци морају бити адекватни, релевантни и не претерани за сврхе за које се прикупљају и/или даље обрађују, да се ажурирају и чувају не дуже него што је потребно, док се у члану 7 прописују законом дозвољени основи обраде личних података. Овај правни документ се није примењивао директно на државе чланице, те је било неопходно да државе чланице овакву идеју о заштити података имплементирају у домаће законодавство. Због брзог технолошког развоја, Европска унија је 2016. године заменила Директиву новим законодавним оквиром када је усвојила Општу Уредбу 2016/679, која је ступила на снагу 25. маја 2018. године, познату под називом Општа уредба о заштити података (General Data

---

<sup>18</sup>*Protocol amending the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108);*

<sup>19</sup>*Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012; Consolidated version of the Treaty on the Functioning of the European Union, OJ C 326, 26.10.2012;*

<sup>20</sup>*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;*

Protection Directive), опште познату по скраћеници GDPR.<sup>21</sup> Решења садржана у Општој уредби представљају наставак политике на којој је заснована Директива, с тим што се, после двадесетогодишње праксе њене примене, одређена решења осавременују и уводе се нова, да би се повећала правна сигурност појединаца у вези са обрадом њихових података, како би дошло до јачања поверења у руковоце и обрађиваче података и до несметаног кретања података на традиционалном, као и на дигиталном тржишту, од чега би, повратно, корист имали и сами руковоци и обрађивачи података, у виду бољих пословних резултата.<sup>22</sup> Слично као и у горе поменутој Директиви, и ГДПР у члану 6 дефинише законитост обраде података о личности, и наводи законом дозвољене основе за обраду података о личности прокламујући да ће обрада бити законита уколико се заснива на пристанку, извршењу или закључењу уговора, поштовању правних обавеза руковоца, заштити животно важних интереса, обављању послова у јавном интересу или извршењу законом прописаних овлашћења или остваривању легитимних интереса руковоца.

Може се рећи да конкретна Уредба тј. ГДПР на један свеобухватан начин регулише област заштите података и личности и представља један савремени правни документ по основу ког је донет и наш Закон о заштити података о личности, о коме ће у наставку бити речи.

#### **4.2. Национално законодавство**

Развој технологије, све већа употреба података у различитим областима друштвеног живота и, посебно, нормативна дешавања на европском тлу, условила су и нормативну реакцију Србије у вези са заштитом података о личности. Први Закон о заштити података о личности усвојен је у Србији 1998. године. Трагом развоја демократских стандарда гаранције и заштите људских права, укључујући приступање конвенцијама Савета Европе, Република Србија је 2008. заштиту података о личности загарантовала Уставом (члан 42), као и Законом о заштити података о личности из исте године.<sup>23 24</sup> Тај се закон примењивао у периоду од 2008. до средине 2019. године, оставивши значајан траг у разумевању података о личности и њиховој заштити, посебно кроз праксу надзорног органа – Повереника. Под утицајем права ЕУ и ради усклађивања са

---

<sup>21</sup>General Data Protection Regulation, (EU) 2016/679;

<sup>22</sup><https://www.poverenik.rs/images/stories/dokumentacija-nova/prirucnik/GDPROA.pdf>

приступљено

28.09.2022. године;

<sup>23</sup>Устав Републике Србије («Службени гласник РС» бр. 98/2006, 16/2022) – Одлука о проглашењу Уставног закона за спровођење Акта о промени Устава Републике Србије - Амандмани I - XXIX - "Сл. гласник РС", бр. 115/2021);

<sup>24</sup>Ор. Cit., Закон о заштити података о личности;

европским законодавством правни оквир заштите података о личности доживео је у претходном периоду велике измене у односу на време примене старог ЗЗПЛ из 2008. године. Нови Закон о заштити података о личности донет је 2018. године, ступио је на снагу 21. новембра 2018. године, а у примени је од 21. августа 2019. године.<sup>25</sup> Овај закон представља значајан искорак у области заштите података и у потпуности је усклађен са европском реформом и новом Уредбом 2016/679 (ГДПР). ЗЗПЛ је на савремен начин, у складу са релевантном европском праксом, уредио оквир заштите физичких лица у вези са обрадом података о личности и слободним кретањем таквих података. Закон је експлицитно дефинисао водећа начела обраде података о личности, права лица на која се подаци односе и начине на које они могу да остварују та права, обавезе руковалаца и обрађивача података о личности, пренос података о личности у друге државе и међународне организације, као и надзор који је поверен институцији Повереника за информације од јавног значаја и заштити података о личности. У односу на ранији правни режим, ЗЗПЛ проширено дефинише правна средства, одговорност и казне у случају повреде права физичких лица у вези са обрадом података о личности, као и посебне случајеве обраде података о личности. Када говоримо конкретно о законом дозвољеним основама обраде података о личности, а што је и главна тема овог рада, исти су регулисани чланом 12 актуелног Закона о заштити података о личности. У овом члану, у ставу првом, прописује се да ће обрада бити законита уколико се заснива на пристанку, извршењу или закључењу уговора, поштовању правних обавеза руковоца, заштити животно важних интереса, обављању послова у јавном интересу или извршењу законом прописаних овлашћења или остваривању легитимних интереса руковоца, док се у трећем ставу предвиђа један изузетак односно предвиђа се да се наведени основи не примењују на обраду коју врше надлежни органи у посебне сврхе. Обрада коју врше надлежни органи у посебне сврхе је законита само ако је та обрада неопходна за обављање послова надлежних органа и ако је прописана законом. Таквим законом се одређују најмање циљеви обраде, подаци о личности који се обрађују и сврхе обраде. Претхоно наведене одредбе домаћег ЗЗПЛ представљају дословце преписане одредбе важећег ГДПР-а.

Недостаци домаћег Закона о заштити података о личности односе се, пре свега, на нејасне одредбе и преписане механизме из ГДПР-а који не постоје у домаћем правном систему, што у одређеним ситуацијама може довести у питање његову примељивост.

---

<sup>25</sup>Ор. Cit., Закон о заштити података о личности;

Поједина питања нису уређена на истоветан начин, па су остале правне празнине које треба попунити и питања на које треба дати одговор. На првом месту, Закон о заштити података о личности не садржи преамбулу као Општа уредба ЕУ, што значи да не постоји ни законска разрада основних принципа, права грађана и института, од којих су многи први пут нашли место у домаћем правном систему. Постављене су знатно блаже санкције него што је то случај у Општој уредби ЕУ, а јављају се и питања у вези са начином примене санкција. Важно питање видео надзора није добило пажњу у овом законском тексту. Осим тога, потребно је уредити и бројна питања у посебним областима, као што је примена одредаба овог закона од стране органа јавне управе.<sup>26</sup> Ипак, значајно је напоменути да овакав закон свакако представља највиши стандард заштите података о личности у Републици Србији. Такође, доношењем овог закона први пут у историји Србије успоставља се темељан систем заштите података који је постављен као штит приватности грађана, преко којег се бране и друга људска права и слободе.

## 5. ОСНОВНА НАЧЕЛА ОБРАДЕ ПОДАТАКА О ЛИЧНОСТИ

Свака грана права заснива се на принципима, односно вредностима које представљају „извор“ из кога произлазе конкретна правила понашања. Ти принципи у законодавству представљају апстрактна правила понашања и обично се одређују као начела, односно апстракта правна правила из којих произлазе конкретна правила. Основна начела обраде података о личности у домаћем правном систему су садржана у члану 5 ЗЗПЛ-а и то су:

*1. Начело законитости, поштења и транспарентности* које предвиђа да подаци могу да буду обрађивани само уколико постоји одговарајући правни основ за конкретну обраду и уз поштовање свих прописа који се на ту обраду примењују, да руковоаци морају увек имати у виду и интересе лица чије податке обрађују и понашати се поштено у конкретним околностима, у зависности од тога чије податке прикупљају и да од момента када започне прикупљање, лице чији се подаци обрађују у сваком тренутку има право да зна како се са њима поступа – што укључује право да буде упознато са чињеницом да се подаци обрађују, у којој мери, за које сврхе, ко је руковалац и ко су обрађивачи, и слично, а те информације треба да буду саопштене на јасан и разумљив начин.

---

<sup>26</sup>*Op.cit., Стефан Андоновић, Драган Прља, стр. 150;*

2. *Начело ограничења у односу на сврху обраде* које се у суштини састоји од два основна захтева: да се пре започињања обраде прецизно дефинише и изричито објасни због чега се подаци прикупљају, као и да се подаци прикупљени за иницијалну сврху не могу даље обрађивати за било коју другу, некомпатибилну сврху. Начело ограничења у односу на сврху обраде иде за тим да спречи самовољно и непотребно коришћење туђих података, већ да се обрада врши са неким циљем који правни систем препознаје као адекватан за коришћење туђих података. Практично, начело ограничења у односу на сврху обраде значи то да се прикупљање података о личности може вршити само на основу законом предвиђених разлога. Руковалац и обрађивач могу предузети радње обраде само у односу на одређене, изричите и оправдане сврхе. Прикупљање података без одређене сврхе је противправно. Када се укаже потреба за обрадом, руковалац мора тачно одредити из ког разлога се подаци прикупљају и обрађују. Одређеност сврхе значи да руковоаоци и обрађивачи врше делатности у вези са којима су им потребни подаци о личности. Подаци о личности не могу се прикупљати пре него што се јави потреба за њиховом обрадом. Изричитост указује на то да лица чији се подаци обрађују морају на јасан и разумљив начин бити упозната са сврхом обраде. Поред тога, изричитост подразумева и забрану сакривања разлога због којих се подаци о личности обрађују, што имплицира да руковоаоци и обрађивачи не могу давати апстрактне и неодређене разлоге за прикупљање и обраду података о личности. Оправданост значи да стварно, објективно постоји потреба руковоаоца и обрађивача за прикупљањем и обрадом података о личности грађана, која се заснива на законским прописима.

3. *Начело минимизације података о личности* које указује да лични подаци који се прикупљају морају бити ограничени само на оно што је неопходно за конкретну сврху обраде, односно морају бити примерени и релевантни баш за ту сврху. Руковалац или обрађивач немају право да постављају непримерене захтеве грађанима у вези са прикупљањем и обрадом података о личности, тако да они превазилазе разлоге због којих су прикупљени и сврху због које се обрађују. Када постоји потреба за обрадом података о личности, они могу тражити и користити само оне податке о личности који су од суштинске важности за остваривање законитог циља обраде. Члан 5 ст. 1 тач. 3 ЗЗПЛ предвиђа да подаци о личности који се обрађују морају бити примерени, значајни и ограничени на оно што је неопходно утврдити у односу на сврху обраде.<sup>27</sup> Појам примерености односи се на границу довољне количине података о личности која

---

<sup>27</sup>Ор. Cit., чл. 5, Закон о заштити података о личности;

омогућава остваривање претходно утврђене сврхе обраде. Значај, односно релевантност података подразумева неопходну везу између података о личности 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 незаконита. Изостављање неког од наведених елемената значило би повреду начела коришћења најмањег могућег обима података.

4. *Начело потпуности и тачности* које практично захтева од руковалаца педантност у обради личних података. Подаци који се користе у обради морају бити тачни и, када за тим постоји потреба, усклађени са евентуалним променама. Имајући у виду сврхе за које се подаци обрађују, руковалац мора да обезбеди да нетачни подаци буду без одлагања обрисани или исправљени. Подаци се могу сматрати нетачним и у ситуацијама када су непотпуни или када су извучени из контекста. У пракси, ово начело треба да буде примењено тако да руковооци и обрађивачи предузму све потребне и одговарајуће мере које омогућавају тачност и истинитост података о личности који се обрађују.

5. *Начело ограниченог чувања података о личности*, које изискује да се лични подаци смеју чувати у облику који омогућава идентификацију физичких лица само онолико дуго колико је неопходно за испуњење сврхе за коју се подаци обрађују. Ово начело у себи садржи две компоненте: најпре обавезу да се унапред одреди период чувања података, у зависности од сврхе обраде, при чему тај период мора бити неопходан за испуњење сврхе, тј. мора постојати рационално и убедљиво образложење зашто сврха не може бити остварена у краћем року, и након тога брисање или анонимизацију података (тако да више није могућа идентификација) после истека тог периода. Ово начело поставља временске границе чувања података искључиво на време које је заиста потребно да се оствари циљ обраде. Када је испуњена сврха ради које су подаци прикупљени и обрађени, нестаје и потреба за чувањем података, односно губи се основ обраде.

6. *Начело интегритета и поверљивости*, које прокламује да се подаци о личности морају обрађивати на начин који обезбеђује одговарајућу заштиту података о личности, укључујући заштиту од неовлашћене или незаконите обраде, као и од случајног губитка, уништења или оштећења применом одговарајућих техничких, организационих и кадровских мера. Наведене мере нису изричито дефинисане било којим позитивним

прописом, јер оне увек зависе од конкретне ситуације и од читавог низа фактора, као што су: која врста и количина података је у питању, која је сврха обраде, колико дуго и на који начин се подаци чувају, у којим системима, и слично. Приликом обраде података о личности, руковоаоци и обрађивачи могу доћи до значајних информација о животу појединца чије податке обрађују. Уколико би ти подаци били изгубљени, уништени или злоупотребљени од стране трећих лица, могле би настати значајне негативне последице по права и интересе лица чији се подаци обрађују, али и њему блиских лица.

*7. Начело одговорности руковоаоца за поступање у вези са подацима о личности* које практично значи да је терет на руковоаоцу да обезбеди примену свих шест начела у својој организацији, односно да мора бити у могућности да докаже своју усклађеност. Ова одговорност заснива се на односу одговорности са лицем чији се подаци обрађују, али и на односу према целокупној друштвеној заједници и јавном поретку. На тај начин се заштитом података о личности штите универзалне друштвене вредности и целокупни правни системи. Руковалац мора у потпуности да усклади своје пословање са општим прописима који уређују заштиту података и прописима који се односе на област његових делатности. Последично, руковалац мора 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 података. Принцип одговорности подразумева и дужност руковоаоца да континуирано води рачуна о подацима грађана. Практичан аспект овог начела се огледа у томе да би руковоаоци требало да документују све своје одлуке у вези са применом ЗЗПЛ начела. Таква документа могу да укључују одговарајуће политике приватности или политике заштите личних података, које су се у пракси показале врло корисним иако Закон не намеће обавезу њиховог доношења.

## **6. ЗАКОНИТОСТ ОБРАДЕ ПОДАТАКА О ЛИЧНОСТИ**

Када говоримо о законитости обраде личних података, у суштини говоримо о томе да руковалац има право да врши обраду личних података само уколико је она утемељена, заснована на једном од шест расположивих правних основа. Другим речима, када руковалац одреди за коју су му сврху подаци потребни, руковалац мора да се одлучи на основу ког правног основа ће се обрада вршити – јер правила обраде у великој мери од тога зависе. Ако обрада за жељену сврху не може да се заснује ни на једном од расположивих правних основа, онда је таква обрада недозвољена, односно

незаконита. Такође треба нагласити да ниједан од правних основа није “јачи” или “бољи” од других, већ се за основ обраде личних података бира онај основ који највише одговара конкретној сврси пре почетка обраде.

Да би обрада података о личности била законита, она се мора заснивати на једном од неколико законом предвиђених основа. Обрада ће бити законита уколико се заснива на:

1. Пристанку
2. Извршењу или закључењу уговора,
3. Поштовању правних обавеза руковоаца,
4. На заштити животно важних интереса,
5. Обављању послова у јавном интересу или извршењу законом прописаних овлашћења,
6. Остваривању легитимних интереса руковоаца.

### 6.1. Пристанак

Обрада података о личности има законит карактер и основ ако се заснива на пристанку лица чији се подаци о личности обрађују. Пристанак се одређује као свако добровољно, одређено, информисано и недвосмислено изражавање воље којим то лице, изјавом или јасном потврдном радњом, даје пристанак за обраду података о личности који се на њега односе.<sup>28</sup> Дакле, да би пристанак био пуноважан мора да испуњава неколико услова.

Прво, пристанак мора да буде **добровољан односно да буде дат слободно**. Сваки пристанак који је дат под принудом или због употребљене силе, не производи правно дејство и може се побијати пред судом због недостатка воље на страни даваоца. Уколико дође до испитивања да ли је пристанак слободно дат, посебно у пословним односима, мора се обратити пажња да ли је извршење уговора или пружање услуге било условљено давањем пристанка који није неопходан за његово извршење.<sup>29</sup>

Даље, пристанак мора да буде **одређен**. То значи да се мора односити на конкретну обраду (иако се у оквиру радње обраде може предузети више повезаних делатности у циљу извршења обраде), одређене податке или врсте података и конкретну сврху обраде. Информисано давање пристанка значи да лице које даје пристанак мора да буде у потпуности упознато да потписом одређеног документа (писмена) даје сагласност за

---

<sup>28</sup>*Ibid.*, чл. 4 ст. 1 тач. 12;

<sup>29</sup>*Ibid.*, чл. 15 ст. 4;

обраду својих података о личности. Дакле, информисан је, лице чији ће се подаци прикупати и обрађивати разуме на шта пристаје, има све потребне информације од руковоаца да би могло да донесе информисану одлуку. Евентуално „сакривање“ сагласности у оквиру правила пословања или другог документа у вези са којим се обрађују подаци, не може се сматрати за информисано давање сагласности. Дакле, сагласност мора да буде дата у посебном документу за пристанак или у оквиру документа која се односи на друга питања, али само ако је захтев за давање пристанка лако уочљив, јасно се издваја од осталих одредби, односно питања.<sup>30</sup> У сваком случају, у документу у коме је потребно дати пристанак, неопходно је користити разумљив стил, уз употребу јасних и једноставних речи који упућују на давање сагласности.<sup>31</sup> То значи да просечан човек може да разуме да потписом на документу даје другом лицу могућност да преузме и користи његове податке о личности.

Пристанак такође треба да представља **недвосмислено изражавање воље** које значи да сагласност мора да буде јасно постављена и представљена даваоцу сагласности, без могућности да се сагласност крије под другим називима или документима. Сагласност се даје јасном и прецизном изјавом воље даваоца сагласности да пристаје на обраду тачно одређених података о личности у тачно одређену сврху. Дакле, овде не треба да постоје непознати елементи који се односе на неодређеност података или разлога због којих се обрађују. Јасно изражене потврдне радње у случају немогућности писаног давања сагласности остварују правне последице давања сагласности. Примера ради, овде може бити реч о давању отисака прста уколико је давалац сагласности неписмен.

Уколико постоји више сврха на које је потребно да лице пристане, пристанак мора бити **гранулиран**, што значи да јасан пристанак треба да се да за сваку појединачну сврху.

Пристанак мора бити дат **безусловно**. По својој правној природи, пристанак на обраду података о личности представља строго личну изјаву воље, будући да је може дати само физичко лице на које се подаци односе или за то посебно овлашћено лице. Пристанак на обраду података о личности мора се дати без тражења против услуге, што значи да није условљен прихватањем других услуга или услова (на пример, није спојен са прихватањем целокупних услова пословања). Како се изјава воље о обради података

---

<sup>30</sup>Ор. Cit., Стефан Андоновић, Драган Прља, стр. 58;

<sup>31</sup>Ор. Cit., чл. 15 ст. 2, Закон о заштити података о личности;

може изјавити на различите начине (писменим или електронским путем), реч је о неформалном правном послу.

Закон о заштити података о личности не садржи експлицитну одредбу о формама у којима се пристанак може дати. Ипак, како руковалац или обрађивач морају, када се за то укаже потреба, да буду у могућности да предоче пристанак лица чији се подаци обрађују то значи да пристанак мора бити **документован**, односно да мора бити у писаном или електронском облику, ради касније могућности коришћења као доказа.

Још једна битна катаактеристика пристанка јесте да представља **опозиву изјаву воље**. Основно је правило да пристанак може да траје до опозива. Опозив пристанка на обраду података о личности може се дати у сваком тренутку, а упућује се руковоаоцу. Опозив се мора дати у јасном и једноставном облику, на истоветан начин на које се пристанак може дати. Подразумева се да опозив не повлачи за собом ништавост радњи обраде које су учињене пре давања опозива, јер би се на тај начин нарушила концепција обраде података о личности која се заснива на пристанку. Није оправдано отежавати повлачење пристанка додатним формалностима, на пример попуњавањем формулара или позивањем одређених служби, ако је пристанак дат мејлом.<sup>32</sup> Закон о заштити података о личности не одређује временско трајање датог пристанка. Овај закон једино предвиђа право лица које је дало пристанак на обраду да има могућност опозива у сваком тренутку.<sup>33</sup> У теорији влада став да би адекватно решење ове правне празнине било да се пристанак временски ограничи на одређени временски период (1 или 2 године) након чега би руковалац, односно обрађивач био дужан да поново добије пристанак, односно да добије продужење пристанка. Након престанка овог периода, пристанак би аутоматски требало да престане да важи, уколико се не продужи. Сматра се да би се на тај начин избегле негативне последице неограниченог трајања пристанка, а руковоаци и обрађивачи имали би дужност пажљивог поступања са подацима грађана.

Малолетна лица уживају посебну заштиту у вези са њиховим подацима о личности због њиховог степена зрелости и могућности да сагледају опасности и ризике који се јављају код употребе интернета, друштвених мрежа и њихових података. С једне стране, деца и млади се посматрају као дигитална генерација, пионери у развијању дигиталне компетенције, док, с друге стране, посматрају се као рањива група корисника

---

<sup>32</sup>Ор. Cit., Д. Кривокапић, Ј. Адамовић, Д. Тасић, А. Петровски, П. Калезић, Ђ. Кривокапић, стр. 42;

<sup>33</sup>Ор. Cit., чл. 15 ст. 3. Закон о заштити података о личности;

интернета која је у потенцијалном ризик.<sup>34</sup> Ова чињеница се одражава и на могућност давања пристанка на обраду таквих података. Дакле, посебна правила о давању пристанка важе ако су даваоци деца, тј. малолетна лица. Одређена посебна правила из ЗЗПЛ-а односе се само на обраду података о деци у вези са услугама информационог друштва. Ако руковалац обрађује податке лица млађих од 15 година у том контексту, онда ће обрада њихових података бити законита само ако је пристанак дало лице које је носилац родитељске одговорности над дететом (обично родитељи). Ако је лице старије од 15 година, пристанак може дати самостално. Стога би руковаоци који пружају услуге које су у вези са услугама информационог друштва, требало да успоставе механизме који омогућавају да се утврди да је свако лице које даје свој пристанак довољно старо да има право то да учини (без потребе да се утврди тачна старосна доб). У зависности од ризика који се односе на обраду података, ова верификација се може урадити једноставно, тражењем изјаве да је корисник довољно стар да обезбеди сопствени пристанак или, у неким случајевима, коришћењем услуге верификације треће стране. У сваком случају, уколико пристанак дају малолетна лица, текст пристанка треба да буде посебно прилагођен њиховом узрасту.

Пристанак мора да се даје јасном потврдном радњом којом се изражава добровољан, конкретан, информисан и недвосмислен пристанак лица на које се подаци односе на обраду који се односе на њега, као што је писана изјава (укључујући и електронску изјаву) или изјава у усменој форми. Иако закон укључује усмену форму, као законит начин прибављања пристанка, треба имати у виду проблем са евентуалним доказивањем, па се због тога овај вид форме не препоручује.

Давање пристанка може да обухвата штиклирање поља приликом посете интернет странама, попуњавање посебног обрасца за давање пристанка, бирање техничких подешавања за услуге информационог друштва или другу изјаву или радњу којом се јасно показује у том контексту да лице на које се подаци односе прихвата предложеноу обраду својих података о личности.

Пристанак неће бити законито прибављен уколико:

- је држање корисника пасивно односно уздржано;

---

<sup>34</sup>Зуковић Слајана, Слијепчевић Сенка, „Родитељска контрола понашања деце на интернету и социјалним мрежама“, у *Настава и васпитање*, бр. 64/2, Педагошко друштво Србије и Институт за педагогију и андрагогију Филозофског факултета Универзитета у Београд, Београд 2015. године, стр. 241-242;

- уколико је поље за означавање пристанка у електронској форми унапред штиклирано;
- постоји јасна неравнотежа у односу странака (посебно уколико је једна страна орган власти);
- нема истинског и слободног избора;
- ако је немогуће одбити или повући пристанак без последица;
- ако би се и даље обрађивали подаци на другачијој законитој основи ако је пристанак одбијен или повучен;
- уколико се тражи „пристанак“ на обраду података као предуслов за приступање услугама.<sup>35</sup>

## 6.2. Закључење и извршење уговора

Приликом преговора око закључења или код извршења уговора углавном се јавља потреба једне од уговорних страна да обради податке о личности друге уговорне стране. Ради безбедности и убрзања пословног промета предвиђено је да је законита она обрада података о личности која је неопходна у циљу извршења уговора или предузимања радњи које воде ка закључењу уговора.<sup>36</sup> Дакле, није довољно да постоји било каква потреба за обрадом података у циљу извршења уговора. Услов за закониту обраду јесте да је таква обрада података о личности неопходна. То значи да је код неких уговора могуће извршити уговор, а да се не обрађују подаци о личности, па у тим ситуацијама не постоји ни основ за закониту обраду. Пример за такав уговор би била свакодневна куповина основних животних намирница у продавници. Док са друге стране, као пример законите обраде података о личности у циљу извршења уговора може се навести уговор о купопродаји путем интернета. Код овог уговора, будући да се продавац и купац физички не налазе на истом месту, купац мора да остави поједине личне податке како би се извршила достава попут имена, презимена, адресе становања и контакт телефона. У овом случају, јавља се потреба за обрадом података у циљу извршења уговора. Код овог основа обраде личних података мора се водити рачуна да су подаци заиста неопходни тј. сама чињеница да су подаци дати у уговорном контексту не значи да руковалац по овом основу може да користи све податке до којих је дошао. Због тога се ово не би могло сматрати одговарајућим правним основом за продавца који хоће да профилише своје купце на основу постојећих куповина и да им

<sup>35</sup><https://dataprivacymanager.net/pristanak-kao-uslov-za-obradu-podataka-o-licnosti/> приступљено дана 01.10.2022. године;

<sup>36</sup>Ор. Cit., Д. Кривокапић, Ј. Адамовић, Д. Тасић, А. Петровски, П. Калезић, Ђ. Кривокапић, стр. 41;

шаље нове промотивне понуде са циљем директног маркетинга, иако је до података дошао преко уговора. Подаци које је руковалац прикупио на основу уговорног услова не могу се користити у маркетиншке или друге сврхе. Такође, ЗЗПЛ експлицитно наводи да мора да се ради о уговору баш са лицем чији се подаци обрађују. Дакле, овај правни основ се не може користити ако се ради о извршавању уговора са неким трећим лицем. Међутим, пошто ЗЗПЛ не наводи да уговорна страна мора бити сам руковалац, може се закључити да се овај правни основ може користити и ако руковалац обрађује личне податке у циљу извршавања уговора између лица на које се подаци односе и неког трећег лица. Пример за то би могао да буде уговор са посредницима код промета непокретности као што су на пример агенције за промет некретнина.

### **6.3. Поштовање правних обавеза**

Поред поштовања уговора, Закон као посебан основ предвиђа поштовање правних обавеза које има руковалац. Иако је термин “правне обавезе” поприлично неодређен, уз ослањање на тумачење правила из ГДПР-а може се закључити да се овде заправо ради о обавезама руковаоца да поштује позитивне прописе који се на њега примењују.<sup>37</sup> Дакле, у одређеним ситуацијама, руковалац има дужност да достави податке о личности органу јавне власти или другом лицу. Таква дужност се јавља као последица потребе за нормалним и ефикасним одвијањем друштвених, правних и привредних токова. Сходно томе, законита је свака обрада података о личности која је неопходна у циљу поштовања правних обавеза руковаоца. Суштински, то значи да руковалац мора да предузме неку радњу обраде података, како би са друге стране испунио правну обавезу према другом лицу. Примера ради, Закон о спречавању прања новца и финансирања тероризма, као једну врсту мере за спречавање и откривање прања новца и финансирања тероризма, предвиђа достављање информација, података и документације Управи за спречавање прања новца.<sup>38</sup> Обвезници према овом закону јесу банке, овлашћене мењачнице, брокерско-дилерска друштва, платне институције, посредници у промету непокретности, предузетници и правна лица која се баве пружањем рачуноводствених услуга, порески саветници и многи други. Како је у овом случају законом конституисана обавеза достављања података, међу којима се могу наћи и подаци о личности, постоји и законит правни основ за обраду таквих података. Такође, чланом 9 Закона о евиденцијама и обради података у области унутрашњих послова прописана је обавеза Министарства унутрашњих послова за разменом података са

<sup>37</sup>*Op. Cit., article 6, General Data Protection Regulation;*

<sup>38</sup>*Закон о спречавању прања новца и финансирања тероризма, („Сл. гласник РС“, бр. 113/2017, 91/2019);*

државним органима, органима аутономних покрајина, јединицама локалне самоуправе, имаоцима јавних овлашћења и правним лицима, али и физичким лицима на основу образложеног писменог захтева који мора да садржи податке о подносиоцу захтева (име и презиме, ЈМБГ, име једног родитеља, датум и место рођења, пребивалиште и адресу и податке за контакт), прецизно наведену сврху коришћења података, правни основ и врсту, односно количину података која је неопходна за опредељену сврху.<sup>39</sup> Ако руковалац мора да обрађује неке податке зато што се то од њега захтева према неком другом пропису, онда је овај основ ваљан уколико се лични подаци обрађују само у мери у којој пропис то налаже. У том случају, када се обавеза не заснива на праву Републике Србије, већ на одредбама страног права, потребан је одговарајући међудржавни споразум или одлука домаћег органа о признању и извршењу стране одлуке, како би такав основ био законит и у Републици Србији.

#### **6.4. Заштита животно важних интереса**

Обрада података о личности има законит карактер када је неопходна да би се заштитио важан интерес лица на које се подаци односе или другог физичког лица. Неопходан услов јесте угроженост животно важног интереса физичких лица. Подаци о личности могу носити информацију о одређеној околности или чињеници која може спасити живот одређеног лица. Генерално говорећи, у питању су заправо ситуације живота и смрти. Примера ради, обрада је неопходна за надгледање епидемија и њихово ширење, или у случајевима хуманитарних кризних ситуација, у ситуацијама природних катастрофа и катастрофа узрокованих људским деловањем.<sup>40</sup> Стога ће на овај основ по правилу моћи да се ослоне државни органи који имају одређене специфичне надлежности у оваквим ситуацијама или организације са јавним овлашћењима. Круг осталих потенцијалних руковалаца ће бити много мањи. Интересантан случај се десио и у Републици Србији током пандемије корона вируса, када је на снази била мера ограничења кретања у смислу боравка у угоститељским објектима. Наиме, да би било које лице могло да борави у неком угоститељском објекту у одређеном периоду неопходно је било да поседује ковид сертификат – потврду о вакцинацији, који је био интегрисан у одређен QR код који би приликом читавања пружио информације о конкретном лицу у виду имена, презимена, адресе пребивалишта, јединственог матичног броја грађана, датум вакцинисања, тип вакцине и слично. Будући да су те

---

<sup>39</sup>Чл. 9, Закон о евиденцијама и обради података у области унутрашњих послова („Сл. гласник РС”, бр. 24/2018);

<sup>40</sup>Ор. Cit., Д. Кривокапић, Ј. Адамовић, Д. Тасић, А. Петровски, П. Калезић, Ђ. Кривокапић, стр. 43;

ковид сертификате проверавали запослени у угоститељском објекту, дакле неовлашћена лица, тако што су скенирали кодове и самим тим имали увид у прегршт личних података неког лица, поставља се питање оправданости такве врсте прикупљања и обраде нечијих личних података, али и питање повреде начела ограничења у односу на сврху обраде и начела минимизације података, јер да би неко лице могло да борави у неком објекту довољно је било само добити информацију да ли је конкретно лице вакцинисано или не, без даљег приступа другим подацима, поготово од стране неовлашћених, трећих лица, у овом случају запослених у угоститељском објекту и без даљег упута да ли се скенирани подаци чувају, где, на који период и друга важна питања.

### **6.5. Јавни интерес**

Правни основ који се састоји у обављању послова у јавном интересу или извршења законом прописаних овлашћења руковооца, по правилу ће моћи да користе само органи власти или институције којима су поверена јавна овлашћења. Да би овај основ био валидан, обрада треба да има своју конкретну основу у закону. Органи јавне власти обављају велики број послова који се односе непосредно или посредно на лична стања грађана. У том смислу, они имају потребу да приступе одређеним подацима о личности како би се решила одређена животна ситуација, у смислу утврђивања права, обавезе или интереса. Под органима јавне власти треба подразумевати све имаоце јавних овлашћења који одлучују о стањима и ситуацијама грађана. Примера ради, катастар непокретности има право да обрађује поједине податке о личности оних физичких лица који су закључили уговор о промету непокретности, а у циљу уписа промене власника непокретности, чиме се извршава законом предвиђена дужност катастра.<sup>41</sup> Ипак, како свако правило има изузетке, тако је и овде. Ова одредба се односи и на сва остала лица која прикупе и на неки начин користе личне податке грађана у циљу извршења обавезе у јавном интересу. Тако, обрада података о личности у циљу пријављивања учињеног кривичног дела од стране неког службеника заполоног у некој установи не представља законско овлашћење, али представља вршење посла у јавном интересу, па и обавезу предвиђену кривичним законодавством као кривично дело „Непријављивање кривичног дела и учиниоца“ за чије непоштовање је предвиђена казна затвора. Одличан пример за прикупљање и обраду података о личности на основу јавног интереса јесте и актуелни попис становништва који је тренутно у току у Републици Србији. Обрада

---

<sup>41</sup>Ор. Cit., Стефан Андоновић, Драган Прља, стр. 64;

података о личности у оквиру пописа становништва, домаћинства и станова 2022. године врши се у јавном интересу и представља правну обавезу Републичког завода за статистику, а Закон о попису становништва, домаћинства и станова 2022. године усклађен је са Законом о заштити података о личности.<sup>42</sup> На крају, оно што је јако битно истакнути код овог основа обраде личних података јесте чињеница да основ за обраду података о личности у циљу обављања послова у јавном интересу или извршења законом прописаних овлашћења мора бити одређен законом. Законом треба установити и циљ обављања послова којима се остварује јавни интерес или законско овлашћење.

### **6.6. Легитимни интерес**

Законита је и она обрада података о личности која је неопходна у циљу остваривања легитимних интереса руковоаца или треће стране, осим ако су над тим интересима претежнији интереси или основна права и слободе лица на које се подаци односе, а посебно ако је лице на које се подаци односе малолетно лице. Интерес треба разликовати од сврхе због које се обрађују подаци. Интерес се односи на позитивне стране обраде података о личности, односно корист коју имају руковалац или трећа страна, што треба разликовати од сврхе обраде.<sup>43</sup> Значајно је да интереси морају бити легитимни, односно прихватљиви са позиције правног поретка, па је у том смислу нелегитиман онај правни интерес који се не заснива на начелима заштите података, онај интерес који тежи да оствари неке противправне последице или онај интерес који је усмерен на малициозно коришћење правних норми (нпр. остваривање противправне новчане користи за себе или друго лице, незаконито остваривање монополске позиције на тржишту, итд.). Ипак, није довољно само утврдити легитимни интерес руковоаца или трећег лица. Потребан услов је и да такав интерес не претеже над интересима лица на које се подаци односе или над њиховим правима и слободама. У том смислу је важно напоменути да руковалац, у складу са начелом одговорности, има обавезу да спроведе тест балансирања и то тако што ће са једне стране ставити своје легитимне интересе, а са друге слободе лица на које се подаци односе на који начин ће моћи да донесе одлуку о томе на који начин ће обрађивати нечије лични податке по овом основу тако да успут не повреди интересе појединца. Законитост обраде се не може заснивати на претежнијем легитимном интересу када се у позицији руковоаца налази орган јавне власти, како се не би превише проширило поље дискреционе оцене.

---

<sup>42</sup>Чл. 27 – 31, Закон о попису становништва, домаћинства и станова 2022. године ("Сл. Гласник РС", бр. 9/2020 и 35/2021);

<sup>43</sup>Ор. Cit., Стефан Андоновић, Драган Прља, стр. 65;

Први корак руковоаца приликом процене испуњености услова за примену легитимног интереса као правног основа за обраду је да утврди специфичан циљ који жели да оствари намераваном обрадом, односно позитиван исход који би проистекао као резултат намераване обраде. Тај циљ се може огледати у одређеној користи за самог руковоаца, или за трећу страну тј. за одређеног појединца, организацију, или јавност уопште. Подразумева се да циљ који није правно допуштен, или није у складу са професионалним стандардима одређеног сектора, гране или области не може представљати легитимни интерес за обраду података о личности. Уз то, потребно је да руковалац буде јасан и одређен у погледу конкретног циља намераване обраде, уместо позивања на неки уопштен пословни интерес као свој легитимни интерес за обраду података о личности (као што је, примера ради, повећање профита компаније).<sup>44</sup> Ако обрада није нужна за остварење циља или се циљ обраде може постићи без обраде података о личности или на мање инвазиван начин по приватност лица (нпр. обрадом мање количине података, друге врсте података и слично), онда намеравана обрада није неопходна, и не може се сматрати да је испуњен овај услов из члана 12 став 1 тачка 6 Закона о заштити података о личности. Што подаци чија се обрада намерава више задиру у приватност лица на које се односе, већа је вероватноћа да ће њихова обрада подразумевати већи ризик за права и слободе лица, те да ће потреба заштите тих права бити претежнија у односу на корист коју руковалац намерава да оствари. За сваки препознати могући узрок руковалац треба да процени вероватноћу његовог појављивања и озбиљност штете коју може нанети по интересе, права и слободе лица о чијим се подацима ради и на основу добијеног података извршити процену ризика. Полазећи од резултата извршене анализе, руковалац треба да процени да ли је у конкретном случају заштита права лица пропорционална очекиваној користи, или штета по права лица превазилази могућу корист, у ком случају легитимни интерес, највероватније, неће бити адекватан правни основ намераване обраде. Руковалац, такође, може да размотри предузимање додатних мера заштите које ће применити како би умањио могућност настанка штете и/или ублажио њене последице по права лица. На крају ваља напоменути да према правилима ЗЗПЈ органи власти не смеју да користе овај основ приликом обављања послова из своје надлежности тј. законодавац је искључио могућност примене легитимног интереса као правног основа за обраду података о личности од стране органа власти у случају када се обрада врши у оквиру

---

<sup>44</sup><https://www.poverenik.rs> - одељак за најчешће постављана питања у вези заштите личних података приступљено дана 05.10.2022. године;

надлежности органа. Ово све најпре из разлога што државни органи морају да поступају у оквиру законских надлежности, јер је закон једини основ из кога могу црпети своја овлашћења и самим тим приступати обради података о личности грађана. С друге стране, због своје неодређености и широке применљивости, примена овог основа у раду државних органа могла би лако водити злоупотребема, прекорачењу овлашћења којима се не би ни знале прецизне границе и на крају правној несигурности.<sup>45</sup> С обзиром на своју флексибилност, легитимни интерес као основ обраде података о личности има веома широку примену, али управо његова прилагодљивост и неодређеност може га чинити у исто време и непопуларном и ризичном опцијом за руковооце. Због тога се и процена утицаја највише врши у случају обрада које за основ имају управо легитимни интерес.

Када се ради о легитимном интересу као законом дозвољеном основу за обраду података о личности у циљу директног маркетинга и непосредног оглашавања постоји неслагање између решења које нуди Преамбула ГДПР-а и решења које нуди домаће законодавство. У члану 63 домаћег Закона о оглашавању утврђено је да је за директно оглашавање (упућивање огласне поруке) према физичким лицима потребна њихова претходна сагласност, која се може опозвати у сваком моменту, а оглашивач, односно преносилац огласне поруке, мора то да омогући. Утврђено је, такође, да се директно оглашавање према физичким лицима врши у складу са правилима о оглашавању путем средстава комуникације на даљину у складу са прописом који уређује заштиту потрошача.<sup>46</sup> Чланом 38 Закона о заштити потрошача утврђено је да је забрањено непосредно оглашавање телефоном, факсом, електронском поштом, и другим средствима комуникације на даљину, без претходног пристанка потрошача.<sup>47</sup> Сходно томе, правни основ за обраду података о личности у сврху директног маркетинга јесте пристанак лица на које се односе подаци који се обрађују. Са друге стране, у тачки 47 Преамбуле Опште уредбе о заштити података прописано је да се може сматрати да постоји легитиман интерес код обраде података о личности за потребе директног маркетинга, те да такво решење није у супротности са Општом уредбом из разлога што је тим прописом примена легитимног интереса као правног основа за обраду података о личности у сврху директног маркетинга предвиђена као могућност, те свака држава

---

<sup>45</sup><https://www.milic.rs/blog/zastita-podataka/legitimni-interes-kaos-ovnov-obrade-podataka-o-licnosti/>  
пристишљено дана 05.10.2022. године;

<sup>46</sup>Чл. 63, Закон о оглашавању („Службени гласник РС“, бр. 6/16 и 52/19 – др. закон);

<sup>47</sup>Чл. 38, Закон о заштити потрошача („Службени гласник РС“, бр. 62/14, 6/16 – др. закон и 44/18 – др. закон);

може да уреди то питање и на другачији начин у складу са својим правним системом, водећи рачуна и о другим правним актима ЕУ који регулишу одговарајуће области друштвених односа.<sup>48</sup>

## 7. ОБРАДА ПОСЕБНИХ ВРСТА ПОДАТАКА О ЛИЧНОСТИ

Поједине врсте података о личности уживају већи степен заштите у односу на заштиту која се уобичајено пружа. Тако, јављају се категорије података које се начелно не смеју обрађивати. Ти подаци се класификују као посебна врста података о личности или „осетљиви подаци“. У ову групу спадају подаци који се односе на расно и етничко порекло, политичко мишљење, верско и филозофско уверење, чланство у синдикату, генетске податке, биометријске податке, податке о здравственом стању и податке о сексуалном животу и сексуалној оријентацији лица.<sup>49</sup> Закон прописује да је обрада посебних врста података о личности у принципу забрањена, осим у изузетним случајевима. Другим речима, за обраду података из ове категорије није довољно само да постоји један од претходно описаних правних основа, већ мора да буде испуњен бар још један додатни услов. Додатни услови у којима је обрада посебних врста података дозвољена прописани су чл. 17 ст. 2 тач. 1-10 ЗЗПЛ и укључују следеће ситуације:

- када лице на које се подаци односе да изричит пристанак на обраду за једну или више сврха обраде, осим ако је законом прописано да се обрада неврши на основу пристанка;
- када је обрада неопходна у циљу извршења обавеза или примене законом прописаних овлашћења руковооца или лица на које се подаци односе у области рада, социјалног осигурања и социјалне заштите, ако је таква обрада прописана законом или колективним уговором;
- када је обрада неопходна у циљу заштите животно важних интереса лица на које се подаци односе или другог физичког лица, ако лице на које се подаци односе није у могућности да да пристанак за обраду;
- када се обрада врши у оквиру регистроване делатности и уз примену одговарајућих мера заштите од стране задужбине, фондације, удружења или друге непрофитне организације, под условом да се таква обрада врши само у односу на

---

<sup>48</sup>*Preamble of the General Data Protection Regulation, (EU) 2016/679, par. 47;*

<sup>49</sup>*Op. Cit., чл. 17, Закон о заштити података о личности;*

чланове, бивше чланове или лица која имају редовне контакте са организацијом у вези са циљем организације;

- када се обрађују подаци о личности које је лице на које се они односе учинило јавно доступним;

- када је обрада неопходна у циљу подношења, остваривања или одбране неког правног захтева или када суд поступа у оквиру својих надлежности;

- када је обрада неопходна у циљу остваривања значајног јавног интереса одређеног законом, под условом да је таква обрада сразмерна остваривању циља, уз поштовање суштине права на заштиту података о личности и примену одговарајућих мера заштите основних права лица чији се подаци обрађују;

- када је обрада неопходна у сврху превентивне медицине или медицине рада, ради процене радне способности запослених, медицинске дијагностике, пружања услуга здравствене или социјалне заштите односно управљања здравственим или социјалним системима, на основу закона или на основу уговора са здравственим радником, ако се обрада врши од стране или под надзором здравственог радника или другог лица које има обавезу чувања професионалне тајне;

- када је обрада неопходна у циљу остваривања јавног интереса у области јавног здравља, као што је заштита од озбиљних прекограничних претњи здрављу становништва или обезбеђивање високих стандарда квалитета и сигурности здравствене заштите и лекова или медицинских средстава, на основу закона који обезбеђује одговарајуће и посебне мере заштите права и слобода лица на које се подаци односе, посебно у погледу чувања професионалне тајне;

- када је обрада неопходна у сврхе архивирања у јавном интересу, у сврхе научног или историјског истраживања или у статистичке сврхе, ако је таква обрада сразмерна остваривању циљева који се намеравају постићи, уз поштовање суштине права на заштиту података о личности и ако је обезбеђена примен одговарајућих и посебних мера заштите основних права и интереса лица на које се ови подаци односе.

Рецимо, ситуација када је лице „очигледно учинило јавнодоступним“ своје податке о личности те се такви подаци могу даље обрађивати представљала би објава података о личности, попут фотографија или виде озаписа на друштвеним мрежама попут Facebook- а, Instagram-а или Twitter-а, уз коришћење опције да су такви подаци

доступни свима, без ограничавања на одређени круг лица („пријатеља“ или „пратиоца“), што омогућава даље коришћење ових података без посебне сагласности. Овај случај се може квалификовати као имплицитно давање сагласности, будући да у условима информационо-комуникационих технологија и интернета свако лице треба да буде свесно да подаци који су обелодањени и учињени доступним свима, могу бити коришћени у разне сврхе. При свему томе, треба имати у виду да је готово немогуће пратити даљи проток једном објављених података.<sup>50</sup>

Даље, руковооци у области рада, социјалног осигурања и социјалне заштите имају право да обрађују посебне податке када је таква обрада неопходна ради извршења обавезе њихове организације. Ова обрада мора бити предвиђена посебним законом или колективним уговором о раду, што значи да није довољна појединачна одлука руковооца као основ обраде посебних врста података о личности. Закон или колективни уговор о раду који дозвољава обраду посебних врста података у претходно поменуте сврхе мора прописати и адекватне мере заштите права и слобода за лица на које се подаци односе. Разлог успостављања мера лежи у осетљивом карактеру радних и социјалних односа у друштву и великог утицаја података о личности у овим друштвеним областима. Обрада посебних категорија података може се предузети и ради остваривања превентивних дужности у медицини или медицини рада у циљу оцењивања радне способности запослених и будућих запослених, што мора бити утемељено на закону или колективном уговору. Такође, посебне врсте података могу се обрађивати и у циљу успостављања медицинске дијагностике, као и пружања услуга здравствене и социјалне заштите. Логично, већина ових ситуација ће се односити на управљање медицинским подацима у циљу постављања одговарајуће дијагнозе или терапије, што наравно не искључује и остале врсте података које могу имати утицај на методе и начин лечења, попут верске припадности и импликација таквог статуса на здравље лица.<sup>51</sup> Пример за претходно наведено би могао бити случај обраде података о крсној слави запосленог, што припада подацима о верском уверењу, са циљем омогућавања том запослену одсуство са посла тог дана. Такође, ситуације у којима је неопходно обрађивати медицинске податке запосленог у смислу утврђивања компетенције за неко радно место које у опису посла садржи и руковање оружјем, тада ће се сматрати оправданим обрада здравствених података лица у циљу утврђивања

---

<sup>50</sup>А. Дилигенски, Д. Прља, Д. Церовић, *Право заштите података ГДПР*, Институт за упоредно право, Београд 2018. године, стр. 106;

<sup>51</sup>*Op. Cit.*, Стефан Андоновић, Драган Прља, стр. 79;

компетенције за конкретно радно место, па чак и процена адекватних медицинских стручњака.

Обрада посебних врста података о личности коју врше надлежни органи у посебне сврхе прописана је чланом 18 ЗЗПЛ и иста је допуштена је само ако је то неопходно, уз примену одговарајућих мера заштите права лица на које се подаци односе, у једном од следећих случајева:

- надлежни орган је законом овлашћен да обрађује посебне врсте података о личности;
- обрада посебних врста података о личности врши се у циљу заштите животно важних интереса лица на које се подаци односе или другог физичког лица;
- обрада се односи на посебне врсте података о личности које је лице на које се они односе очигледно учинило доступним јавности.<sup>52</sup>

Свакако оно што је јако битно напоменути да приликом обраде посебно осетљивих података, због тога што је њихова обрада у принципу забрањена, у први план избија начело минимизације података, односно њихова обрада треба да буде сведена на крајњи минимум који је неопходан да би се остварила сврха обраде.

## **8. ПОСЕБНИ СЛУЧАЈЕВИ ОБРАДЕ ПОДАТАКА О ЛИЧНОСТИ**

У домаћем ЗЗПЛ од члана 88 до члана 94 прописани су посебни случајеви обраде података о личности тј. обрада и слободе изражавања и информисања, слободан приступ информацијама од јавног значаја, обрада јединственог матичног броја грађана, обрада у области рада и запошљавања, мере заштите и ограничење примене закона на обраду у сврхе архивирања у јавном интересу, у сврхе научног или историјског истраживања или у статистичке сврхе, обрада од стране цркве и верских заједница и обрада у хуманитарне сврхе од стране органа власти..<sup>53</sup>

Најпре се говори о обради и слободи изражавања и информисања односно да се закон не примењује на обраду која се врши у сврхе новинарског истраживања и објављивања информација у медијима, као и у сврхе научног, уметничког или књижевног изражавања уколико су, у сваком конкретном случају, ограничења примене ЗЗПЛ неопходна у циљу заштите слободе изражавања и информисања. Конкретније, у овим ситуацијама се неће примењивати одредбе ЗЗПЛ које се односе на начела обраде,

---

<sup>52</sup>*Op. Cit.*, чл. 18, Закон о заштити података о личности;

<sup>53</sup>*Ibid.*, чл. 88-94;

права лица на која се подаци односе, руковоаоца, обрађивача и заједничког руковоаоца, као и њихове обавезе, пренос података о личности у друге земље и међународне организације и остале посебне случајеве обраде. Изузетак од примене одређених одредби Закона важи током конкретне активности која за сврху има новинарско истраживање и објављивање информација у медијима, односно научно, уметничко или књижевно изражавање. Након што је конкретна активност готова, све податке који више нису потребни требало би обрисати или анонимизовати.<sup>54</sup>

Даље се говори о обради и слободном приступу информацијама од јавног значаја. На обраду информација од јавног значаја које садрже податке о личности примењује се, поред Закона о заштити података о личности и Закон о слободном приступу информацијама од јавног значаја. То значи да орган јавне власти који тражиоцу информације чини доступним такве информације, а да оне притом садрже податке о личности, мора водити рачуна о томе да успостави баланс између права јавности да зна с једне, и права на заштиту података о личности с друге стране. Орган јавне власти од кога су тражене информације од јавног значаја које садрже податке о личности, требало би да, пре него што тражене информације учини доступним, анонимизује све оне личне податке који нису апсолутно неопходни за конкретну информацију и њен контекст. То даље значи да ће орган јавне власти у сваком конкретном случају морати да пронађе одговарајући баланс између два супротстављена права - права јавности да зна и права на заштиту података о личности. Одличан пример за наведено би било прибављање судских одлука преко Захтева за приступ информацијама од јавног значаја, где суд приликом одлучивања по поднетом захтеву мора да „извага“ оправданост чињења доступним неке одлуке и да уколико одлучи позитивно, одлуку достави без увида у личне податке странака.

На обраду јединственог матичног броја грађана (ЈМБГ) примењују се одредбе посебног закона који регулише ЈМБГ, уз примену одредби ЗЗПЛ у делу који се односи на заштиту права и слобода лица на којесе подаци односе. Закон о јединственом матичном броју грађана прописује да се ЈМБГ одређује електронски, у складу са правилима прописаним законом, и уноси се у јединствену електронску евиденцију о матичним бројевима коју води Министарство унутрашњих послова.<sup>55</sup> Закон о ЈМБГ прописује да се на обраду података о личности и евиденције које води Министарство

---

<sup>54</sup>Адамовић, *Водич за медије: заштита личних података и новинарски изузетак*, Share Фондација, Београд, 2018. године, стр. 42;

<sup>55</sup>Закон о јединственом матичном броју грађана (“Сл. гласник РС”, бр. 24/2018);

унутрашњих послова, као и на садржину тих евиденција, ажурирање, брисање, рокове чувања и мере заштите података, примењују одредбе оних закона којим се уређују евиденције и обрада података у области унутрашњих послова.<sup>56</sup> ЈМБГ служи за вођење евиденције података о личности, као и за повезивање са другим евиденцијама државних органа и корисника који имају законски основ за коришћење матичног броја.

На обраду у области рада и запошљавања, уз примену одредби ЗЗПЛ, примењују се и одредбе Закона о раду.<sup>57</sup> ЗЗПЛ прописује да ако закон који уређује рад и запошљавање или колективни уговор садрже одредбе о заштити података о личности, морају се прописати и посебне мере заштите достојанства личности, легитимних интереса и основних права лица на које се подаци односе, посебно с обзиром на транспарентност обраде, размену података о личности унутар мултинационалне компаније, односно групе привредних субјеката, као и систем надзора у радној средини.

Уколико се обрада података о личности врши у сврхе архивирања у јавном интересу, у сврхе научног или историјског истраживања или у статистичке сврхе, примењују се одговарајуће техничке, организационе и кадровске мере у циљу обезбеђивања минимизације података. Примера ради, уколико се сврха обраде може остварити уз примену псеудонимизације, онда би требало применити ову техничку меру заштите података о личности. Намера законодавца је да обавезе оног ко врши обраду личних података за неку од ових сврха, да анонимизује податке о личности тако да се лице о чијим се подацима ради не може идентификовати, под условом да се на овакав начин може остварити сврха обраде. Уколико се обрада врши у сврхе научног или историјског истраживања или у статистичке сврхе, не примењују се одредбе ЗЗПЛ које регулишу право на приступ лица на које се подаци односе, право на исправку и допуну, право на ограничење обраде и право на приговор, уколико је такво ограничење неопходно за остваривање ових сврха обраде, односно уколико би примена одредби о правима онемогућила или значајно отежала остварење ових сврха обраде. Исто важи и за обраду у сврху архивирања у јавном интересу, с тим што се у том случају не примењују ни одредбе ЗЗПЛ које се односе на право на преносивост података, право на брисање или ограничење обраде коју врши надлежни орган у посебне сврхе, обавезу

---

<sup>56</sup>Закон о евиденцијама и обради података у области унутрашњих послова ("Сл. гласник РС", бр. 4/2018);

<sup>57</sup>Закон о раду ("Сл. гласник РС", бр. 24/2005, 61/2005, 54/2009, 32/2013, 75/2014, 13/2017 - одлука УС, 113/2017 и 95/2018 - аутентично тумачење);

руководила да врши обавештавање у вези са исправком или брисањем података и ограничењем обраде, обавезу обавештавања руководиоца у вези са исправком или брисањем података и ограничењем обраде коју врше надлежни органи у посебне сврхе, као и остваривање права лица на које се односе подаци када обраду врше надлежни органи у посебне сврхе и провера Повереника.<sup>58</sup>

ЗЗПЛ прописује да, уколико цркве и верске заједнице примењују свеобухватна правила у погледу заштите физичких лица у односу на обраду, та постојећа правила се могу и даље примењивати под условом да се ускладе са ЗЗПЛ. У том случају, примењују се одредбе ЗЗПЛ које се односе на инспекцијска и друга овлашћења Повереника, осим уколико црква, односно друга верска заједница не образује посебно независно тело које ће вршити та овлашћења, под условом да такво тело испуњава законом предвиђене услове за избор Повереника.

Оно што је такође предвиђено кроз ЗЗПЛ јесте да орган власти може да обрађује податке о личности у циљу прикупљања средстава за хуманитарне сврхе, али да том приликом мора применити одговарајуће мере заштите права и слободалица на које се подаци односе у складу са ЗЗПЛ. Тако прикупљене податке, орган власти не може да уступа другим лицима.

## **9. ЗАШТИТА И НАДЗОР НАД ОБРАДОМ ПОДАТАКА О ЛИЧНОСТИ**

У циљу заштите основних права и слобода физичких лица у вези са обрадом, послове праћења примене закона у складу са прописаним овлашћењима врши Повереник за слободан приступ информацијама од јавног значаја и заштиту података о личности, као независан државни орган. Од свог оснивања, у оквиру своје надлежности, Повереник је стварао праксу у области заштите података доношењем мишљења, упозорења, решења у поступку инспекцијског надзора. Поред тога, Повереник је подносио кривичне пријаве, као и захтеве за покретање прекршајног поступка у случајевима када је постојала сумња да је дошло до повреде права приватности или одређене одредбе законских норми у области заштите података.

Повереник је овлашћен да у конкретном случају изврши инспекцијски надзор над спровођењем законских одредби. Циљ овог поступка јесте утврђивање да ли руководиоци и друга одговорна лица поступају у складу са Законом, а посебно да ли су права лица чији се подаци обрађују повређена, као и предузимање прописаних мера у случају кад

---

<sup>58</sup>*Op. Cit., Д. Кривокапић, Ј. Адамовић, Д. Тасић, А. Петровски, П. Калезић, Ђ. Кривокапић, стр. 87;*

се у поступку утврди да је дошло до повреде Закона. Поступак се покреће на иницијативу самог Повереника или на основу притужбе коју подноси лице на које се односе подаци који се обрађују. Повереник је дужан да подносиоца притужбе обавести о току и исходу поступка који је притужбом инициран, као и о могућности коришћења правних лекова против одлуке Повереника која је донета поводом притужбе.<sup>59</sup> На поједина питања поступка сходно се примењују правила закона којим се уређује инспекцијски надзор, као и правила општег управног поступка. Против одлуке Повереника која је донета у поступку инспекцијског надзора свако лице на које се ова одлука односи има право да се тужбом обрати Управном суду. Тако, то право може користити лице на које се односе подаци који се обрађују, руковалац, обрађивач или друго лице. Тужба се подноси у року од 30 дана од дана пријема одлуке Повереника, односно у року од 60 дана од дана подношења притужбе у случају ако Повереник не донесе одлуку по притужби или не изврши своју обавезу обавештавања подносиоца притужбе.<sup>60</sup>

Лице на које се односе подаци који се обрађују има право на заштиту пред парничним судом ако сматра да су му радњом обраде повређена права прописана Законом. Поступак заштите покреће се подношењем тужбе против руковаоца, односно обрађивача и то вишем суду на чијој територији тужени има пребивалиште, боравиште или седиште. Тужба се може поднети и суду на чијој територији тужилац има пребивалиште или боравиште, осим ако се тужба подноси против органа власти. Ревизија правноснажне одлуке донете по парничној тужби је увек допуштена. Закон прописује садржину тужбених захтева који се могу истаћи у поступку пред судом. Ови захтеви се тако односе на давање прописаних информација, исправку, допуну, односно брисање података, ограничавање обраде, давање и преношење података у структурисаном облику и прекид обраде.<sup>61</sup> Ако се ради о одлуци која је донета на основу аутоматизоване обраде података, односно профилисању, тужбом се може захтевати и само утврђивање да је дошло до повреде законских одредби. Такође, тужбом се може захтевати и накнада материјалне и нематеријалне штете која је проузрокована повредом Закона. По правилу, одговорност за штету лежи на руковаоцу. Обрађивач одговара за штету само у случају кад се утврди да није поступао у складу са

---

<sup>59</sup>Гајин Саша, *Заштита података о личности у сектору безбедности – Водич кроз законску регулативу*, Центар за унапређивање правних студија и мисија ОЕБС-а у Србији, Београд, 2019. година, стр. 24;

<sup>60</sup>Ор. Cit., чл. 83, Закон о заштити података о личности;

<sup>61</sup>Ibid., чл. 84;

законским обавезама које се односе само на њега или да није поступао у складу са упутствима руковоаца.

Када се ради о прекршајном поступку, закон прописује новчане казне за кршење законских одредби. Распон новчаних казни усклађен је са одредбама закона којим се уређују прекршајна одговорност. Новчане казне се могу изрећи уз прописане мере за отклањање стања повреде Закона или уместо њих. Закон налаже да новчане казне морају бити делотворне и сразмерне учињеном прекршају, узимајући у обзир њихову превентивну функцију. Приликом одлучивања о кажњавању и висини казне, мора се водити рачуна о низу околности прописаних Законом<sup>62</sup>, као што је: природа, тежина и трајање стања повреде законских одредби, а у контексту врсте, обима и сврхе обраде, броја лица чији се подаци обрађују и висине проузроковане штете; намера или степен непажње одговорног лица; предузимање, односно непредузимање радње усмерена на отклањање стања повреде законских одредби или ублажавања штете; степен сарадње одговорног лица са Повереником и др. Овлашћење за новчано кажњавање припада Поверенику и прекршајном суду. Повереник је овлашћен да изрекне новчану казну на основу прекршајног налога ако приликом инспекцијског надзора утврди да је дошло до прекршаја за који је Законом прописана новчана казна у фиксном износу. Ако лице коме је Повереник изрекао новчану казну одбије да је плати, у складу са одредбама закона који уређује прекршајну одговорност, као и ако се ради о прекршајима за које Закон не прописује новчану казну у фиксном износу, поступак утврђивања прекршајне одговорности и изрицања новчане казне спроводи надлежни прекршајни суд.<sup>63</sup>

Када је даље реч о заштити података у смислу обавеза руковоаца, узимајући у обзир ниво технолошких достигнућа и трошкове њихове примене, природу, обим, околности и сврху обраде, као и вероватноћу наступања ризика и ниво ризика за права и слободе физичких лица који произилазе из обраде, руковалац је приликом одређивања начина обраде, као и у току обраде, дужан да примени одговарајуће техничке, организационе и кадровске мере које имају за циљ обезбеђивање делотворне примене начела заштите података о личности, као што је смањење броја података и да обезбеди примену неопходних механизма заштите у току обраде, како би се испунили услови за обраду прописани овим законом и заштитила права и слободе лица на која се подаци односе. Руковалац је дужан да сталном применом одговарајућих техничких, организационих и

---

<sup>62</sup>Чл. 42, Закон о прекршајима ("Сл. гласник РС", бр. 65/2013, 13/2016, 98/2016 - одлука УС, 91/2019, 91/2019 - др. закон и 112/2022 - одлука УС);

<sup>63</sup>Ор. Cit, Гајин Саша, стр. 26;

кадровских мера обезбеди да се увек обрађују само они подаци о личности који су неопходни за остваривање сваке појединачне сврхе обраде. Та се обавеза примењује у односу на број прикупљених података, обим њихове обраде, рок њиховог похрањивања и њихову доступност.<sup>64</sup> Стандардне мере које се данас примењују обухватају систем привилегија, енкрипцију, псеудонимизацију и слично. Важан сегмент безбедности података у информационом систему може се решити контролом приступа различитим сетовима података и то кроз систем привилегија и рола, односно дефинисањем различитих улога у обради података за различите групе запослених, пословних партнера и корисника. Неке сетове података могу да виде сви без разлике, у друге увид могу да имају само стручни сарадници, треће могу да мењају само запослени са посебним овлашћењима, итд. Роле се дефинишу у складу са потребама и обавезама у организацији, док информациони систем аутоматски региструје време и место сваког приступа.<sup>65</sup> Овај систем подразумева доделу корисничких налога и неки облик потврде власништва лозинком, квалификованим сертификатом, биометријским информацијама. Лозинке или шифре су најчешћи метод аутентификације и зато је важно да буду што комплексније, да не садрже податке о кориснику ни речи природног језика. Енкрипција или аутоматско шифрирање садржаја постаје општи стандард у заштити безбедности информационих система, односно података који се у систему обрађују. Локална енкрипција дискова односисе на физичке уређаје на којима се чувају важни подаци као додатни метод заштите, односно нови ниво контролисаног приступа. У случају крађе компјутера или дискова, енкрипција је солидна препрека неовлашћеном приступу подацима.<sup>66</sup> Током читавог процеса обраде личних података, уколико се они не морају чувати у изворном облику, препоручује се анонимизација или псеудонимизација. Анонимизација подразумева неповратан прекид веза између података и идентитета особе на којусе ти подаци односе. Псеудонимизација је привремено маскирање података који се по потреби могу вратити у изворни облик, обично уз помоћ шифрарника или оригиналног документа.<sup>67</sup>

---

<sup>64</sup>Ор. Cit., чл. 42, Закон о заштити података о личности;

<sup>65</sup>Ор. Cit., Д. Кривокапић, Ј. Адамовић, Д. Тасић, А. Петровски, П. Калезић, Ђ. Кривокапић, стр. 53;

<sup>66</sup>Ibid, стр. 54;

<sup>67</sup>Ibid.

## 10. ПРИМЕРИ ИЗ ПРАКСЕ МЕЂУНАРОДНИХ СУДОВА

### 10.1. Case of Peck v. The United Kingdom - Application no. 44647/98 (28/01/2003)<sup>68</sup>

Чињенично стање: Подносилац представке је био господин Џефри Денис Пек. У својој представи Европском суду за људска права у Стразбуру апликант се ослонио на наводну повреду члана 8 Европске конвенције за заштиту људских права и основних слобода тј, повреду права на приватност. У току 1995. године подносилац представке је боловао од депресије и једног дана је изашао на улицу у граду и покушао кухињским ножем да пререже вене и изврши самоубиство. Није имао сазнања да је конкретна улицама покривена уличним видео надзором и да је цео догађај документован. Касније је тај снимак заједно са пропратним фоографијама доспео на насловне стране престижних локалних новина, а убрзо затим се проширио и на друга новинска издања, док лице апликанта није било сакривено већ се јасно могло видети о коме се ради. Део видео снимка је приказан и на више локалних телевизија. Подносилац представке је тврдио да објављивање снимка и фотографија представља озбиљно мешање у његов приватни живот. Релевантни снимак се односио на покушај самоубиства, он није био свестан тога да се све то снима, а снимак је показао непосредне последице ове епизоде док је још увек држао нож, хапшење полиције и реаговање хитне помоћи. Снимак је обелодањен писаним и аудиовизуелним медијима са великом публиком, без његовог пристанка и знања и без маскирања или адекватног прикривања идентитета. Његов лик, чак и у тим околностима, емитован је милионима и препознао га је велики број особа које су га познавале, укључујући чланове породице, пријатеље и колеге.

Закључак суда: Суд је утврдио да у конкретном случају нису постојали оправдани разлози за мешање у приватни живот апликанта, нису постојали оправдани разлози за објављивање идентитета апликанта и објављивање снимка и фотографија је учињено без пристанка лица, што је све навело суд да утврди повреду члана 8 Конвенције и да апликанту на име нематеријалне штете због претрпљене узнемирености, стреса и осећаја срамоте досуди износ од 11.800 еура.

Овакав закључак суда нам указује да је чак и пре 24 година, будући да је представка поднета 1998. године, када се није придавао толики значај заштити личних података, суд ипак придао велику важност истима утврђујући да је у конкретном случају ипак дошло до неоправданог мешања јавних власти у приватан живот

---

<sup>68</sup>Case of Peck v. the United Kingdom, Application no. 44647/98, (28/01/2003) – преузето са „Hudoc“ базе;

појединца на начин што је дозвољено да снимак и фотографије са јавних камера доспу у јавност и буду објављени без пристанка лица које се налази на снимку и фотографијама. Иако стара, поменута пресуда је итекако значајна за област заштите података од личности будући да представља прве кораке препознавања ове јако битне области.

## **10.2. Case of Big brother watch and others v. the United Kingdom [GC] - Application no. 58170/13, 62322/14 and 24960/15<sup>69</sup>**

Чињенично стање: У овом случају се ради о три представке које су Европском суду за људска права поднете у периоду од 2013. – 2015. године од стране новинара и организација за заштиту људских права против Велике Британије. Подношење представки уследило је након указивања Едварда Сноудена<sup>70</sup> у вези са програмима електронског надзора којима управљају обавештајне службе Сједињених Америчких Држава и Уједињеног Краљевства, да државе користе широк спектар техника за шпијунирање људи у земљи и иностранству. Сноуден је открио да Велика Британија користи програм под називом „TEMPORA“ како би омогућила Државном штабу за комуникације (GCHQ) да приступи „спољним“ комуникацијама на велико које пролазе дуж оптичких каблова који пролазе између Уједињеног Краљевства и Северне Америке. УК не само да користи ове податке за своје потребе, већ даје и NSA<sup>71</sup> приступ овим подацима. Прикупљени подаци укључују интернет и телефонску комуникацију, као што су садржај е-поште, Facebook уноса и историје веб страница, као и метаподатке. Подносиоци представке су се жалили на обим и величину програма електронског надзора којим управља Влада Уједињеног Краљевства тачније на три различита режима надзора од стране државе: масовно пресретање комуникација, пријем и пресретање материјала страних влада и обавештајних агенција и добијање комуникационих података од провајдера комуникационих услуга верујући да су били предмет надзора и да су њихови лични подаци незаконито прикупљени, што је све последично довело до повреде члана 8 Конвенције. Апликанти су тврдили да је држава

---

<sup>69</sup>Case of Big brother watch and others v. the United Kingdom [GC], App no. 58170/13, 62322/14 and 24960/15, (25/05/2021) - преузето са „Hudoc“ базе;

<sup>70</sup>Едвард Џозеф Сноуден (енг. Edward Joseph Snowden) је бивши амерички радник Централне обавештајне агенције, који је радио као саветник за Државну безбедносну агенцију САД. Сноуден је изазвао велику контроверзу када је у јавност изнео тајне документе који су показали постојање великог броја тајних пројеката надзирања, као на пример, PRISM и Boundles informant и документе који показују да су САД спроводиле хакерске нападе у рачунаре широм света, између осталог и у току састанка Г-20 у Лондону 2009. године, у Хонгконгу и Кини. Сноуден је предао документе новинарима Гардијана и Вашингтон поста, у јуну 2013 – преузето са <https://sr.m.wikipedia.org>;

<sup>71</sup>Државна безбедосна агенција, позната по свом акрониму НСА (од енгл. скраћенице NSA (National Security Agency)), сматра се највећом америчком владином обавештајном агенцијом.

прикупљала податке о њима кроз поменути три режима надзора што није било прописано законом, није било неопходно нити сразмерно легитимном циљу, обрађивала је податке без ваљаног основа, складиштила, преносила, све без њиховог знања или пристанка, као и да разлика између интерне и екстерне комуникације била је не само лоше дефинисана, већ и бесмислена, при чему је већина комуникација вероватно била сврстана у категорију „спољашње“. Навели су да се у ери савремених технологија генерише огромна количина комуникационих података, који сами по себи доста говоре о некој особи, а који су структурирани на такав начин да су рачунари могли да их обрађују и траже обрасце у њима брже и ефикасније од сличних претрага садржаја. Са друге стране, држава је навела да су подаци прикупљани у сврху заштите националног интереса и националне безбедности, јер не само да им је то омогућило да открију до сад непознате претње, већ им је омогућило и праћење познатих циљева ван њихове територијалне надлежности. УК је става да се државама у случајевима масовног надзора треба оставити широка маргина слободне процене, јер је моћ масовног пресретања комуникација била предмет детаљног и сталног разматрања од стране низа независних тела последњих година и постојало је једногласно мишљење да не постоји никаква алтернатива или комбинација алтернатива довољна да замени моћ пресретања „на велико“. Држава је такође навела да иако је прикупила све те податке, нема мешања у право на приватност појединца тиме што она складиште те податке, али би до повреде дошло када би неко претражио тако прикупљене податке по одређеним параметрима, а селекција и свако испитивање које је уследило били су веома пажљиво контролисани, ниједан обавештајни извештај није могао бити направљен о било каквој комуникацији или комуникацијским подацима осим ако их није прегледао аналитичар, а што је све било у складу са важећим прописима.

Закључак суда: У овом случају, суд је најпре заузео општи став да у случајевима прикупљања података масовним пресретањима комуникације и обраде тако добијених података суд сматра да процес мора бити предмет „end to end safeguard“ (комплетна заштита) како би се смањио ризик од злоупотребе моћи масовног пресретања, што значи да на домаћем нивоу треба у свакој од фаза процеса извршити процену неопходности и сразмерности предузетих мера, да масовно пресретање треба да буде предмет одобрења од стране независног органа на самом почетку, када се дефинишу предмет и обим операције и да операција треба да буде предмет надзора и независног *ex post facto* прегледа. По мишљењу суда, ово су основне заштитне мере које ће бити

камен темељац сваког режима масовног прокупљања података у складу са чланом 8 Конвенције. Суд није спорио навод државе који се тичао одбране националних интереса и националне безбедности, јер прво, зато што су терористи, криминалци и непријатељске стране обавештајне службе постајале све софистицираније у избегавању откривања традиционалним средствима и друго, зато што је природа глобалног интернета значила да је рута којом ће одређена комуникација путовати постала изузетно непредвидљива. Међутим, суд је једногласно донео одлуку да је дошло до повреде члана 8. Европске конвенције – права на приватност у погледу режима масовног пресретања комуникација апликаната јер такво пресретање комуникације лица није било прописано законом и није била сразмерна мера која је тежила легитимном циљу, једногласно је одлучио и да је дошло до повреде члана 8 у вези са режимом добијања комуникационих података од провајдера комуникационих услуга будући да је овакву одлуку одобрио државни секретар, а не неко тело независно од извршне власти, да није постојао претходни пристанак лица за прикупљањем и обрадом података нити адекватан правни основ за овакво поступање, није био ограничен приступ подацима искључиво у сврху борбе против „тешког криминала“ и није захтевана претходна ревизија од стране суда или независног административног органа, док је са 12 гласова за и 5 против донео одлуку да није дошло до повреде члана 8 у вези са режимом Уједињеног Краљевства за пријем и пресретање материјала страних влада и обавештајних агенција. Суд је закључио да је британски закон поставио јасна, детаљна правила која регулишу када су обавештајне службе биле овлашћене да захтевају пресретнути материјал од страних обавештајних агенција и како, када се прими, тражени материјал треба да буде прегледан, коришћен и касније уништен.

Ова одлука суда има значајне импликације не само на правни оквир Уједињеног Краљевства за програме масовног пресретања приватне комуникације, већ и на закон о приватности података, будућност програма масовног надзора и режима размене обавештајних података у УК, Европи и шире. Одлука је посебно релевантна за претходни период због пандемије вируса COVID 19, јер су националне власти покушавале да се све више ослањају на наметљиве методе прикупљања података и праћења контаката како би спречио ширење вируса COVID 19. Такође, ово је прва одлука о дозвољености међународне размене обавештајних података у складу са Европском конвенцијом о људским правима и тако ће обликовати будућност режима размене обавештајних података. Овде је приступ Великог већа у оштрој супротности са

приступом Европског суда правде, где је нагласак на заштитним мерама које пружају треће земље које добијају информације. Врло је вероватно да ће режими масовног надзора постати све легитимнији у Великој Британији, Европској Унији, широј Европи па и шире. Као што упозорава судија Pinto de Albuquerque свом издвојеном мишљењу, „У неким деловима Европе, разне тајне службе ће бити у великом искушењу да искористе веома опуштену моду суда да формулише правне стандарде и невини људи ће платити цену раније или касније.”<sup>72</sup>

### 10.3. CJEU - C-673/17 - Planet49 (01/10/2019)<sup>73</sup>

Чињенично стање: Немачка компанија „Planet 49“ је на свом веб сајту организовала онлајн лутрију. Да би неко лице учествовало, непходно је било да се унесе име и презиме и адреса. Испод поља за унос ових података стојале су два квадратића за чекирање. Први квадрат се односио на давање сагласности корисника да компанија и одређени сарадници компаније може да му телекомуникационим каналима (позив, смс, мејл) шаље промотивни и маркетинг материјал који се односи не само на конкретну компанију, већ и материјал сарадника компаније, а такође је стајало и да се овај пристанак може повући било када, а други квадрат се односио на давање сагласности корисника да компанија може да инсталира веб аналитику тј. „колачиће“ на његовом компјутеру што би значило да корисник регистрацијом ради учествовања у лутрији, дозвољава компанији да инсталира колачиће који омогућавају праћење понашања корисника на сајту и да те податке користи за таргетирање одређеним постовима и рекламама, сходно интересима корисника. Први квадрат је био празан, док је други већ унапред био чекиран. Поред је стајало и да подешавања за ове колачиће могу бии обрисани било када. Да би неко лице могло да учествује у лутрији, било је неопходно да чекира бар један квадрат тј. једини слободан. Немачка организација за заштиту потрошача (the “Bundesverband”) је иницирала судски поступак против компаније „Planet 49“ наводећи да овакав пристанак не испуњава критеријуме слободног и информисаног пристанка и тражила је разјашњење да ли је сагласност путем унапред означених поља валидан облик пристанка уопште. Случај је стигао до Савезног суда правде Немачке који је размотрио питања у вези са обимом сагласности према одредбама Data Protection Directive 95/46/EC, ePrivacy Directive

<sup>72</sup>Op. Cit., Case of Big brother watch and others v. the United Kingdom [GC] -partly concurring and partly dissenting opinion of judge Pinto de Albuquerque - преузето са „Hudoc“ базе;

<sup>73</sup>Planet49, CJEU-C-673/17,(01/10/2019), преузето

[https://curia.europa.eu/juris/document/document\\_print.jsf?docid=218462&text=&dir=&doclang=EN&part=1&occ=first&mode=req&pageIndex=0&cid=1415539;](https://curia.europa.eu/juris/document/document_print.jsf?docid=218462&text=&dir=&doclang=EN&part=1&occ=first&mode=req&pageIndex=0&cid=1415539)

2002/58/EC и GDPR-а. С обзиром да је конкретан случај пред Суд правде доспео 2017. године, пре почетка примене ГДПР-а 2018. године, а Савезни суд правде Немачке је тражио решење којим ће наложити овој компанији забрану оваквог поступања у даљем пословању, одлука суда темељи се на одредбама и Директиве 95/46/EC и ГДПР-а.

Одлука суда: Суд је заузео став да у односу на пристанак који се помиње у одредбама релевантне законске регулативе, овако прибављени пристанак од стране компаније „Planet 49“ није ваљано конституисан ако је, у облику колачића, складиштење информација или приступ информацијама које су већ потхрањене у терминалној опреми корисника веб странице, јер се давање пристанка практично намеће претходним означањем поља за потврду које корисник мора поништити уколико жели да одбије давање пристанка. Суд је такође заузео став и да власници веб сајтова треба да имају обавезу обавештавања посетилаца њихових сајтова о колачићима њиховом трајању и да ли и која трећа лица могу имати приступ подацима прикупљеним путем колачића. Дакле, једини правноваљани пристанак јесте изричито дат пристанак који испуњава све критеријуме који су прописани. Пристанак мора да представља слободно изражавање воље и да корисник свој пристанак даје активном радњом тако што ће означити поље, а не поништити поље које је већ означено.

Последица доношења овакве одлуке огледа се у томе што су сви власници веб сајтова који су желели да користе веб аналитику како би пратили понашање корисника сајтова и на тај начин унапредили садржај, одрадили стратешки добро маркетиншко таргетирање и тако увећали себи профит, сада морали да на своје сајтове поставе обавештење о колачићима са свим неопходним информацијама, као и политику приватности сајта, а све тако да поље за пристанак не буде већ претходно чекирано. Такође, ова одлука суда је од великог значаја, јер је кроз њу суд упоредио одредбе актуелних законских регулатива по датом питању.

#### **10.4. CJEU - C-61/19 - Orange Romania SA v Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) (11/11/2020)<sup>74</sup>**

Чињенично стање: Orange România SA је пружалац мобилних телекомуникационих услуга на подручју Румуније. У марту 2018. године Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP), што је надзорни орган за заштиту података о личности у Румунији (као наш Повереник за

---

<sup>74</sup>Orange Romania SA v (ANSPDCP), CJEU - C-61/19 - (11/11/2020) преузето са <https://gdprhub.eu/CJEU - C-61/19 - Orange Romania SA v ANSPDCP>;

информације од јавног значаја и заштиту података о личности) је у складу са румунским законодавством којим се штити област података о личности, овој компанији упутио санкције због чињенице да су прикупљали и чували копије личних карти и самим тим податке о њиховим корисницима без њиховог изричитог пристанка. Издат је и налог руковаоцу да уништи постојеће копије личних карти и да прекине ову незакониту праксу. Наиме, компанија Orange România SA је приликом потписивања уговора о пружању телекомуникационих услуга тражила од својих клијената да приложе и копију личне карте. У тим уговорима се јесу налазиле одредбе о прикупљању и обради личних података за које су корисници потписивањем уговора дали свој пристанак, али нигде у уговору није стојала одредба да се потписивањем уговора лица обавезују да ова компанија може прикупљати и чувати копије њихових личних карата. Овакав пристанак корисници су морали да дају писменим путем, на посебном образцу. Неки од поменутих уговора су имали приложен и овај образац, али већина није, што је и утицало на одлуку надзорног тела Румуније. Компанија се жалила на овакву одлуку надзорног тела надлежним органима унутар државе.

Одлука суда: Суд правде ЕУ је установио да уговор о пружању телекомуникационих услуга који садржи клаузулу у којој се наводи да је субјекат података обавештен о прикупљању и чувању копије свог личног документа у сврху идентификације и самим тим и личних података и да је потписивањем уговора дао сагласност за то, није такав да докаже да је то лице ваљано дало свој пристанак, како је предвиђено законским одредбама. Најпре, постоји могућност да је сам контролор штиклирао поље које се односи на ту клаузулу пре потписивања уговора, затим тако постављени услови уговора су могли довести у заблуду субјекта података у погледу могућности закључивања дотичног уговора, јер се може сматрати да контролор неоправдано утиче на слободу избора да се приговори том прикупљању и складиштењу, а намеће се услов да субјект података, како би одбио пристанак, мора да попуни додатни образац који наводи то одбијање. Дакле, према ставу суда, једино јасан и недвосмислен, безусловно дат пристанак се може сматрати законитим пристанком.

Из конкретног случаја се јасно може закључити да се одредбе ГДПР-а које се односе на карактеристике пристанка морају поштовати. Овде имамо јасан пример неадекватног пристанка, будући да лица нису било информисана о томе који подаци ће се прикупљати, у коју сврху, на колики временски период, а потписивање уговора са жељом добијања телекомуникационе услуге не значи и да лице пристаје на обраду

података, већ се пристанак за све претходно побројане радње мора прибавити на прописан начин, на посебном писаном обрасцу који ће садржати све неопходне информације.

**10.5. Case no. 20-CIV-03346 - Kelly Whalen and others v. Facebook, (07/08/2020), Superior Court of California<sup>75</sup>**

Чињенично стање: Тужиоци су тврдили да је компанија прикупљала, складиштила и профитирала од биометријских података више од 100 милиона корисника апликације „Instagram“ без њиховог знања или сагласности, као што је прописано Законом о приватности за биометријске податке Илиноиса. Конкретно, тужиоци су тврдили да је „Facebook“, који је власник апликације Instagram, користио информације за „напајање, обуку и развој свог софтвера за препознавање лица“. Тражили су да се случај сертификује као групна тужба у име корисника Instagramа који живе у Илиноису. Facebook је истакао да је сваки корисник апликације у овом случају пристао на одредбе о препознавању лица које се налазе у условима коришћења апликације Instagram и да су примили неколико обавештења о ажурирањима услова коришћења апликације заједно са могућношћу да исте не прихвате. Софтвер за препознавање лица ради тако што скенира лица неименованих људи на фотографијама или видео снимцима како би анализирао детаље лица појединаца и креирао одговарајући „шаблон лица“ за свако лице, а затим чува тај шаблон лица за каснију употребу и/или га упарује са онима које већ има у бази података идентификованих лица. Facebook кришом хвата заштићене биометријске податке корисника апликација без њиховог информисаног пристанка и, што је још горе, а да их заправо не обавештава о својој пракси. И ова пракса није само на поменутој апликацији, већ на свим апликацијама које су у власништву тужене компаније. Тужитељка у конкретном случају је приступала Instagramу на оба своја рачунара, али и преко телефона како би постављала фотографије, прегледала садржај који су поставили други корисници и реаговала на тај садржај путем коментара и „лајкова“. Она је често означавала себе и друге на фотографијама које су објављиване на апликацији, а појављује се и на фотографијама које су други поставили на Instagram. Тужиља није била свесна да Facebook преко ње прикупља било какве податке о препознавању лица или друге биометријске податке током употребе Instagramа.

Закључак суда: Врховни суд Калифорније је закључио да Facebook никада није обавестио кориснике Instagramа да прикупља њихове биометријске податке. У ствари,

---

<sup>75</sup>*Kelly Whalen and others v. Facebook, Case no. 20-CIV-03346, (07/08/2020), Superior Court of California, преузето са <https://www.classaction.org/media/whalen-v-facebook-inc.pdf>;*

Facebook активно обмањује кориснике Instagrama о томе да ли прикупља податке о препознавању лица. Instagram-ова политика приватности прописује: „Иако сте искључили, користимо технологију препознавања лица која ће вас препознати на фотографијама, видео снимцима и искуствима са камером.” Корисници Instagrama немају могућност да искључе било који софтвер за препознавање лица унутар апликације. Штавише, Instagram политика приватности података такође наводи: „Ако уведемо технологију препознавања лица у ваше искуство на Instagramu, прво ћемо вас обавестити, а ви ћете имати контролу над тим да ли користимо ову технологију за вас.“ Дакле, корисницима Instagrama није чак ни дата прилика да дају писану сагласност, јер Facebook аутоматски обрађује садржај и дели га на својим платформама. Чак и ако корисник нема активирано препознавање лица на свом личном налогу, његова фотографија може и даље бити скенирана, прикупљена и унета у Фејсбукову базу података ако се поклапа са подацима корисника који има активирану поставку за препознавање лица. Због свега наведеног, суд је донео одлуку да је дошло до повреде одредаба Закона о приватности за биометријске податке Илиноиса и определио казну коју Facebook треба да плати у укупном износу од 650 милиона долара.

Наведени случај је врло користан пример преко кога се може увидети пракса великих интернет компанија попут Facebook-а које су бесплатне, дакле не плаћа се никаква цена за њихово преузимање и коришћење, отварање профила и слично, али се заправо плаћају. Ту цену плаћају корисници остављањем и превише својих података на друштвеним мрежама, који се прикупљају, обрађују, складиште и даље преносе, све без знања корисника на који начин овакве компаније и зарађују, тргујући личним подацима корисника.

#### **10.6. Case 10 O 84/20 - LG Itzehoe (Germany) (11/06/2020)<sup>76</sup>**

Чињенично стање: Google својим корисницима нуди услуге „GoogleMaps“ и „Google Earth“. Обе услуге омогућавају корисницима да виде сателитске слике имовине субјекта података коју је снимио Google. Када се врши претрага уносом адресе некретнине, црвена ознака локације није директно на имању већ на улици. Међутим, када се унесу ГПС координате, црвена чиода за локацију је директно на имању. Фотографија из ваздуха приказује локацију и величину стамбене зграде, као и различите аспекте некретнине (зелене површине, кровна површина, тераса, башта).

---

<sup>76</sup>LG Itzehoe (Germany), Case 10 O 84/20 - (11/06/2020) преузето са <https://gdprhub.eu/index.php?title=LG-Itzehoe-10-O-84/20>;

Тужба је у поменутом поступку поднета поводом сателитских снимака објављених на наведеним сервисима, у погледу којих је тужилац, као лице на чију се имовину (објекат и његову околину) спорне фотографије односе, захтевао да „Google“ фотографије и снимке пикселизира или оно што се на њима налази на други начин учини препознатљивим, тврдећи да оне садрже његове личне податке, при чему није овластио „Google“ нити неко треће лице да исте сачини и објави.

Закључак суда: Окружни суд Немачке је одбио предметни тужбени захтев позивајући се одредбу члана 6 став 1 тачка Ф ГДПР-а, налазећи да интерес руковоаца да настави да користи фотографије претеже над интересом субјекта на кога се предметни подаци односе, тј. интересом да своју имовину учини препознатљивом. Наиме, сходно становишту које је заузео поступајући суд, постоји шира, тј. потреба јавности да коришћењем услуга „Google“-а као руковоаца подацима о личности у конкретном случају сагледа одређени простор, при чему не постоји конкретна веза између изгледа фотографисаног објекта и других личних података његовог власника (нпр. имена и адресе).

Конкретан случај указује на употребу легитимног интереса као једног од законитих основа обраде нечијих података и како то заправо изгледа у пракси. Може се дакле закључити да чињеница да „Google“ поседује сателитске снимке и фотографије нечијих објеката, па и снимке и фотографије наших кућа, зграда, викендица и слично, не представља повреду података о личности, јер над правом на приватношћу сваког од нас, конкретно приватности изгледа и локације наших објеката, претеже интерес јавности за коришћењем поменутих сервиса „Google“-а који пружају увид у просторни план неког града, насеља или слично. А такође се може закључити и да снимак или фотографија нечијег приватног власништва, у овом случају објекта, не представља податак о личности.

## **11. ПРИМЕРИ ИЗ ПРАКСЕ ДОМАЋИХ СУДОВА**

Чланом 146. Кривичног законика прописано је кривично дело „Неовлашћено прикупљање личних података“ те је предвиђено да ко податке о личности који се прикупљају, обрађују и користе на основу закона неовлашћено прибави, саопшти другом или употреби у сврху за коју нису намењени, казниће се новчаном казном или затвором до једне године, као и свако ко противно закону прикупља податке о личности грађана или тако прикупљене податке користи, а уколико ово дело учини

службено лице у вршењу службе, казниће се затвором до три године.<sup>77</sup> Став 3. овог члана КЗ-а прописује више казне за учиниоце који изврше дело у својству службеног лица. У оваквим случајевима, кривични поступак односно гоњење предузима надлежно јавно тужилаштво, док се за дела из ставова 1. и 2. то чини по приватној тужби, како је то утврђено чланом 153 КЗ-а.

У случају Основног суда у Алексинцу К бр. 359/20 кривично дело извршио је административни радник општине, који је без сагласности оштећене унео њен ЈМБГ у потврду коју издаје општина и предао је њеном бившем супружнику. Изречена је условна казна.<sup>78</sup>

У предмету Основног суда у Ужицу К бр. 547/20 у улози осуђеног био је полицијски службеник који је искористио своју ИД картицу да би приступио службеном рачунару путем којег је проверио рок важења регистрације једног аутомобила, док је за други аутомобил проверио место пребивалишта власника истог као место регистрације возила. Ове податке је после саопштио пријатељу са којим је имао претходни договор то да уради. И у овом предмету је изречена условна казна.<sup>79</sup>

У предмету Основног суда у Новом Саду К.бр.1249/20 покренутом по приватној тужби, кривично дело се састојало у томе што су окривљени на својој Фејсбук страници објавили документ - одлуку са личним подацима приватног тужиоца, који су неовлашћено прибавили, и на тај начин омогућили неограниченом броју људи да има увид у исту. У овом поступку суд је ирекао окривљеном условну осуду.<sup>80</sup>

Први основни суд у Београду је у предмету 32 К бр. 54/2019 донео одлуку којом је окривљеног ослободио оптужбе у поступку по приватној тужби, јер је на сајту Савета за борбу против корупције неовлашћено на списку купаца вила објавио адресу приватног тужиоца, прикупљену на основу Закона о јавној својини, без његове сагласности, а из разлога што је суд сматрао да у току поступка није могло бити несумњиво и неспорно утврђено да је окривљени извршио то кривично дело. Као један од разлога је био тај да је суд сматрао да нема доказа да је објављивање предметног извештаја и прилога усмерено на конкретну личност, било које физичко или правно

---

<sup>77</sup>Чл. 146, Кривични законик ("Сл. гласник РС", бр. 85/2005, 88/2005 - испр., 107/2005 - испр., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 и 35/2019);

<sup>78</sup>Н. Ницовић, А. Тоскић Цветиновић, М. Тошић, М. Маринковић, В. Шаховић, Д. Милеуснић, У. Мишљеновић., *Приватност и заштита података о личности у Србији, Партнери за демократске промене Србија (Партнери Србија), Београд 2022. година, стр. 25;*

<sup>79</sup>Ibid.

<sup>80</sup>Ibid, стр 26;

лице, те да на тај начин нема доказа да је објављен било који податак о личности за који би била потребна сагласност личности на који се тај податак односи, што је и потврђено у другостепеној одлуци.<sup>81</sup>

Један предмет вођен је пред Основним судом у Зрењанину. Предмет је покренут по оптужном предлогу Основног јавног тужилаштва у Зрењанину, против медицинске сестре. Она је у овом поступку оглашена кривом што је неовлашћено прибавила, саопштила другом и употребила у сврху за коју нису намењени податке о личности, тако што је противно члану 2. Закона о евиденцијама у области здравства РС, у вези са чланом 6. Закона о заштити података о личности, приступила здравствено-информационом систему и неовлашћено из евиденција прибавила податке о оштећеном, које је потом дала свом пуномоћнику у парничном поступку, да искористи у парничном поступку који се водио пред Основним судом у Зрењанину. Суд је у овом поступку донео осуђујућу пресуду, одредивши се за условну осуду, којом се окривљеној одређује казна затвора од 3 месеца, која се неће извршити уколико у наредне 2 године од правноснажности пресуде не понови кривично дело.<sup>82</sup>

Овлашћење које је Поверенику дато законом је да, по спроведеном надзору, надлежном јавном тужилаштву може да поднесе кривичну пријаву у делокругу своје надлежности па се тако јавио и случај подношења кривичне пријаве Основном јавном тужилаштву у Нишу у случају „Малчанског берберина“. Пријава је поднета због цурење информација (исказа окривљеног) из истраге у медије у предмету отмице девојчице.<sup>83</sup>

Пред Прекршајним судом у Лесковцу, због кршења новог Закона о заштити података о личности вођен је један поступак. У том поступку, окривљено правно лице Црвени Крст у Медвеђи и одговорно лице у том правном лицу кажњени су новчаним казнама од 50 хиљада, односно 5 хиљада динара, јер као руковођаци података о личности, нису обрађивали податке о личности на начин који обезбеђује одговарајућу заштиту, услед чега је неовлашћено треће лице М. В. приступило подацима садржаним

---

<sup>81</sup> Д. Милеуснић, Д. Ђурчић, Д. Тасић, Ј. Адамовић, К. Калајић, М. Ковачевић, М. Павловић, Н. Ницковић, У. Мишљеновић, *Приватност и заштита података о личности у Србији, Анализа одабраних секторских прописа и њихове примене, Партнери за демократске промене Србија (Партнери Србија), Београд, 2021. године, стр. 14;*

<sup>82</sup> *Ibid*, стр 26;

<sup>83</sup> <https://insajder.net/arhiva/vesti/poverenik-podneo-krivicnu-prijavu-zbog-objavljanja-iskaza-osumnjicenog-za-otmicu-monike-karimanovic> приступљено дана 15.10.2022. године;

у предметним евиденцијама, којом приликом је исто лице сачинило снимак мобилним телефоном и потом објавило податке о личности на свом Инстаграм налогу.<sup>84</sup>

Иако је Закон о заштити података о личности на снази већ пуне 3 године, евидентан је јако мали број случајева из праксе који се тичу повреде ове области што може бити доста забрињавајуће и што указује да и даље не постоји свест људи о значају ове области, да постоји „устезање“ од покретања судских поступака од стране физичких лица, да поступци који се покрећу по службеној дужности често имају неславан завршетак, да су досуђене казне неадекватне и веома благе у односу на добро које се штити и због свега наведеног, потребно је усавршавати важеће законске прописе, подићи свест људи, радиди на креирању судске праксе која ће допринети очувању и бољој заштити области заштите података о личности.

## 12. ЗАКЉУЧНА РАЗМАТРАЊА

Ноторна је чињеница да је област заштите података о личности, иако од раније фигурира у правном промету, тек од скоро почела да добија све већу пажњу. Може се рећи и да је развој информационах технологија имао велики утицај на то. Законска регулатива која је тренутно важећа не покрива у најбољој мери све аспекте ове области и неопходно је уредити је тако да прати развој информационах технологија, а опет са друге стране, информационе технологије се рапидно брзо развијају да је немогуће да законодавни оквир прати тај темпо. Практика међународних и националних судова и Повереника за информације од јавног значаја и заштиту података о личности иде у том смеру, што је јако добро, јер приликом доношења одлука по питањима из ове области, праксом се постављају нови стандарди који прате савремени развој. Због свега наведеног се мора наћи најадекватније решење којим би се постојећа регулатива постепено прилагодила развоју ових технологија.

Важно је напоменути да све већи број људи у све већој мери користи интернет, разне претраживаче, сајтове, апликације и слично, свакодневно остављајући разне личне податке разним оператерима. Честа ситуација је да приликом приступа неком сајту искочи банер са информацијама о колачићима на сајту који онемогућава у потпуности приступ садржају сајта те се махинално кликне на дугме „Пристајем“ (*eng. I agree*), а да се притом и не прочита шта је све на том банеру о колачићима написано и каква је политика приватности конкретног сајта, а касније само стигне мејл или порука

---

<sup>84</sup>*Op. Cit, Д. Милеуснић, Д. Ђурчић, Д. Тасић, Ј. Адамовић, К. Калајић, М. Ковачевић, М. Павловић, Н. Ницовић, У. Мишљеновић, стр. 30;*

о неким промоцијама или слично тог оператера, па остане питање одакле неке подаци неког лица и смелост да се неко лице узнемирава на тај начин. Управо из тог разлога је неопходно подићи свест људи о значају личних података, о принципима обраде података о личности, скренути пажњу на пристанак који се тако махинално остави неком оператеру, а који је такође од великог значаја за трећа лица. Притом треба пронаћи и решење којим ће се зауставити оваква пракса оператера и других лица који на овакав начину изискују пристанак трећих лица.

Иако је евидентно да велики број људи добија свест о свему овоме и даље је то занемарљиво мали број, те је у том смислу неопходно подробније едуковати грађане о правима која им стоје на располагању када је у питању област заштите података о личности, које све врсте података о личности фигурирају у правном промету, приближити им законске одредбе и активније радити на заштити личних података, а такође је неопходно едуковати и руковооце и обрађиваче који долазе у додир са подацима о личности трећих лица, упознати их са обавезама и одговорностима које имају, јер у свету који нам предстоји заснованом на вештачкој интелигенцији, биотехнологији и алгоритмима за обраду велике количине података улога права заштите података о личности биће све већа.

Оно што се на крају може закључити јесте чињеница да технолошке иновације агресивно продиру све више у наш свакодневни живот, често пресудно утичући на наш посао, навике и приватни живот. Евидентно је да су људи већ кренули, а у будућности ће то бити учесталије, да се све више ослањају на паметне уређаје - телефоне, рачунаре, аутомобиле, па чак и паметне фрижидере. Сваки од паметних уређаја јесте намењен да унапреди и олакша живот, али истовремено прикупља и огроман број података о личности, те се може рећи да будућност припада подацима и да ће подаци представљати „ново гориво“ савременог доба.

### 13. ЛИТЕРАТУРА

- Адамовић, Водич за медије: заштита личних података и новинарски изузетак, Share Фондација, Београд, 2018. године;
- Андоновић Стефан, Прља Драган, Основи права заштите података о личности, Институт за упоредно право, Београд 2020. године;
- Гајин Саша, Заштита података о личности у сектору безбедности – Водич кроз законску регулативу, Центар за унапређивање правних студија и мисија ОЕБС-а у Србији, Београд, 2019. година;
- Дилигенски, Андреј, Прља Драган, Церовић Дражен, Право заштите података ГДПР,, Институт за упоредно право, Београд 2018. године;
- Зуковић Слађана, Слијепчевић Сенка,, „Родитељска контрола понашања деце на интернету и социјалним мрежама“, у Настава и васпитање, бр. 64/2, Педагошко друштво Србије и Институт за педагогију и андрагогију Филозофског факултета Универзитета у Београд, Београд 2015. године;
- Кривокапић Драган, Адамовић Јелена, Тасић Дуња, Петровски Андреј, Калезић Петар, Кривокапић Ђорђе, Водич кроз Закон о заштити података о личности и ГДПР, тумачење новог правног оквира, 2019. године;
- Милеуснић Дамјан, Ђурчић Данило, Тасић Дуња, Адамовић Јелена, Калајџић Кристина, Ковачевић Милош, Павловић Михаило, Ницовић Нина, Мишљеновић Урош, Приватност и заштита података о личности у Србији, Анализа одабраних секторских прописа и њихове примене, Партнери за демократске промене Србија (Партнери Србија), Београд, 2021. године;
- Мишич Клеменч, Лубарда Маја, Заштита података – приручник за руковооце, Повереник за информације од јавног значаја и заштиту података о личности Републике Србије, Београд 2012. године;
- Ницовић Нина, Тоскић Цветиновић Ана, Тошић Милица, Маринковић Милица, Шаховић Влада, Милеуснић Дамјан, Мишљеновић Урош, Приватност и заштита података о личности у Србији, Партнери за демократске промене Србија (Партнери Србија), Београд 2022. година;
- Хећимовић Жељко, Метаподаци, Свеучилиште у Сплиту, Факултет грађевинарства, архитектуре и геодезије, Катедра за геодезију и геоинформатику, Сплит 2016. године.

## 14. ИСТРАЖИВАЧКА ГРАЂА

### Законодавство

- Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012;
- Consolidated version of the Treaty on the Functioning of the European Union, OJ C 326, 26.10.2012;
- 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;
- General Data Protection Regulation, (EU) 2016/679;
- individuals with regard to the processing of personal data and on the free movement of such data;
- Preamble of the General Data Protection Regulation, (EU) 2016/679, par. 47;
- Protocol amending the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108);
- Закон о евиденцијама и обради података у области унутрашњих послова ("Сл. гласник РС", бр. 4/2018);
- Закон о евиденцијама и обради података у области унутрашњих послова ("Сл. гласник РС", бр. 24/2018).
- Закон о заштити података о личности ("Сл. гласник РС", бр. 87/2018);
- Закон о заштити потрошача („Службени гласник РС“, бр. 62/14, 6/16 – др. закон и 44/18 – др. закон);
- Закон о јединственом матичном броју грађана ("Сл. гласник РС", бр. 24/2018);
- Закон о оглашавању („Службени гласник РС“, бр. 6/16 и 52/19 – др. закон);
- Закон о попису становништва, домаћинства и станова 2022. године("Сл. Гласник РС", бр. 9/2020 и 35/2021;
- Закон о потврђивању Конвенције о заштити лица у односу на аутоматску обраду личних података ("Сл. лист СРЈ - међународни уговори", бр. 1/92, "Сл. лист СЦГ - међународни уговори", бр. 11/2005 - др. закон и "Сл. гласник РС - међународни уговори", бр. 98/2008 - др. закон и 12/2010);
- Закон о прекршајима ("Сл. гласник РС", бр. 65/2013, 13/2016, 98/2016 - одлука УС, 91/2019, 91/2019 - др. закон и 112/2022 - одлука УС);
- Закон о раду ("Сл. гласник РС", бр. 24/2005, 61/2005, 54/2009, 32/2013, 75/2014, 13/2017 - одлука УС, 113/2017 и 95/2018 - аутентично тумачење);

- Закон о ратификацији Европске конвенције за заштиту људских права и основних слобода, измењене у складу са протоколом број 11, протокола уз Конвенцију за заштиту људских права и основних слобода, протокола број 4 уз Конвенцију за заштиту људских права и основних слобода којим се обезбеђују извесна права и слободе који нису укључени у конвенцију и први протокол уз њу, протокола број 6 уз Конвенцију за заштиту људских права и основних слобода о укидању смртне казне, протокола број 7 уз Конвенцију за заштиту људских права и основних слобода, протокола број 12 уз Конвенцију за заштиту људских права и основних слобода и протокола број 13 уз Конвенцију за заштиту људских права и основних слобода о укидању смртне казне у свим околностима("Сл. лист СЦГ - међународни уговори", бр. 9/2003, 5/2005 и 7/2005 - испр. и "Сл. гласник РС - међународни уговори", бр. 12/2010 и 10/2015);
- Закон о спречавању прања новца и финансирања тероризма, „Сл. гласник РС“, бр. 113/2017, 91/2019;
- Кривични законик ("Сл. гласник РС", бр. 85/2005, 88/2005 - испр., 107/2005 - испр., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 и 35/2019)
- Устав Републике Србије («Службени гласник РС» бр. 98/2006, 16/2022) – Одлука о проглашењу Уставног закона за спровођење Акта о промени Устава Републике Србије - Амандмани I - XXIX - "Сл. гласник РС", бр. 115/2021);

#### Интернет линкови

- <https://enterprivacy.com/2017/03/01/categories-of-personal-information/>
- <https://www.milic.rs/zastita-podataka-o-licnosti/>
- [https://www.echr.coe.int/Documents/Convention\\_MNE.pdf](https://www.echr.coe.int/Documents/Convention_MNE.pdf)
- <https://www.poverenik.rs/images/stories/dokumentacija-nova/prirucnik/GDPRQA.pdf>
- <https://dataprivacymanager.net/pristanak-kao-uslov-za-obradu-podataka-o-licnosti/>
- <https://www.poverenik.rs>
- <https://www.milic.rs/blog/zastita-podataka/legitimni-interes-kao-osnov-obrade-podataka-o-licnosti/>
- <https://sr.m.wikipedia.org>
- [https://curia.europa.eu/juris/document/document\\_print.jsf?docid=218462&text=&dir=&doclang=EN&part=1&occ=first&mode=req&pageIndex=0&cid=1415539](https://curia.europa.eu/juris/document/document_print.jsf?docid=218462&text=&dir=&doclang=EN&part=1&occ=first&mode=req&pageIndex=0&cid=1415539)
- <https://gdprhub.eu/CJEU - C-61/19 - Orange Romania SA v ANSPDCP>
- <https://www.classaction.org/media/whalen-v-facebook-inc.pdf>

- [https://gdprhub.eu/index.php?title=LG Itzehoe - 10 O 84/20](https://gdprhub.eu/index.php?title=LG_Itzehoe_-_10_O_84/20)
- <https://insajder.net/arhiva/vesti/poverenik-podneo-krivicnu-prijavu-zbog-objavljivanja-iskaza-osumnjicenog-za-otmicu-monike-karimanovic>

### **Судска пракса**

- Case of Big brother watch and others v. the United Kingdom [GC], App no. 58170/13, 62322/14 and 24960/15, (25/05/2021);
- Case of Peck v. the United Kingdom, Application no. 44647/98, (28/01/2003);
- Kelly Whalen and others v. Facebook, Case no. 20-CIV-03346, (07/08/2020), Superior Court of California;
- LG Itzehoe (Germany), Case 10 O 84/20 - (11/06/2020);
- Orange Romania SA v (ANSPDCP), CJEU - C-61/19 - (11/11/2020);
- Planet49, CJEU - C-673/17 - (01/10/2019).

## Сажетак и кључне речи

Област заштите личних података је у ери свакодневног развоја и унапређења глобалног интернета и информационих технологија почела да добија неопходну пажњу. Са друге стране, интернет је донео нове начине на које се може повредити нечија приватност са много погубнијим и далекосежнијим последицама по оштећеног. Кроз податке о личности који се на овакав начин могу прикупити, може се заћи у најдубље сфере личности, а људски интегритет се може непоправљиво угрозити на најтеже начине. У свету данашњице, све апликације и сви уређаји потхрањују се подацима корисника, са или без знања корисника што са собом даље носи многобројне ризике и што заштиту података о личности чини свакако битном темом.

Сврха овог рада јесте да пружи општи увод у област обраде података о личности, али и да кроз приказ практичних примера из праксе прикаже поступање надлежних органа на међународном и домаћем терену. Ауторка кроз рад приказује теоријско дефинисање података о личности, теоријску поделу истих, а затим обрађује нормативни оквир ове области са циљем приказа релевантног нормативног оквира којим је регулисана дата област уз критички осврт на поједина решења закона. У централном делу рада детаљније су обрађени законом прописани основи обраде личних података уз навођење ситуација у којима руковалац и обрађивач могу прикупљати податке појединаца, на који начин, у коју сврху, на колики временски период, који је положај субјекта чији се подаци прикупљају и обрађују, како се врши обрада категорије посебно осетљивих података, али и чини кратак осврт на посебне случајеве обраде података о личности. Значај овог дела рада се огледа у томе што ауторка обрађујући теоријска и законска решења, ипак пружа и приказ примене наведеног у пракси. У трећем делу рада су обрађени одабрани практични случајеви из међународне и домаће праксе кроз чију анализу се може утврдити да ли се и у којој мери води рачуна о законитој обради личних података, да ли се релевантни прописи тумаче, али и примењују на адекватан начин, колико су учесници овог процеса упознати са својим правима и обавезама и слична питања од значаја. Током обраде овог дела рада ауторка даје и сопствени допринос теми кроз изношење свог осврта на задату тему, али и образлажући значај конкретног случаја. Иако је пракса међународних судова многобројнија и самим тим подробнија, пракса домаћих органа свакако покушава да одржи корак пратећи развој међународних судова и на тај начин креирајући адекватну

домаћу судску праксу по питању области заштите података о личности. На самом крају рада изнета су закључна разматрања ауторке.

Ауторка сматра да је неопходно подробније едуковати грађане о правима која им стоје на располагању када је у питању област заштите података о личности, које све врсте података о личности фигурирају у правном промету, али и подробније едуковати и руковооце и обрађиваче тих података по питању начина обраде података о личности трећих лица, треба активније радити на приближавању и адаптацији законских одредби и активније радити на заштити личних података уопште.

Кључне речи: приватност, подаци о личности, обрада података о личности, руковалац, обрађивач, информационе технологије, закон

## **Summary and key words**

### **Processing of personal data**

In the era of daily development and improvement of the global Internet and informational technologies, the field of personal data protection began to receive the necessary attention. On the other hand, the Internet has brought new ways in which one's privacy can be violated with much more disastrous and far-reaching consequences for the injured party. Through personal data that can be collected in this way, one can go into the deepest spheres of the personality, and human integrity can be irreparably threatened in the most serious ways. In today's world, all applications and all devices feed on user data, with or without the user's knowledge, which further brings with it numerous risks and which makes the protection of personal data an important topic.

The purpose of this paper is to provide a general introduction to the field of personal data processing, but also to present practical examples to show the actions of competent authorities on the international and domestic level. Through the work, the author shows the theoretical definition of personal data, the theoretical division of the same, and then elaborates the normative framework of this area with the aim of presenting the relevant normative framework that regulates the given area with a critical review of individual solutions of the law. In the central part of the work, the legally prescribed basis for personal data processing are dealt with in more detail, stating the situations in which the handler and the processor can collect the data of individuals, in what way, for what purpose, for what period of time, what is the position of the entities whose data is collected and processed, how the category of particularly sensitive data is processed, but also makes a brief overview of special cases of personal data processing. The importance of this part of the work is reflected in the fact that the author, while dealing with theoretical and legal solutions, also provides an account of the application of the above in practice. In the third part of the paper, selected practical cases from international and domestic practice are processed, through the analysis of which it can be determined whether and to what extent the legal processing of personal data is taken into account, whether the relevant regulations are interpreted and applied in an adequate way, as far as the participants of this process are aware of their rights and obligations and similar issues of importance. During the processing of this part of the work, the author makes her own contribution to the topic by presenting her review of the given topic, but also by explaining the importance of the specific case. Although the practice of international courts is more numerous and therefore more limited, the practice of domestic authorities certainly tries

to keep pace by following the development of international courts and thus creating adequate domestic judicial practice in the area of personal data protection. At the very end of the paper, the author's concluding remarks were presented.

The author believes that it is necessary to educate citizens in more detail about the rights that are available to them when it comes to the area of personal data protection, which all types of personal data figure in legal transactions, but also to educate the controllers and processors of that data in more detail about the way of processing personal data of third parties, we should work more actively on approximation and adaptation of legal provisions and work more actively on the protection of personal data in general.

Keywords: privacy, personal data, processing of personal data, handler, processor, informational technology, law

## Биографија ауторке

Петровић Марина је рођена 11.06.1998. године у Књажевцу. Завршила је основну школу „Димитрије Тодоровић Каплар“ у Књажевцу као носилац Вукове дипломе. Техничку школу у Књажевцу, смер комерцијалиста – оглед завршила је 2017. године такође као носилац Вукове дипломе и исте године је уписала основне студије на Правном факултету, Универзитета у Нишу. Основне академске студије завршила је 2021. године са просечном оценом 8,97. Исте године је уписала мастер студије на Правном факултету у Нишу, смер „Информационе технологије“.

Као студент, кандидаткиња је била учесник разних трибина, семинара и конференција. Током школске 2020/2021 године учествовала је у пројекту пружања бесплатне правне помоћи грађанима, а који пројекат је реализован путем Мобилне правне подршке на Правном факултету у Нишу уз подршку Амбасаде Сједињених америчких држава и Одбора за људска права у Нишу. Кандидаткиња је била полазник Обуке за примену Европске конвенције за заштиту људских права и основних слобода која је реализована од стране организације Civil Rights Defenders, Правног факултета у Нишу и Moot court, дебатног и беседничког клуба „Iustitia“ Ниш.

Кандидаткиња је учествовала на разним такмичењима у току студирања и то на Националном такмичењу у симулацији кривичног поступка 2020. године на ком такмичењу је са екипом освојила специјалну награду „Rising stars“, на Premotcourt такмичењу одржаном 2021. године на Правном факултету у Нишу где је са екипом освојила треће место, затим је исте године узела учешће и на Регионалном Moot Court такмичењу у организацији Civil Rights Defenders-а на ком је са екипом освојила друго место, као и на Moot court такмичењу одржаном у Сарајеву у организацији Савета Европе. На Premoot court такмичењу „Бранко Маринковић“ одржаном 2022. године на Правном факултету у Нишу била је коментор екипе „Онора“ која је освојила специјалну награду „Rising stars“. На 16. Регионалном Moot Court такмичењу у организацији Civil Rights Defenders-а 2022. године била је секретар већа у полуфиналу и великом финалу такмичења. Кандидаткиња је полазник и прве школе приватности коју спроводи организација „Партнери Србија“.

У току мастер студија, кандидаткиња је обавила обавезну стручну праксу у познатој компанији „Better collective“ у Нишу. Новембра 2021. године је уписана у

Именик адвокатских приправника Адвокатске коморе у Нишу и од тада се налази на обављању приправничке вежбе у адвокатској канцеларији у Нишу са циљем стицања практичних знања и оставрења услова за полагање правосудног испита.

Због постигнутог успеха у току студија, кандидаткиња је била стипендиста Министарства просвете и општине Књажевац, а 2022. године је била и добитник специјалне стипендије „Будућност Књажевца“ коју додељује општина Књажевац.

Кандидаткиња је оспособљена за рад на рачунару и служи се енглеским и шпанским језиком.

**ИЗЈАВА О ИСТОВЕТНОСТИ**  
**ШТАМПАНОГ И ЕЛЕКТРОНСКОГ ОБЛИКА МАСТЕР РАДА**

Име и презиме аутора мастер рада: Петровић Марина

Наслов мастер рада: „ОБРАДА ПОДАТАКА О ЛИЧНОСТИ“

Ментор: Проф др Милош Прица

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

У Нишу, \_\_\_\_\_ 2022. године

Потпис аутора

---

Петровић Марина  
Бр. индекса: М001/21 – ИТ

## ИЗЈАВА О АУТОРСТВУ И ОДОБРАВАЊУ ОБЈАВЉИВАЊА МАСТЕР РАДА

Изјављујем да је мастер рад, под насловом „ОБРАДА ПОДАТАКА О ЛИЧНОСТИ” пријављен и одбрањен на Правном факултету Универзитета у Нишу:

- резултат сопственог истраживачког рада;
- да овај мастер рад у целини, нити у деловима, нисам пријављивала на другим факултетима, нити универзитетима;
- да нисам повредила ауторска права, нити злоупотребила интелектуалну својину других лица.

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

Аутор мастер рада: Петровић Марина

У Нишу, \_\_\_\_\_ 2022. године

Потпис аутора

---

Петровић Марина  
Бр. индекса: М001/21 – ИТ