Милош Прица, асистент
Правни факултет Универзитета у Нишу

UDK: 342.738:004

ОГРАНИЧАВАЊЕ ПРИВАТНОСТИ ДРЖАВНОМ ИНТЕРВЕНЦИЈОМ ЗАСНОВАНОЈ НА ПРИМЕНИ ИНФОРМАЦИОНИХ ТЕХНОЛОГИЈА[1]

„Свако друштво које би се одрекло мало слободе, да би добило мало сигурности, неће заслужити ниједно, а изгубиће обоје.
Бенџамин Фреклин

Апстракт**:** *Рад је посвећен само једном аспекту приватности – личним подацима, који у данашњим правним поретцима бивају подвргнути различитим видовима државне интервенције. Интервенционичка нарав савремене правне државе бива наглашена применом информационих технологија, намећући мноштво видова задирања у приватност појединца. Будући правно везано, то задирање путем прикупљања, обраде и коришћења личних података, од стране државе и њој сличних носилаца империјума, израз је правоваљаног остваривања различитих облика јавног интереса. Притом, ограничавање приватности обрадом личних података у правима савремених држава – премда правоваљано, може бити оправдано (легитимно) и неоправдано (нелигитимно). Оправдано ограничавање намеће „збиљски јавни интерес", док срж неоправданог чини „симуловани (привидни) јавни интерес", који прикрива властодржачку потребу запоседања слободе појединца. Особиту пажњу аутор посвећује неоправданом ограничавању приватности појединца, највећма због чињенице да примена нових информационих технологија у савременом информационом друштву доводи до промене природе и сврхе конвенционалних (традиционалних) захвата државе у приватну сферу појединца. Аутор настоји да на постављена питања одговори анализовањем типичних случајева у праву Србије и у упоредном праву.*

Кључне речи*: приватност, лични подаци, државна интервенција, јавни интерес.*

1 Рад представља резултат истраживања на пројекту "Заштита људских и мањинских права у европском правном простору", пројекат националног карактера (бр. 179046) који финансира Министарство за науку и технолошки развој Владе Републике Србије.

I. Увод

Лични подаци су део права на приватност, једног права-слободе, о којем влада несагласје у правној књижевности.[2] Лични податак је свака информација која се односи на физичко лице, без обзира на облик у коме је изражена (папир, трака, филм, електронски медиј). Постоје две категорије личних података. Прва категорија обухвата податке који чине физички део саме личности. Реч је о биометријским подацима (својеручни потпис, отисак прстију, дигитализована слика лица, скен очне рожњаче и др.), који, као непроменљиви и неодвојиви од личности, представљају личне податке у ужем смислу. Другој категорији личних података припадају типови података који говоре о личности, али нису њен физички део (име, национална припадност, пол, језик, вероисповест и сл.). Будући одвојиви од личности, те и потенцијално заменљиви, ови типови података представљају личне податке у ширем смислу, за које ћемо из разлога јасног предочавања и разликовања употребити израз „подаци о лицу".[3]

Право на приватност представља једно од основних субјективних права. У сржи овога права стоји интерес титулара да његов приватни живот[4] трећим лицима буде доступан у мери у којој је то опредељено његовом вољом.

---

2 Заправо, посленици науке су несагласни у погледу добара која су угрожена обрадом података о личности. О томе: Владимир В. Водинелић, *Обрада података и заштита личности,* Анали Правног факултета у Београду, 2-3/1989, стр. 172-196; Ловро Штурм, *Правни аспекти заштите података у савременим информационим системима,* Анали Правног факултета у Београду, 6/1986, стр. 652-665; Драгица Попеску, *Право приватности*, Билтен Окружног суда у Београду, 2008, стр. 55-69.

3 в. Оливер Суботић, Биометријски системи идентификације, Београд, 2007, стр. 20-21.

4 У погледу значења појма „приватан живот" знаковита су правна схватања Европског суда за људска права у Стразбуру (у наставку Суд), настала у примени чл. 8. Европске конвенције о људским правима, који гласи: „Свако има право на поштовање свог приватног и породичног живота, дома и преписке". Полазећи од тога да Суд није утврдио експлицитну дефиницију приватног живота, у прилици смо само да предочимо одређујуће идеје водиље Суда у примени чл. 8. Конвенције.

Прво, Суд је заузео гледиште да заштита приватног живота, поред негативне обавезе, садржане у заштити појединца од самовољног мешања јавних власти, може бити изражена и кроз конкретне обавезе садржане у стварном поштовању приватног живота (рецимо у случају Airey v. Irska, Суд је сматрао да је предлагач био жртва кршења чл. 8. по основу тога што по домаћем праву не постоји систем правне помоћи у поступку расставе, те се одбијањем приступа суду директно утицало на приватан и породичан живот). в. Жил Диретр, Изводи из најзначајнијих одлука Европског суда за људска права, Београд, 2006, стр. 233.

Друго, Суд је мишљења да се приватни живот не може ограничити на „унутрашњи круг" у којем би појединац могао да се креће у приватном животу који одабере, чиме би из њега био искључен спољни свет који није тим кругом обухваћен. У том смислу правно схватање појма приватног живота, по мишљењу Суда, не искључује професионалну или пословну делатност појединца (в. Niemietz v. Nemačka; Huvg v. Francuska; Chappeli v. Ujedinjeno Kraljevstvo). Ibid, стр. 229-230.

Суштину (биће) права на приватност обликује потреба појединца да ужива пуну аутономију спрам три врсте својих интереса: аутономије одлучивања у интимним и личним стварима, заштите од откривања личних околности и интерес заштите од неосноване присмотре од стране власти.[5]

Правна књижевност познаје две концепције (типа) приватности – класичну и савремену, у чијој основи лежи разлика између двеју државних форми: либералне правне државе, која је изнедрила класичну концепцију приватности и савремене правне државе, у чијем се поретку развио тзв. савремени тип приватности. Либерална правна држава (настаје крајем 18. и у свом изворном облику битише до почетка 20. века) била је крајње неинтервенционистичка држава; њени задаци састојали су се у остваривању циља моћи, циља безбедности и правнога циља (заштита државе, јавнога поретка и субјективних права појединаца). Придев „либерална“ у свом називу получила је захваљујући идеологији либерализма која је пропагирала аутономију појединца и грађанског друштва. Следствено томе, приватност као еманација слободе појединца (негативне слободе) стајала је у поретку либералне правне државе потпуно ван државне интервенције, на темељу чега су посленици правне књижевности либералну приватност дефинисали као „право појединца да буде остављен на миру“.[6]

Време либералне правне државе ишчезло је почетком 20. века, када долази до проширивања задатака државе. Осим задатака који чине нужно биће државне власти (одбрана, унутрашња безбедност, финансије, дипломатија и правосуђе), интервенција државе захвата све области унутардруштвеног живота. Такво стање, са извесним противдејствовањем (нео)либерализма (период након 2. светског рата и последња деценија 20. века), своју коначну потврду добива на концу 20. и у првој деценији 21. века, где стварност постојећих држава белодано показује да је интервенционистички концепт државе нужност. Саобразно томе, у поретцима савремених држава јавни интерес, као „суштинска потреба једне целине, својом важношћу надређена појединачним интересима грађана и организација“,[7] представља „вишу норму“ у односу на субјективна права

Треће, Суд налази да појам „приватан живот“ обухвата физички и морални интегритет личности, укључујући следећа лична добра: име, пол, сексуални живот, тајност преписке и телефонске и електронске комуникације, личне податке и др. Ibid, стр. 234-250. На крају, становиште Суда можемо апстраховати констатацијом да појам „приватан живот“ обухвата физички и духовни интегритет личности, а да је циљ јемства, које се пружа чл. 8 Конвенције да обезбеди развој личности сваког лица без спољног мешања у његове односе са другим људима.

5 Предраг Димитријевић, Право информационе технологије, Ниш, 2011, стр. 245.

6 Класичну концепцију приватности определиле су судије Samuel Warren и Louis Brandais, који су крајем 19. века у раду „Право на приватност (The Right to Privacy). в. Предраг Димитријевић, op. cit., стр. 244.

7 Зоран Томић, Управно право, Београд, 2011, стр. 198.

грађана, што узрокује неопходност ограничења субјективних права. Таквој нарави (форми) државе не пристаје класична концепција приватности, јер приватни живот појединца у поретку такве државе не може остати сасвим ван захвата државне власти. Напослетку не и због тога што и сами интереси грађана то налажу. Уместо „права да буде остављен на миру“, супстрат савремене концепције приватности сачињава право да прикупљање, обрада и коришћење личних података остану под контролом лица о чијим се подацима ради. Та се контрола очитује се у правно гарантованом „кругу оправданих интереса“[8]

8 „Круг оправданих интереса“, према становишту Владимира В. Водинелића, обухвата следећа права лица: 1) да може да употреби податак о себи, да се послужи њиме, да му се пружи прилика да га сам дâ, да се податак прибави од њега самог; 2) да се одређене врсте података о њему уопште не прикупљају, обрађују, преносе и користе; 3) да може да одлучи хоће ли и које податке о себи дати, коме, када и за коју сврху, смеју ли се обрађивати, преностити трећима и користити; 4) да податке о њему прикупљају, обрађују, преносе и користе само субјекти који су на то овлашћени; 5) да (овлашћени субјекти) о њему прикупљају, обрађују, преносе и користе само оне податке, који су (им) неопходни за допуштену делатност и сврху; 6) да се о њему прикупљају, обрађују, преносе и користе само истинити, потпуни, незастарели, јасни, једнозначни подаци, да се подаци не промене или да им се не измени смисао издвајањем из изворног контекста, из контекста примарне намене или повезивањем са другим подацима; 7) да може да (са)зна који су то субјекти који би могли располагати и можда располажу подацима о њему, и којом врстом тих података (који субјекти могу да прикупљају, обрађују, преносе и користе које личне податке); 8) да може да сазна да ли и које податке о њему поседују конкретан, одређени субјект, којих их је прикупио, од кога их је прибавио и коме их преноси; 9) да може да провери да ли међу подацима о њему, које прикупља, обрађује, преноси и користи дотични субјект, има и таквих за чије прикупљање, обраду, преношење и коришћење тај субјект није овлашћен; 10) да може да провери да ли међу подацима о њему, које прикупља, обрађује, преноси и користи дотични субјект, има и таквих који том субјекту нису неопходни за допуштену сврху и делатност; 11) да може да провери да ли су подаци о њему, које дотични субјект прикупља, обрађује, преноси и користи, истинити, потпуни, незастарели, јасни, једнозначни, непромењени, да ли им се изменило значење издвајањем из изворног контекста, из контекста примарне намене или повезивањем с другим подацима; 12) да може да спречи да субјект започне прикупљање, обраду, преношење или коришћење података о њему ако за то није овлашћен, или ако подаци о њему нису неопходни за допуштену сврху и делатност, или ако су подаци о њему неистинити, непотпуни, застарели, нејасни, вишезначни, промењени или би се променили, измењеног смисла или би им се изменио смисао издвајањем из изворног контекста, из контекста примарне намене или повезивањем са другим подацима; 13) да може да исходи, постигне да се (привремено) прекине (већ започето) прикупљање, обрађивање, преношење или коришћење података о њему, док се не разјасни је ли субјект за то овлашћен (постоји ли правни основ, овлашћење за прикупљање, обраду, пренос или коришћење тих података), или јесу ли ти подаци неопходни за допуштену сврху и делатност, или јесу ли ти подаци неистинити, непотпуни, застарели, нејасни, вишезначни, промењени, измењеног значења издвајањем из изворног контекста, из контекста примарне намене или повезивањем с другим подацима, као и да може да исходи да се (трајно) обустави прикупљање, обрађивање, преношење или коришћење података о њему у погледу којих се то што је спорно не може разјаснити (non liquet); 14) да може да постигне да се бришу подаци о њему ако су прикупљени, обрађивани,

титулара, који не могу бити нарушени ни у једном случају јавним интересом руковођеног прикупљања, обраде и коришћења личних података.[9] Дакако, „круг оправданих интереса" појединца о чијим се подацима ради происходи из природе савремене интервенционистичке државе. Наиме, не само у погледу односа поводом обраде личних података, већ и код других правних института (експропријација, одговорност државе за штету проузроковану законитим радом, примена полицијских овлашћења и др.), у сржи законописања стоји нужност успостављања „правичне равнотеже" између државног интервенционизма и субјективних права, односно јавног и приватног интереса, која („правична равнотежа") представља услов легимитета и опстанка савремене правне државе.

II. Правни режим заштите личних података

Упоредно право познаје два приступа заштити личних података[10]. Први приступ[11] оличава доношење закона којим се на свеобухватан начин уређује заштита личних података, док потоњи[12] обухвата парцијалну нормативно-правну регулативу, усмерену на поједине аспекте обраде личних података. Притом, осим свеобухватног правног нормирања, одређујућу карактеристику првога приступа представља конституисање посебног органа у чијој се надлежности налази старање о заштити личних података.[13]

преношени или коришћени без правног основа, без овлашћења за то, или ако нису били или више нису неопходни за допуштену сврху и делатност, да се обнове подаци о њему ако су избрисани без правног основа, да се врате подаци о њему ако су пренети неовлашћеном субјекту или без правног основа, да се исправе неистинити, допуне непотпуни, ажурирају застарели, појасне нејасни, определи значење вишезначних, успостави пређашње стање промењених, коригују они чије значење измењено издвајањем из изворног контекста, из контекста примарне намене или повезивањем с другим подацима, да се раздвоје од података који им мењају смисао, да се повежу са подацима који им дају прави смисао, и др.; 15) да се похрањени подаци не повреде, оштете, изгубе, отуђе или униште, и уопште обезбеде од утицаја неовлашћених. в. Владимир В. Водинелић, *op. cit*., стр. 192-193.

9 Предраг Димитријевић, op. cit., стр. 247.

10 Заштити личних података посвећени су и извори међународнога права. Наводимо најважније: *Смернице за регулисање досијеа са компјутеризованим личним подацима E/CN.4/1990/72 (усвојен Резолуцијом Генералне скупштине УН бр. 45/95); Смернице OECD-a из 1980; Европска конвенција о заштити лица у односу на аутоматску обраду личних података (усвојена у Савету Европе 1981.); Директиве Европске уније: Директива о слободној циркулацији и процесуирању података 95/46; Директива о правној заштити база података 96/9; Директива о заштити личних података (1998).*

11 Етаблиран је у највећем броју земаља (све државе чланице Европске уније, Аустралија, Нови Зеланд, Канада и др.).

12 Постоји у Сједињеним Америчким Државама.

13 Орган о којем овде говоримо може бити инокосног или колегијалног принципа организације руковођења. Као инокосни може постојати у виду „Комесара за заштиту

Одређујућа обележја првога приступа на снази су и у нашем важећем праву. Темељ заштите личних података у нас постављен је уставном нормом[14] којом се јемчи заштита података о личности (чл. 42. став 1.), са произилазећим правом свакога да буде обавештен о прикупљеним подацима о својој личности, као и правом на судску заштиту због њихове злоупотребе (чл. 42. став 4.). Устав забрањује и кажњава употребу података о личности изван сврхе за коју су прикупљени, осим за потребе вођења кривичног поступка или заштите безбедности државе, на начин предвиђен законом (чл. 42. став 3.). На основу предочених уставних норми, године 2008. донесен је Закон о заштити података о личности[15] (у даљем тексту закон),[16] којим је старање о заштити података о личности стављено у надлежност Повереника за информације од јавног значаја и заштиту података о личности.

Најпре истакнимо да законом нису обухваћене поједине групе података: 1) подаци који су доступни свакоме, објављени у јавним гласилима и публикацијама или приступачни у архивама, музејима и другим сличним организацијама; 2) подаци који се обрађују за породичне и личне потребе и нису доступни трећим лицима; 3) подаци који се о члановима политичких странака, синдиката и других удружења обрађују од стране тих организација, али под условом да члан да писмену изјаву да одређене одредбе закона не важе за обраду података о њему за одређено време, али не дуже од његовог чланства у тој организацији; и 4) подаци које је лице објавило о себи, а способно је да се само стара о својим интересима.

Обрада података о личности,[17] врши се по правилу уз пристанак лица, који подлеже строгим условима пуноважности. Полазећи од пристанка лица, овде

приватности“ (Канада), „Повереника за заштиту личних података“ (Немачка), или „Регистрара за заштиту података“, што је случај у Великој Британији. У колегијалном облику постоји као „Комисија за заштиту личних података“ (Аустрија), „Уред за заштиту приватности“ (Белгија), „Комисија за заштиту података“ (Шведска), „Национална комисија за информатику и слободе“ – тзв. CNIL (Француска), те као „Рачунарски одбор“ на Исланду. в. Стеван Лилић, *Законодавство о заштити података, упоредно-правни осврт,* Анали Правног факултета у Београду, 2-3/1989, стр. 278-284.

14 Устав Републике Србије («Сл. гласник РС», бр. 98/2006), чл. 42. став. 1-4.

15 Законом се уређују услови за прикупљање и обраду података о личности, права лица и заштита права лица чији се подаци прикупљају и обрађују, ограничења заштите података о личности, поступак пред надлежним органом за заштиту података о личности, обезбеђење података, евиденција, изношење података из Републике Србије и надзор над извршавањем овог закона.

16 «Сл. гласник РС», бр. 97/2008.

17 Обрада података је свака радња предузета у вези са подацима као што су: прикупљање, бележење, преписивање, умножавање, копирање, преношење, претраживање, разврставање, похрањивање, раздвајање, укрштање, обједињавање, уподобљавање, мењање, обезбеђивање, коришћење, стављање на увид, откривање, објављивање, ширење, снимање, организовање, чување, прилагођавање, откривање путем преноса или на други начин чињење доступним,

претпоставке правоваљаности обраде података, законописац је утврдио листу случајева недозвољене обраде података. Недозвољена обрада података постоји: када физичко лице није дало пристанак или се обрада врши без законског овлашћења; ако се обрада врши у другу сврху од оне за коју је одређена (без обзира на пристанак или законско овлашћење); када сврха обраде није јасно одређена, ако је измењена, недозвољена или већ остварена; уколико је лице на које се подаци односе одређено или одредиво и након што се оствари сврха обраде; ако је начин обраде недозвољен; уколико је податак који се обрађују непотребан или неподесан за остварење сврхе обраде; ако су број или врста података који се обрађују несразмерни сврси обраде; и, напослетку, када је податак неистинит и непотпун, односно када није заснован на веродостојном извору или је застарео. Осим тога, поједини подаци о личности не могу бити предмет обраде, ни уз пристанак лица. Тако, нарочито осетљиви подаци који се односе на националну припадност, расу, пол, језик, вероисповест, припадност политичкој странци, синдикално чланство, здравствено стање, примање социјалне помоћи, жртву насиља, осуду за кривично дело и сексуални живот могу се обрађивати само на основу слободно датог пристанка лица, осим када закон обраду не допушта ни уз пристанак.

С друге стране, премда је пристанак по правилу услов, у појединим случајевима обрада података о личности биће правоваљана и без пристанка лица: када је неопходно остварити животно важне интересе лица (живот, здравље и сл.); у сврху извршења законских или уговорних обавеза закљученим између лица и руковаоца, као и ради припреме закључења уговора; у другим законом нормираним случајевима, а ради остварења претежног оправданог интереса лица, руковаоца или корисника; као и у случају када је органу власти обрада неопходна ради обављања послова из своје надлежности у циљу остваривања интереса националне или јавне безбедности, одбране земље, спречавања, откривања, истраге и гоњења за кривична дела, економских, односно финансијских интереса државе, заштите здравља и морала, заштите права и слобода и другог јавног интереса. Закон допушта и обраду података у историјске, статистичке и научноистраживачке сврхе, под условом да не служе доношењу одлука или предузимању мера према одређеном лицу.

Лице на које се подаци односе легитимисано је да захтева обавештење о обради, да изврши увид у податке, као и да поднесе захтев за издавање копије податка. Гарантије предоченим правима пружена су путем правних средстава, која стоје на располагању лицу на које се подаци односе, а наиме да противу

прикривање, измештање и на други начин чињење недоступним, као и спровођење других радњи у вези са наведеним подацима, без обзира да ли се врши аутоматски, полуаутоматски или на други начин. Обрађивач података је физичко или правно лице, односно орган власти, коме руковалац на основу закона или уговора поверава одређене послове у вези са обрадом.

решења руковоаца[18]изјави жалбу Поверенику за информације од јавног значаја и заштиту података о личности, те да противу коначнога решења Повереника може тужбом да покрене управни спор пред Управним судом, које је решење сасвим на висини принципа правне државе. Излагање општега режима заштите података о личности у нас окончајмо закључком да је важећи Закон највећма сагласан упоредно-правним и међународно-правним стандардима у овој области.

Међутим, постојање матичног општег закона по мери принципа правне државе, спрам заштите личних података, стоји као неопходан, али не и довољан услов. Упоредно право јасно нам казује да систем заштите података о личности уистину не може бити потпун и правно-логички конзистентан уколико је утемељен само на једном општем закону. Заправо, потпуност и делотворност система заштите личних података постојаће једино када се на основу општега закона о заштити личних података донесу посебни закони и одговарајући прописи подзаконског ранга. Да наречено заиста представља услов целовитости и ефикасности система заштите личних података белодано показује и наше важеће право. Наиме, Закон о заштити података о личности у нас представља матични општи закон, чије одредбе и начела захтевају даљу законску конкретизацију у појединим, спрам заштите личних података, врло осетљивим областима, као што су: национална безбедност, одбрана, кривично правосуђе, медицински подаци, медији, уметничко и књижевно изражавање, телекомуникације и Интернет, биометрија, видео-надзор, банкарство и финансијски подаци, политички избори, директни маркетинг, електронски документи и електронски потпис, агенције за физичко-техничку заштиту, овлашћења приватних детектива и др.[19] У периоду после доношења Закона о заштити података о личности законска конретизација извршена је у малом броју горе предочених области, с тим да су поједини донесени закони очигледно несагласни, не само важећем матичном закону о заштити података о личности, него и Уставу Републике Србије. Осим тога, Влада Србије није усвојила ни акт о начину архивирања и о мерама заштите нарочито осетљивих података, као ни Акциони план за спровођење Стратегије заштите података о личности, што нам допушта да закључимо да систем заштите личних података у нас још није заокружен. Манљивост српског система заштите личних података узрокована је и чињеницом недоследног неизвршавања законске обавезе појединих руковаоца о похрањивању сопствених база личних

18 Руковалац података је физичко или правно лице, односно орган власти који обрађује податке.

19 в. Стеван Лилић, Интернет доспео до петине, www.politika.rs/rubrike/Sta-da-se-radi/Internet-dospeo-do-petine.sr.html 10. 3. 2011; Александар Ресановић, Рокови прошли, прописа нема, www.politika.rs/rubrike/Sta-da-se-radi/Rokovi-prosli-propisa-nema.sr.html 5. 3. 2011; Родољуб Шабић, Чији су наши лични подаци, 2011. 01. www.istinomer.rs/teme/ciji-su-nasi-licni-podaci/27. 01. 2011. (странице последњи пут посећене 14. 11. 2012.)

података у централни регистар Повереника за информације од јавног значаја и заштиту података о личности.

III. Неоправдано (нелигитимно) ограничавање приватности путем државне интервенције засноване на примени информационих технологија

Као што смо већ видели, обрада личних података је допуштена само уколико за њу постоји изрични законски основ или уколико се врши уз пристанак лица о чијим се подацима ради. Без тога обрада података је недозвољена, без обзира ко је врши и о каквој врсти обраде је реч – прикупљање, коришћење, стављање на увид, чување, ширење или објављивање. Будући недозвољена, таква обрада личних података разуме се да је и неоправдана (нелегитимна). Међутим, због неслућених размера примене информационих технологија, ваља размотрити могућност да допуштени видови обраде личних података (било да су засновани непосредно на закону, или се врше уз пристанак лица) представљају неоправдано (нелегитимно) ограничавање приватности појединца. Реч је о томе да примена информационих технологија представља целисходан инструмент задовољења истинских јавних потреба, само под условом да приватност појединца не подлеже већим ограничењима у односу на конвенционалну (традиционалну) обраду личних података. Када, пак, аутоматизована обрада личних података, у односу на конвенционалну, у крајњем исходу значи повећану ефикасност за онога ко се служи таквом обрадом и већи ризик угрожавања приватности појединца, посреди је неоправдано (нелигитимно) ограничавање приватности. У таквим случајевима конвенционални (традиционални) захвати државне власти у приватну сферу појединца (у зависности од облика и интезитета примене информационих технологија) мењају своју природу и сврху, истичући у први план властодржачку потребу задирања у слободу појединца. Предочено мењање природе својстава постоји и у бићу самог информационог друштва. Информационим друштвом можемо сматрати оно друштво које функционише претежно помоћу информационих технологија, које као снага напретка служи и интересима грађана. Његова супротност јесте тзв. информационо контролисано друштво“ (друштво информатичке репресије), када центри моћи користе информационе технологије ради надзора над понашањем грађана.[20]

У правним поретцима савремених држава, типове неоправданог ограничавања приватности појединца, применом савремених информационих технологија, установили смо код издавања биометријских личних докумената, као и код појединих видова надзора електронске комуникације грађана.

20 Оливер Суботић, op. cit., стр. 50.

1. Биометријски идентификациони документи

Идентификациони документи у конвенционалном (папирнатом) облику (лична карта, пасош, возачка дозвола), као израз консензуса јавног и приватног интереса, начелно представљају допуштен и оправдан вид задирања у приватност појединца. Карактер оправданог задирања у приватност појединца произлази из чињенице да идентификациони документи представљају неопходну претпоставку нормалног одвијања друштвеног живота и остваривања зајемчених права грађана. С тога, прикупљање, обрада и коришћење личних података у поступку издавања конвенционалних идентификационих докумената постоји као разумљиво и нужно ограничавање приватности, зарад остваривања оправданог задатка савремене интервенционистичке правне државе. Међутим, развојем информационих технологија настају електронски идентификациони документи, који, видећемо касније, могу променити природу и сврху у тој мери да њихов карактер незаменљиве претпоставке нормалног одвијања друштвеног живота постане сенка властодржачког средства надзора.

Електронски идентификациони документи могу постојати као биометријски и небиометријски. Израз биометрија грчког је порекла и представља кованицу речи bios (живот) и metrion (мерење). Најсажетије казано, биометријом се означава идентификација особе на основу њених биолошких особина, из чега можемо закључити да су беометријски методи идентификације грађана засновани на мерењу одређених својстава организма, особеним за сваког човека, ради потврђивања његовог идентитета у друштвено-институционалном смислу.[21] Имајући то у виду, биометријским називамо оне правно-информационе системе који користе различита физио-биолошка својства и/или мерења понашања људског тела која се могу користити за конкретну идентификацију дате особе.[22]И коначно, биометријски идентификациони документи су само они електронски документи који садрже карактеристичне биометријске податке њеног имаоца.

У карактеристичне традиционалне биометријске податке спадају: својеручни потпис (познат још у најранијим културним круговима), отисци прстију, облик прстију, шаке, руке и др. Савремене информационе технологије омогућиле су дигитализацију биометријских података, којој групи припадају дигитална обрада слике лица из неколико перпектива, дигитални отисак прстију, дигитални својеручни потпис, скен очне рожњаче и др. Напослетку, напоредо са развојем информационих технологија настаје усавршавање биометријских система идентификације, што омогућава проширивање листе биометријских података новим биометријским подацима: генерисање тродимензионалног

21 Према: Ibid, стр. 20.

22 Ibid, стр. 20.

модела лица, препознавања распореда вена, анализе ДНК структуре, детекцију мириса и специфичних хемијских својстава коже за сваког човека.[23]

У упоредном праву примена биометријске технологије варира од државе до државе. Посматрано у односу на поједине врсте идентификационих докумената, може се закључити да је у упоредном праву биометријска технологија прихваћена као правило код издавања пасоша, док је у погледу личних карти (још увек) у сенци њеног конвенционалног облика.

Правило о облигаторности биометријских пасоша новијег је датума. Наиме, њихово увођење дошло је као резултат политике Сједињених Америчких Држава у периоду непосредно након напада који су се догодили 11. септембра 2011. године.[24]Сједињене Америчке Државе најпре су (USA Patriot Act - потписан 26. октобра 2001. и Законом о повећаној безбедности границе и реформи визног система из 2002.) поседовање биометријског пасоша поставиле као услов уласка на њихову територију, а затим је Међународна организација за цивилно ваздухопловство Уједињених Нација године 2003. прописала стандард (ICAO 9303) о електронским пасошима који ће садржати биометријске личне податке. Стандард (ICAO 9303) предвиђа дигитализовану слику лица, не захтевајући притом образовање централне базе података. Предочени стандард прихваћен је од стране Европске уније и Савета Европе, с том разликом што биометријски пасоши европских држава чланица дотичних организација, поред дигитализоване слике лица садрже и дигитализоване отиске прстију, чиме су европске државе предвиделе више биометријских података, него што је случај у Сједињеним Америчким Државама. Иако иницијатори и покровитељи увођења биометријских пасоша, биометријски пасоши у Сједињеним Америчким Државама садрже само дигитализовану слику лица. Ипак, заједничка одлика биометријских пасоша Сједињених Америчких Држава и европских јесте чињеница непостојања централних база података.

У погледу личних карти, упоредно право познаје неколико решења.[25] Прво, постоје државе које нису увеле личну карту као обавезан идентификациони документ. То су државе англо-америчког правног круга у којима карактер идентификационог документа по правилу имају возачке дозволе. Осим тога, личне карте нису обавезан идентификациони документ у појединим европским државама (нпр. Данска). Друго решење очитује се у постојању личне карте конвенционалног облика (папирнатог или пластифицираног). Примера ради, тој групи држава припадају Француска, Немачка и Грчка. На крају, трећи модел јесу

23 Ibid, стр. 18-19.

24 11. септембра 2001. дошло је до кординисаних напада на Сједињене Америчке Државе. Напади су извршени авионима, који су претходно отети. Два авиона су ударила у зграду Светског трговинског центра, трећи је ударио у зграду Пентагона у Вашингтону, док се четврти срушио у области саставне државе Пенсилваније.

25 Оливер Суботић, op. cit., стр. 71-84.

електронске личне карте, код којих разликујемо биометријске и необиметријске. Небиометријске електронске личне карте могу постајати као обавезне (Белгија, Естонија) или необавезне (Норвешка, Финска). Беометријске личне карте исто тако могу почивати на принципу облигаторности (Шпанија, државе „трећег света“) или на принципу добровољности издавања, где спада и Србија.

Биометријске личне карте уведене су у нас Законом о личној карти[26] из 2006. године.[27] Куриозитет тог закона огледао се у чињеници да је њиме установљено обавезно издавање биометријских личних карти, као и то да је њиме било предвиђено образовање централне базе биометријских података (дигитализованих отисака прстију, дигитализоване слике лица са фацијалним особеностима и дигитализованим потписом). Под притисцима јавног мњења, законској норми о обавезном издавању биометријских личних карти била је придодата Уредба о упису података у образац личне карте,[28] којом је установљен принцип добровољног издавања биометријских личних карти. Принцип добровољности у издавању биометријских личних карти касније је потврђен изменама и допунама Закона о личној карти.[29]

У чему се огледа неоправдано задирање у приватност појединца издавањем биометријских личних докумената? Полазећи од тога да је оправдано задирање у приватност само оно које служи легитимном јавном циљу, увођење биометријских докумената под императивом је задовољења јавног и приватног циља. Када говоримо о првом, потребно је да биометријски идентификациони документи представљају неопходан услов остваривања јавног интереса, који се на други начин успешно не би могао постићи, док у погледу потоњег, биометријски идентификациони документи не смеју стварати већу опасност злоупотребе личних података и приватности појединца. Притом, према принципу сразмерности, чија је примена овде опредељена природом ствари, тај однос јавног и приватног могли бисмо изразити тако што ћемо закључити да увођење биометријских идентификационих докумената неће уследити, ако су штетне последице по приватност појединца веће у односу на оне ради чијег спречавања би се посегло за њиховим увођењем.

---

26 „Сл. Гласник РС“, бр. 62/06.

27 У Србији је још 2003. купљена скупоцена опрема ради инсталирања биометријског система идентификације.

28 „Сл. гласник РС“, бр. 4/2007. У члану првом Уредбе стоји: „Само на основу изричите сагласности лица коме се издаје лична карта у образац личне карте може да се угради чип који у том случају садржи и податак о пребивалишту и адреси стана лица коме се издаје лична карта.“ Осим Закона и Уредбе донесен је и Правилник о личној карти („Сл. гласник РС“, бр. 11/2007), као извршно-спроводбени пропис.

29 „Сл. гласник РС“, бр. 36/2011.

Увођење биометријских докумената правда се потребом борбе против тероризма и организованог криминала, као и потребом модернизације управе.[30]

Како биометријска технологија изискује драстично увећавање броја информација које држава поседује о појединцу, биометријски идентификациони документи несумњиво олакшавају извршавање државних задатака. У том погледу веће могућности контроле држави омогућавају успешније супротстављање тероризму и организованом криминалу. Међутим, биометријски документи нити су нужан услов постизања тог циља, нити се пак зарад остваривања тога циља у стање „основане сумње“ сме стављати сваки ималац биометријског личног документа. Уосталом, ако узмемо у обзир да биометријска лична документа пуни замах добијају након терористичких напада у Сједињеним Америчким Државама, парадоксалност тих циљева долази и одатле што је иницијатор и покровитељ увођења биометријских докумената (биометријских пасоша) држава која уједно стоји на челу „глобалног тоталитаризма“. Када је реч о модернизацији управе, искуства информационо најразвијенијих држава казују нам да напредни принцип е-управе није утемељен на биометријској технологији.[31]

С друге стране, биометријски систем идентификације носи са собом бројне ризике по слободу појединца. Ради се најпре о томе да издавање биометријских докумената може за последицу имати и образовање централизоване базе биометријских података.[32]Централизоване базе биометријских података омогућавају носиоцима империјума власти да располажу великим бројем личних података, из чега извире велики тоталитарни потенцијал.[33] Сасвим је јасно да је у погледу безбедности и приватности биометријских података грађана прихватљивији систем у којем подаци не напуштају идентификациони документ. Прецизније речено, то је систем у којем не постоји позадинска централна база података и у коме је ималац карте потпуни и одговорни власник биометрије у електронском облику.

---

30 Оливер Суботић, Биометријски пасоши: чињенице и контроверзе, „Православље“, бр 1024/2009, http://pravoslavlje.spc.rs/broj/1024/tekst/cinjenice-i-kontroverze/ (страница последњи пут посећена 5. новембра 2012.)

31 Е-управа, као израз информационог друштва у служби је грађана. У државама е-управе приоритетне јавне услуге потпуно су информатизоване, из чега произлази непостајање писане или шалтерске комуникације.

32 У стручним круговима преовлађује став да је уместо централне базе података далеко безбедније и по приватност појединаца боље тзв. решење 1:1 („један на један“) идентификације, где су биометријски подаци смештени само на смарт карти и не напуштају је приликом аутентфикације идентитета, што имаоцу биометријског документа пружа неупоредиво већу контролу над биометријским подацима.

33 Многи у биометријским идентификационим документима виде прву етапу у тзв. трофазном процесу: прво један чипом снабдевен документ, потом једини документ са чипом и на крају само чип, као документ који се не носи у џепу, већ у телу под кожом.

Заговорници увођења биометријске технологије притом истичу да су савремени биометријски системи савршени, што демантују и теорија и пракса. Централизоване базе биометријских података могу бити мета напада и споља и из унутра. Суштина проблема је у чињеници да пракса показује да не постоји стопроцентно заштићени електронски систем који би заштитио податке од неауторизованог коришћења.[34]

Дакле, са становишта субјективних права појединаца, типично неоправдано задирање у приватност појединца постоји код система биометријске технологије заснованој на обавезности издавања биометријских докумената и централизованој бази биометријских података. Мањи тоталитарни потенцијал постоји код система биометријске идентификације утемељеној на принципу добровољности издавања биометријских личних докумената, без стварања јединственог регистра биометријских података. Но, по нашем суду, било да се ради о првом или другом систему, нелегитимност (неоправданост) биометријског задирања проузрокована је чињеницом непостојања „правичне равнотеже" између државног интервенционизма и субјективних права.

2. Надзор електронске комуникације грађана од стране органа јавне власти

Надзор електронске и других средстава комуникације у правном поретку савремене правне државе почива на неколико темељних принципа. Најпре, реч је о једном од основних субјективних права, од чије се неповредивости само изузетно може одступити. Саобразно принципу правне државе, одступања од тајности писама и других средстава комуницирања, дозвољена су само на одређено време и на основу одлуке суда, уколико су неопходна за вођење кривичног поступка или за заштиту безбедности државе. Предочено становиште у свему је заступљено у важећем Уставу Републике Србије (члан 41.). Дакако, ограничавање тајности комуникације грађана спроводи се на основу закона, али не и непосредно законом! Следствено томе, случајеви одступања од неповредивости тајности комуникације грађана непосредно законом, без одобрења суда, дубоко су противни принципу правне државе. То тим пре што су могућности контроле државе над појединцима у савременом информационом друштву достигле неслућене размере, због чега се, услед непостајања судскога одобрења, у питање доводи и сам легитимитет савремене правне државе.

Типичне случајеве одступања од принципа правне државе у погледу тајности (слободе) комуникације грађана нуди нам важеће право Републике Србије. Премда се то не односи на важећи Устав Србије, законски оквир електронских и других комуникација је неконзистентан, неусаглашен и добрим дело несагласан са праксом Европског суда за људска права у Стразбуру, као и са стандардима

34 Оливер Суботић, op. cit., стр. 45.

права Европске уније. Противно начелу правно-нормне хијерархије, у важећем српском праву на снази су законске норме које надзор комуникације грађана уређују противно Уставу Србије. По чисто временском следу поменимо најпре Закон о телекомуникацијама,[35] који је био на снази до 31. децембра 2011. године. Дотични закон (члан 55. став 1.) предвиђао је одступање од тајности комуникације грађана одобрењем суда, али и непосредно законом, на основу чега је Уставни суд донео одлуку (Iуз-149/2008 од 28.05.2009) о његовој несагласности са Уставом Србије. Област електронских комуникација у нашем праву сада је уређена Законом о електронским комуникацијама (у наставку Закон),[36] који ће, по свему судећи, доживети судбину свог претходника. Наиме, Закон предвиђа да ће се задржаним подацима о оствареној и неоствареној комуникацији, без задирања у садржај комуникације, приступати, не на основу одобрења суда, већ по налогу државних органа (политичке и редовне полиције),[37]због чега је иницира поступак оцене уставности закона. У међувремену окончан је поступак оцене уставности једног другог закона, који је донесен годину дана пре Закона о електронским комуникацијама. Реч је о Закону о војно-безбедносној агенцији и војно-обавештајној агенцији[38], који (члан 13. став 6. и члан 16. став 2.) је предвидео да тајни електронски надзор телекомуникација и информационих система ради прикупљања података о телекомуникационом саобраћају и локацији корисника, без увида у њихов садржај, може да наложи директор Војно-безбедносне агенције или лице које он овласти. Одлуком Уставног суда, дотични чланови Закона су оглашени неуставним (IУз-1218/2010 од 19.04.2012). Изложена законска решења белодано показују да је законски оквир у нашем важећем праву несагласан стандардима Европског суда за људска права у Стразбуру.[39] Према правном схватању Европског суда за људска права, информације везане за време и дужину телефонског разговора, а посебно изабрани бројеви саговорника, представљају „саставни део комуникације путем телефона“. Следствено томе, уступање тих информација државном органу без пристанка претплатника, по

35 „Сл. гласник РС“, бр. 44/2003.

36 „Сл. гласник РС“, бр. 44/2010.

37 (в. члл. 128-129. Закона о електронским комуникацијама).

38 „Сл. гласник РС“, бр. 88/2009.

39 Овде додајмо да се пред Уставним судом покренута иницијатива за оцену уставности Законика о кривичном поступку („Сл. гласник РС“, бр. 72/2011), са образложењем да слово Законика ставља у надлежност Јавном тужиоцу (не само суду) да наложи предузимање мера тајног надзора комуникације. Осим тога, поменимо да је правно-технички приступ, који овде излажемо, у праву Србије заступљен и у подзаконској сфери. Тако је, године 2008. Републичка агенција за телекомуникације (РАТЕЛ), донела Техничке услове за подсистеме, уређаје, опрему и инсталације интернет мреже, којима је био предвиђен неограничени надзор и архивирање свих облика електронских комуникација. в. Предраг Димитријевић, *Право приватности на интернету (позитивноправни оквир)*, Зборник радова Правног факултета у Нишу, 2008, стр. 53-55.

мишљењу Суда представља мешање у права зајемчена чл. 8. Конвенције (права преписке и права на приватан живот).[40]

Према томе, принцип судске контроле законитости овде стоји као услов постојања савремене правне државе. По нашем суду, легитимитет свог појмовног одређења, савремена правна држава може обезбедити једино путем независне, делотворне и правичне судске функције државне власти. С друге стране, природа и облици државног интервенционизма савременог доба наметнули су питања, која се у периоду постанка правне државе нису могла ни замислити. Белодано је да се услед нарушавања „правичне равнотеже“ између државног интервенционизма и субјективних права, које настаје у правном поретку савремене правне државе, основано може поставити питање њеног легитимитета. С тим у вези, стоји и питање да ли савременој правној држави одговара сентенца „од демократије ка тоталитаризму“?[41]

РЕЗИМЕ

Лични подаци су део права на приватност, једног права-слободе, о којем влада несагласје у правној књижевности. Лични податак је свака информација која се односи на физичко лице, без обзира на облик у коме је изражена (папир, трака, филм, електронски медиј). Постоје две категорије личних података. Прва категорија обухвата податке који чине физички део саме личности. Реч је о биометријским подацима (својеручни потпис, отисак прстију, дигитализована слика лица, скен очне рожњаче и др.), који као непроменљиви и неодвојиви од личности представљају личне податке у ужем смислу. Другој категорији личних података припадају типови података који говоре о личности, али нису њен физички део (име, национална припадност, пол, језик, вероисповест и сл.). Будући одвојиви од личности, те и потенцијално заменљиви, ови типови података представљају личне податке у ширем смислу, за које ћемо из разлога јасног предочавања и разликовања употребити израз „подаци о лицу“.

Обрада личних података је допуштена само уколико за њу постоји изрични законски основ или уколико се врши уз пристанак лица о чијим се подацима ради. Без тога обрада података је недозвољена, без обзира ко је врши и о каквој врсти обраде је реч – прикупљање, коришћење, стављање на увид, чување, ширење или објављивање.

40 Жил Дитертр, op. cit., стр. 245-246; Милан Николић, *Практични аспекти заштите приватности корисника и безбедности електронских комуникационих мрежа и услуга у Србији*, www.telekomunikacije.rs (страница последњи пут посећена 5. новембра 2012).

41 О томе: Иван Иљин: «У потрази за праведношћу», Светигора 2001; Видети и код: М. Петровић, *Појам тоталитаризма,* Архив за правне и друштвене науке, 1-3/1996, стр. 463-471. Од истог аутора: Наука о управљању као претпоставка управне политике, Ниш, 2011. стр. 124.

Ограничавање приватности обрадом личних података у правима савремених држава – премда правоваљано, може бити оправдано (легитимно) и неоправдано (нелигитимно). Оправдано ограничавање намеће „збиљски јавни интерес", док срж неоправданог чини „симуловани (привидни) јавни интерес", који прикрива властодржачку потребу запоседања слободе појединца. Код потоњих реч је о томе да примена информационих технологија представља целисходан инструмент задовољења истинских јавних потреба, само под условом да приватност појединца не подлеже већим ограничењима у односу на конвенционалну (традиционалну) обраду личних података. Када, пак, аутоматизована обрада личних података у односу на конвенционалну у крајњем исходу значи повећану ефикасност за онога ко се служи таквом обрадом и већи ризик угрожавања приватности појединца, посреди је неоправдано (нелигитимно) ограничавање приватности. У таквим случајевима конвенционални (традиционални) захвати државне власти у приватну сферу појединца (у зависности од облика и интезитета примене информационих технологија) мењају своју природу и сврху, истичући у први план властодржачку потребу задирања у слободу појединца.

У правним поретцима савремених држава, типове неоправданог ограничавања приватности појединца применом савремених информационих технологија установили смо код издавања биометријских личних докумената, као и код појединих видова допуштеног надзора електронске комуникације грађана.

Miloš Prica, LL.M.
Teaching Assistant,
Faculty of Law, University of Niš

Limiting Privacy by State Intervention based on the Application of Information Technologies

Summary

In this paper, the author deals with an aspect of privacy involving personal data, which are frequently subject to different forms of state intervention in the contemporary legal systems. The intervention of the contemporary legal state is most prominent in the application of information technologies, which generate ample opportunities for encroaching on the privacy of an individual. Being legally grounded, this intrusion into one's private life by collecting, processing and using one's personal data by the state and governing authorities ("holders of imperium") may be a valid expression of different public interests. In spite of being valid and legally grounded, this interference with one's privacy may be either justified (legitimate) or unjustified (illegitimate). The justified limitation may be imposed due to "an actual public interest", whereas the essence of the unjustified limitation is "a simulated public interest" which conceals the need of the governing authorities to encroach on the freedoms of an individual. In particular, the author focuses on the unjustified limitation of an individual's privacy, particularly given the fact that the use of new information technologies in the contemporary information society changes the nature and the purpose of conventional/ traditional forms of state intervention into one's privacy. The author endeavours to provide answer to the posed questions by analysing typical cases in the Serbian legislation and comparative law.

***Key words**: privacy, personal data, state intervention, public interest*