

УНИВЕРЗИТЕТ У НИШУ

ПРАВНИ ФАКУЛТЕТ

**ПРИНЦИПИ ЗАШТИТЕ ПРИВАТНОСТИ У
ПРАВУ СЈЕДИЊЕНИХ АМЕРИЧКИХ ДРЖАВА**

(мастер рад)

Ментор:

Проф. др Милош Прица

Студент:

Тијана Божић

М 004/23-ИТ

Ниш, 2024. године

Садржај

УВОД	1
I ПОЈАМ ЛИЧНИХ ПОДАТАКА И ЊИХОВА ЗАШТИТА	5
1. Теоријско одређење појма података	5
2. Лични подаци.....	7
3. Врсте личних података	10
4. Прикупљање и обрада података о личности.....	13
5. Крађа података.....	14
6. Заштита података о личности.....	16
6.1. Право на приватност	16
6.2. Право на заштиту података о личности	19
II ПРИНЦИПИ И ЗАШТИТА ПОДАТАКА О ЛИЧНОСТИ У ЕВРОПСКОМ КОНТИНЕНТАЛНОМ ПРАВУ	22
1. Право Европске Уније у области заштите података о личности	22
2. Општа уредба о заштити података о личности – GDPR	26
3. Начела заштите података о личности у европском праву.....	28
4. Заштита података о личности у Србији и поређење са регулативом ЕУ.....	31
III ПРИНЦИПИ И ЗАШТИТА ПОДАТАКА О ЛИЧНОСТИ У АНГЛОАМЕРИЧКОМ ПРАВУ	34
1. Англоамеричко право у области заштите података о личности.....	34
2. Правни акти која регулишу заштиту података о личности у англоамеричком праву	35
3. Начела заштите података о личности у англоамеричком праву	41
3.1. Први принцип заштите података о личности у англоамеричком праву – контрола приступа личним информацијама	41
3.2. Други принцип заштите података о личности у англоамеричком праву – правичност	49

3.3. Трећи принцип заштите података о личности у англоамеричком праву – приватност личних података	51
3.4. Четврти принцип заштите података о личности у англоамеричком праву – сигурност података	53
3.5. Пети принцип заштите података о личности у англоамеричком праву – транспарентност	55
3.6. Шести принцип заштите података о личности у англоамеричком праву – ограничење сврхе и употребе података	58
3.1. Седми принцип заштите података о личности у англоамеричком праву – одговорност.....	59
3.2. Осми принцип заштите података о личности у англоамеричком праву – минимизација.....	63
3.3. Девети принцип заштите података о личности у англоамеричком праву – квалитет и интегритет	65
IV ЗАКЉУЧАК.....	67
ЛИТЕРАТУРА.....	69
САЖЕТАК.....	77
SUMMARY	78
БИОГРАФИЈА.....	79

УВОД

Рачунари и рачунарске мреже несумњиво пружају невероватан приступ информацијама, што је довело до драматичног повећања доступних података о појединцима широм света. Сада се може пронаћи мноштво додатних информација о свакој особи, од њихове локације и кретања до њених активности, интересовања, па чак и финансијских трансакција. Међутим, са овим повећањем доступних података долази до ризика од злоупотребе, што поставља озбиљна питања о приватности и безбедности појединаца. Институције и појединци све више користе ове податке у различите сврхе, од економске до политичке користи. Неки чак прелазе границу законитости, користећи личне податке на незаконит начин. Овај експоненцијални раст података представља изазове за појединце који брину о својој приватности и безбедности, у односу на институције и друге који желе да користе ове информације у своју корист.

Јасно је да је овај тренд раста података у супротности са принципима приватности и ствара ризик тамо где постоји сукоб интереса. Заштита података постаје витална заштита индивидуалних права сваке особе и законски је регулисана у многим земљама како би се осигурало да се подаци користе одговорно и законито. Дакле, заштита података није само питање закона већ и моралне одговорности према сваком појединцу и његовој приватности. Очување интегритета личних података је од суштинског значаја за очување слободе и аутономије сваког појединца у дигиталном добу.

Право на приватност је тесно повезано са основним правима и слободама које уживају грађани, и са степеном демократије и поштовања људских права у друштву. Закони који штите приватност постоје у свим земљама, а њихов циљ је да осигурају да се лични подаци особа не користе или објављују без њихове дозволе или без законских ограничења. Ови подаци укључују све аспекте идентитета особе, од психолошких и културних до економских и породичних. Друштва која се заснивају на принципима владавине права и поштују права и слободе грађана посебно се ангажују у заштити приватности. Она се сматрају тежиштем људских слобода и поштују право сваке особе да контролише своје личне податке и приватни живот. С друге стране, друштва која теже ауторитаризму или која имају слабије институционалне механизме заштите

грађана често користе методе које угрожавају приватност и власништво над њиховим личним подацима.

За разлику од Европске уније, која има јединствен оквир, САД имају систем који се састоји од мреже савезних и државних закона и прописа који покривају обраду података у различитим индустријама и пословним операцијама. Савезни закони обично регулишу прикупљање, складиштење и коришћење осетљивих, јавно доступних личних података. С друге стране, државни прописи обично регулишу захтеве за обавештавање након што дође до кршења безбедности личних података који нису јавно доступни. Непрофитне организације које послују у САД морају да се придржавају оба нивоа закона да би испуниле захтеве.

Амерички приступ заштити личних података критикован је због своје фрагментиране природе, што може довести до празнина у заштити и недоследности у различитим секторима и државама. Овај систем може да створи изазове за предузећа која морају да се крећу кроз различите захтеве и за потрошаче којима је можда тешко да разумеју своја права и заштиту. Такође, у току је дебата о потреби за свеобухватним савезним законом о приватности података који би ускладио заштиту у свим државама и секторима. Заговорници тврде да би такав закон обезбедио јасније стандарде и јачу заштиту за потрошаче, док противници упозоравају на прекомерну регулативу која би могла да угуши иновације и наметне значајне трошкове поштовања прописа за предузећа.

Посебно у англоамеричком правном систему, концепт контроле приступа личним информацијама представља кључни аспект који обухвата низ правних норми и принципа. Принципи заштите података о личности представљају темељни оквир за разумевање начина на који се регулише приступ и коришћење личних података, а његова примена има далекосежне импликације на заштиту приватности и права појединаца. Циљ овог рада је да се истражи и анализира природа и дomet принципа заштите података о личности у контексту англоамеричког права, са посебним освртом на механизме контроле приступа личним информацијама. У том смислу, рад ће се бавити правним основама које дефинишу ове принципе, еволутивним развојем законских оквира, као и специфичним правним и институционалним решењима која су усвојена ради њихове имплементације. Посебна пажња биће посвећена анализи

регулаторних оквира који доприносе формирању и заштити права на приватност у дигиталном добу.

Научни метод представља систематски приступ стицању знања, при чему се користе утврђене технике. Избор одговарајуће методологије зависи од предмета истраживања, његових циљева и формулисаних хипотеза које ће бити проверене. У дисертацији ће се применити основне методе истраживања, укључујући анализу и синтезу. Метод анализа ће бити искоришћен за проучавање Устава из 1921. године, с циљем да се истраживачки предмет распарча на елементе. То подразумева детаљну анализу поступка доношења устава, његових садржаја и примене у пракси. Правноисторијска метода ће бити корисна за истраживање процеса доношења регулаторног оквира за заштиту података личности. Упоредноправни метод биће примењен за упоређивање принципа заштите личних података у САД и другим државама и организација, а, што ће омогућити добијање ширег увида у развој правних односа. С обзиром да правни однос представља социјални однос регулисан правним нормама, социолошка метода ће разјаснити везу између друштва и права. Она ће истражити у којој мери принципи заштите личних података у САД одговарају друштвеним околностима и како их грађани разумеју и примењују у свакодневном животу.

Рад је сачињен од Увода, три поглавља, Закључка и Литературе.

У *Уводу* рада, ауторпредставља основну тему рада, која се односи на личне податке и њихову заштиту. Нагласиће значај овог питања у савременом друштву, где је обрада података о личности постала свакодневица. Упознаће читатеља са основним циљевима истраживања и методологијом која ће се користити у раду.

Прво поглавље под насловом *Појам личних података и њихова заштита*, ће се фокусирати на теоријске анализе о подацима и конкретно на личне податке, укључујући њихове врсте и поступке прикупљања и обраде. Разматраће се и проблеми као што су крађа података и механизми заштите личних података, уз осврт на права појединаца у контексту приватности и заштите.

Друго поглавље под називом *Принципи и заштита податка о личности у европском континенталном праву* ће анализирати законодавни оквир заштите личних података у Европској унији, с посебним акцентом на Општу уредбу о заштити података

(GDPR). Поред тога, истражиће се начела заштите података у европском праву, као и упоредна анализа са правним системом Србије.

Треће поглавље носи наслов *Принципи и заштита података о личности у англоамеричком праву* и оно ће обухватити правне аспекте заштите личних података у англоамеричком праву. Анализираће се важна правна документа и принципи који регулишу ову област, као и специфичности заштите података у овој правној традицији, укључујући контролу приступа, правичност, приватност и безбедност података.

Закључак ће обухватити кључне увиде из претходних поглавља, наглашавајући важност заштите личних података у контексту глобализације и технолошког развоја. Читаоци ће бити упознати са препорукама за будућа истраживања и правне реформе у области заштите личних података.

У *Литератури* ће бити наведени сви извори и литература коришћени у раду, што ће омогућити читаоцима да пронађу додатне информације и контекст о теми заштите личних података.

I ПОЈАМ ЛИЧНИХ ПОДАТАКА И ЊИХОВА ЗАШТИТА

1. Теоријско одређење појма података

Реч „податак“ потиче од латинске речи „*datum*“, што значи „нешто дато“. У савременом контексту, подаци се дефинишу као симболи изражени нумеричким и словним знаковима или у облику аналогних или дигиталних приказа слике или звука. Ови симболи су прилагођени за пренос и интерпретацију од стране људи или аутоматизованих система преко унапред дефинисаних алгоритама. Подаци могу садржати чињенице о субјекту или објекту, укључивати статистичке бројке или чинити део ширих информација. Они представљају забележене чињенице о посматраном објекту, али сами по себи подаци су лишени суштинског значења. Они функционишу као кодови који се, према одређеним правилима, могу декодирати. Тек када се подаци декодирају, повежу са другим подацима, обрађују и интерпретирају, они постају информација.¹

Термин подаци се често користи за означавање специфичне карактеристике својствене ентитету, објекту или феномену. Важно је напоменути да подаци сами по себи немају суштинско значење, али је неопходно да им човек или аутоматизовани систем додели контекстуални оквир како би постали информација и добили своју вредност. Суштинска компонента овог процеса је интелектуална активност појединца или примена алгоритамих процедура аутоматизованим системом, који обликује апстрактну структуру података у погледу релевантности и интерпретације. Људска ментална активност или алгоритамска манипулација од стране аутоматизованих система су од суштинског значаја за трансформацију колекције података, којој инхерентно недостаје семантичко значење, у контекстуално обогаћене информације. Овај процес не само да повећава ниво знања примаоца, већ служи и као основа за информисано доношење одлука. Очигледна је потреба да се подаци организују путем симболичког представљања, што омогућава људима или рачунарима да систематски обрађују ову информациону базу.²

¹Checkland, P., Holwell, S. (1998). *Information, Systems and information Systems: Making Sense of the Field*. New York: Wiley, стр. 18.

²Андоновић, С., Прља, Д. (2020). *Основи права заштите података о личности*. Београд: Институт за упоредно право, стр. 9.

У савременом друштву концепт информације заузима централно место и представља један од најактуелнијих концепата. У суштини, информације су изведене из анализе података који се односе на одређени предмет или феномен, који представља амалгам повезаних података са додељеним значењем. Овај термин се често користи у свакодневном говору, а манифестује се кроз концепте као што су информационо доба, информационо друштво, информациона револуција и информационе технологије. Изузетно снажан утицај информација на савремено друштво огледа се у терминима као што су информационо друштво и информационо доба, који карактеришу модерно доба. Овај термин није ограничен само на неформалну употребу, већ се такође широко примењује у научном дискурсу, безбедносним проверама, медијским извештајима и другим контекстима. Као таква, информација није само лингвистички конструкт, већ је кључна за разумевање и тумачење ширег друштвеног контекста.³

Правни домен додатно наглашава битну дистинкцију између појмова података и информација, што резултира различитим правним поступцима и последицама. У правном оквиру Србије ова разлика је евидентна у Закону о општем управном поступку, где је, у оквиру његових принципа, препознато „начело приступа информацијама и заштите података“, у које се наводи да се тајни и лични подаци штите путем управног поступка.⁴ Овај правни контекст наглашава посебност и значај ова два појма, указујући на њихову незаменљивост и потребу за адекватним правним прописима.

Исто тако, подаци се могу посматрати као симболи који су систематски распоређени, омогућавајући људима или аутоматизованим системима (рачунарима) да ефикасно и ефективно обављају аналитичке операције. У том смислу, организација и структура података постају кључни фактори за разумевање и тумачење информација, доприносећи дубљој анализи и рационалном доношењу одлука.

Такође, у законодавном оквиру Републике Србије специфичан приступ дефинисању појма података манифестује се у одредбама Закона о поверљивости података. Поменути закон прецизира категорију информација као „подаци од интереса за Републику Србију“. Ова формулација обухвата све информације које су у поседу органа јавне власти, а тичу се територијалног интегритета, суверенитета, заштите

³Исто, стр. 10.

⁴Закон о општем управном поступку, Службени гласник РС, бр. 18/2016, 95/2018 - аутентично тумачење и 2/2023 - одлука УС, чл. 15; у даљем тексту ЗООУП.

уставног поретка, људских и мањинских права и слобода, националне и јавне безбедности, одбране, унутрашњих и спољних послова. У складу са наведеним законским одредбама, подаци од интереса представљају кључну категорију информација која има значајан друштвени и политички контекст. Њихова релевантност се огледа у директном утицају на темељне вредности друштва, као што су људска права, национална безбедност и уставни поредак.⁵ Овај правни приступ наглашава важност и осетљивост информација које се односе на питања од општег интереса.

У контексту правног оквира, појам информација је прожет релевантним правним актима, међу којима се издваја Закон о слободном приступу информацијама од јавног значаја. Овај закон, као основни правни инструмент, прецизира дефиницију информација од јавног значаја. Према одредбама наведеног закона, информације од јавног значаја обухватају податке којима располаже орган јавне власти, а који су проистекли из њеног деловања или су у вези са њеном делатношћу.⁶ Важно је нагласити да такве информације морају бити садржане у конкретном документу и да се односе на све аспекте који побуђују легитимни интерес јавности за учење.

У складу са наведеним прописима, информације од јавног значаја постају предмет од посебног правног интереса, чиме се обезбеђује транспарентност и доступност информација које потенцијално утичу на ширу друштвену заједницу. Њено постојање, дефинисано и регулисано правним нормама, представља основну претпоставку за конструктивну интеракцију органа власти и грађана, јер се информације од јавног значаја доживљавају као ресурс од општег интереса који обликује демократски дијалог и учешће грађана у друштвеном животу.

2. Лични подаци

Концепт личних података представља кључни аспект у области заштите и регулисања приватности и дефинисан је као сваки информациони елемент који се односи на идентификовану или неидентификовану особу. Овај идентитет се може директно утврдити на основу једног податка или индиректно повезивањем

⁵Закон о тајности података, Службени гласник РС, бр. 104/2009, чл. 3, ст. 1, тч. 2; ЗОТП.

⁶Закон о слободном приступу информацијама од јавног значаја, Службени гласник РС, бр. 120/2004, 54/2007, 104/2009, 36/2010 и 105/2021, чл. 2, ст. 1; ЗОСПИОЈЗ.

информација између различитих извора. У складу са релевантном законском регулативом, важно је напоменути да подаци о правним лицима нису класификовани као лични подаци према одредбама закона.⁷

Лични подаци обухватају широк спектар информација које омогућавају идентификацију физичког лица. Ови подаци могу укључивати аспекте приватног живота појединца, професионални контекст, као и јавну сферу његових животних активности. Поред тога, лични подаци могу бити садржани у различитим форматима, укључујући писане документе, фотографије, видео материјале, аудио записе, као и у папирним или електронским документима. Поред тога, биометријски подаци, као што су узорци ткива, представљају још један облик личних података који захтева посебну пажњу и регулисање.⁸

Податак о личности, у складу са Законом о заштити података о личности, представља сваку информацију која се односи на идентификовано или неидентификовано физичко лице. Идентификација може бити директна или индиректна, а подаци о личности обухватају, пре свега, информације које омогућавају идентификацију, као што су име и идентификациони број. Осим тога, ови подаци могу укључивати информације о локацији појединца, идентификаторе у електронским комуникационим мрежама или различите карактеристике које се односе на физичко, физиолошко, генетско, ментално, економско, културно и друштвено идентитетно својство дотичне особе.⁹ Важно је нагласити да подаци о личности представљају осетљиву категорију информација која захтева посебну пажњу и заштиту, с обзиром на потенцијалне импликације по приватност и основна права појединца.

Стога, може се рећи да лични подаци представљају део човекове личности. Човекова личност, као суштинска друштвена категорија, заузима значајно место у домену правне науке и праксе. Сви правни системи настоје систематски уредити и усмерити људска понашања путем правних норми, чиме се постиже правна сигурност и предвидљивост у друштву. Понашања људи, инхерентно повезана са човековом личношћу, представљају директни и индиректни фокус нормативних уредби

⁷Тајин, С. (2019). *Заштита података о личности у сектору безбедности, водич кроз законску регулативу*. Београд: Центар за унапређивање правних студија и Организација за европску безбедност и сарадњу, стр. 7.

⁸Исто.

⁹Закон о заштити података о личности, Службени гласник РС, бр. 87/2018, чл. 4, ст. 1, тч. 1; у даљем тексту ЗЗПЛ.

различитих правних грана. Важно је напоменути да правне норме не регулишу суштину човекове личности, с обзиром на њен природни карактер на који није могуће и не би требало утицати. Правни системи, стога, прихватају непоновљиву природу личности, тежећи пружању заштите њеном слободном развоју од свих нежељених утицаја појединца и друштва.¹⁰

Услед комплексности правне природе човекове личности, она се позиционира на граници између приватног и јавног права. Са гледишта јавног права, човекова личност се анализира у контексту односа са државом и њеним органима. Конкретно, ова личност је заштићена у таквим односима, с обзиром на то да држава и њени органи поседују монопол над физичком силом, који не сме бити злоупотребљен према грађанима. Норме јавног права, било да се ради о управном, уставном или кривичном праву, штите вредности од значаја за целокупну друштвену заједницу, али такође и за појединце. Ово имплицира да држава гарантује свим индивидуама једнак приступ различитим механизмима правне заштите у случају повреде или штете, посебно у вези са заштитом од злоупотребе података о личности.¹¹

Приватно-правна заштита, с друге стране, представља концепт према којем појединац аутономно може затражити правну заштиту од стране државних органа с циљем очувања властитих личних интереса. Овај приступ имплицира преузимање активне улоге од стране појединца у сврху заштите властитог друштвеног и правног положаја, који је подложен угрожавању деловањем или пропуштањем радњи трећих лица. У том контексту, приватно-правна заштита подразумева мобилизацију норми јавног права, при чему државни органи са јавним овлашћењима активно учествују у заштити како приватних тако и јавних интереса. Међутим, важно је нагласити да у домену приватно-правне заштите кључно место заузима улога појединца. Овај приступ је регулисан нормама грађанског права, укључујући облигационо, породично, наследно право, и слично.¹²

У вези са подацима о личности уско је повезан и појам приватности. Приватност се најпростије може дефинисати као „право да се буде остављен на миру“.¹³ Право на приватност, у контексту међународног и уставног права, представља изузетно значајну

¹⁰Андоновић, С., Прља, Д. (2020). нав. дело, стр. 11-12.

¹¹Исто, стр. 12.

¹²Види шире: Симовић, И., Лазић, М. (2014). Грађанско правна заштита права личности. *Зборник радова Правног факултета у Нишу*, 68, 272-273.

¹³Warren, S., Brandeis, L. (1890). The Right to privacy. *Harvard Law Review*, 4(5), стр. 195.

димензију основних људских права. Ово право, чији ефекти важе у односу на све индивидуе, има за циљ заштиту лица од потенцијалних нарушавања, било од стране државних органа или других појединаца. У супротности јавности, где се дешава деловање на јавној сцени, приватност подразумева тајност и заштићеност. Централна тачка интересовања овог права означава приватни живот индивидуа, где се основано очекује његова мирност и спокојство, без неовлашћеног мешања у интимне сфере.¹⁴ Дакле, приватност, као право, обухвата право на селективно приказивање детаља свог живота јавности.

3. Врсте личних података

У данашњем модерном друштву, лични подаци се појављују као кључни ресурс са значајном корисном вредношћу. Ови подаци, посматрани као средство личне идентификације, служе као основа у различитим правним контекстима, вршећи функције препознавања и посредовања у правно релевантним односима. Између осталог, лични подаци дају суштинску улогу у процесима као што су извршење законских санкција, пренос финансијских средстава, промена власништва, додела личних имена, уручење спортских признања и на тај начин обликују и утврђују различите правне последице.¹⁵

У правном оквиру значајан сегмент података о личности произилази из њихове релевантности у правним односима, будући да ти подаци постају основ за правне последице у многим ситуацијама. Својим мултифункционалним присуством, лични подаци чине основну компоненту правне заштите која се пружа како физичким тако и правним лицима. Међутим, упркос свом инхерентном значају, правни системи не пружају свеобухватну и једнаку заштиту свим аспектима личних података. Овај асиметричан приступ често проистиче из недостатка адекватних законских

¹⁴Јовановић, С. (2014). Приватност и заштита података на интернету. *Твининг пројекат ЕУ – зборник Везе сувер криминала са ирегуларном миграцијом и трговином људима*, Министарство унутрашњих послова Републике Србије, стр. 94.

¹⁵Андоновић, С., Прља, Д. (2020). нав. дело, стр. 17.

инструмената који би у потпуности омогућили заштиту физичких лица у односу на све категорије личних података.¹⁶

У савременом контексту, информационе и комуникационе технологије (ИКТ) представљају кључни катализатор у ширењу и размени личних података. Ово континуирано ширење и доступност података додатно повећава њихову релевантност у свакодневном животу. Стога је императив правне регулативе прилагођавање динамици савременог друштва како би се обезбедила адекватна и ефикасна правна заштита података о личности у складу са потребама друштва које се развијају.

Постоје различите категорије личних података. *Подаци о личности који се односе на живот појединца* одређују се кроз различите димензије личног живота и чине сложен и разнолик скуп информација од суштинског значаја за свеобухватно разумевање индивидуе. То обухвата психо-физичке елементе које карактеришу године живота, физичке и психичке особине попут боје коже, тежине, висине, облика тела, као и нивоа развијености. Уз то, сагледавају се и историјски аспекти личног живота који обухватају релевантне догађаје и дешавања у животу испитаника, као и повезаност са другим релевантним индивидуама. Осим тога, обраћа се пажња и на лична уверења и мишљења појединца, с обзиром на његово изражавање у вези са одређеним темама, укључујући религијска и филозофска уверења. Обухватају се лични ставови и наклоност према стварима, особама и појавама, што укључује преференције попут омиљене врсте хране, боје, песме, и слично. Ова категоризација података такође обухвата идентификационе информације које се односе на етничко и социјално порекло, укључујући информације о раси, националној и етничкој припадности, језицима које особа говори, као и акцентима који се користе у вербалној комуникацији. Надаље, обухвата и податке о сексуалности, попут родног идентитета, сексуалне оријентације и историје љубавних односа. Коначно, анализира и медицинске податке и информације о здрављу, с нагласком на физичкој и психичкој зрелости, евентуалним недостацима, историји болести, крвној групи и здравственом картону.¹⁷ Интеграција ових разноврсних информација омогућава свеобухватно сагледавање личности појединца у њеној комплексности и разноврсности.

Подаци о личности који се односе на јавни живот појединца обухватају информације о сегментима живота појединца унутар друштвене заједнице. Овај аспект

¹⁶Исто, стр.18.

¹⁷Исто, стр. 18-19.

обухвата податке о породичном животу, укључујући присуство породице, величину породице и динамику породичних односа. Поред тога, обухваћени су и подаци о социјалном окружењу појединца, укључујући пријатељске везе, друштвене конекције и припадност формалним и неформалним организацијама. У склопу јавних података о личности такође се разматрају информације о криминалној прошлости појединца, укључујући евентуалне претходне осуде или тренутне правне поступке који се воде против њега. Ова врста информација пружа увид у јавни карактер појединца и његов однос према друштвеним нормама и законима.¹⁸ Све наведене информације чине саставни део комплексне анализе личности унутар ширег друштвеног контекста.

Подаци о личности усмерени ка професионалном аспекту живота појединца, обухватају информације о друштвеним ангажманима појединца у контексту рада и извршавања професионалних дужности. Овај сегмент података укључује образовне елементе, као што су нивои образовања које је особа стекла, оцене, завршени курсеви итд. Такође, обухвата пословне аспекте, као што су запослење, радно место, оцене у вези с радним резултатима, те информације о одсуству с посла. Финансијски подаци, попут бројева рачуна, банака где се чувају средства, лична имовина, кредитни статус и други релевантни финансијски параметри такође чине део овог скупа података. Радна историја појединца која обухвата информације о фирмама у којима је особа запослена, подаци о колегама, финансијским примањима и трансакцијама, допуњује ову категорију.¹⁹

За обраду овог рада важно је напоменути и поделу на обичне и специфичне (осетљиве) врсте података. Ова класификација личних података кључни је аспект анализе приватности. Ова подела, заснована на степену поверљивости и значају информација за појединца, разликује податке који носе обичне податке о физичком лицу од оних који садрже посебно значајне детаље о личном идентитету. Обични лични подаци обухватају стандардне информације, док осетљиви подаци носе кључне информације о идентитету појединца.²⁰

Кршење осетљивих личних података обично има озбиљније последице за појединца од повреде обичних личних података. Према овој подели, осетљиви подаци о личности уживају виши ниво правне заштите у односу на друге врсте личних података.

¹⁸Исто, стр. 19.

¹⁹Исто.

²⁰Исто, стр. 20.

Ова категорија обухвата информације о верским и филозофским уверењима, расном и етничком пореклу, генетске податке, биометријске податке, податке о сексуалном животу и сексуалној оријентацији, као и податке о здравственом стању. Сви остали лични подаци су класификовани као обични.²¹

4. Прикупљање и обрада података о личности

Лични подаци се подвргавају различитим процесима обраде, укључујући прикупљање, евидентирање, класификацију, груписање, структурирање, чување, прилагођавање, модификовање, откривање путем увида, доставе и слично. Ови подаци се могу дуплирати, упоређивати, брисати или уништити применом различитих метода обраде. Обрада података се такође може ограничити њиховим означавањем.²²

Према ЗОЗПЛ, обрада података о личности представља све поступке или скупове поступака који се изводе аутоматизовано или неаутоматизовано над подацима о личности или њиховим скуповима. Ови поступци укључују прикупљање, бележење, разврставање, груписање, структурисање, похрањивање, уподобљавање или мењање, откривање, увид, употребу, откривање путем преноса или достављања, умножавање, ширење или на други начин чињење доступним, упоређивање, ограничавање, брисање или уништавање.²³ Ограничавање обраде означава поступак означавања похрањених података о личности с циљем ограничавања њихове даље обраде у будућности.²⁴

Профилисање је обрада података која се примењује са циљем да се процене одређене карактеристике особе на коју се подаци односе. Ово може укључивати анализу економског статуса, здравственог статуса, поузданости, преференција и сличних карактеристика.²⁵ Овакви процеси обраде података играју значајну улогу у креирању профила личности и тумачењу различитих аспеката живота особе.²⁶

Одговорност за одређивање сврхе и начина обраде података о личности припада субјекту, познатом као руковалац. Руковалац може бити физичко или правно лице,

²¹Исто.

²²Гајин, С. (2019). нав. дело, стр. 9.

²³Закон о заштити података о личности, чл. 4, ст. 1, тч. 3.

²⁴Закон о заштити података о личности, чл. 4, ст. 1, тч. 4.

²⁵Закон о заштити података о личности, чл. 4, ст. 1, тч. 5.

²⁶Гајин, С. (2019). нав. дело, стр. 9.

укључујући и органе јавне власти.²⁷ Обрада података о личности може се спроводити од стране надлежних органа јавне власти у циљу спречавања, истраживања и откривања кривичних дела, прогона починилаца ових дела и извршења кривичних санкција, што обухвата и превенцију и заштиту од претњи јавној и националној безбедности. На ову врсту обраде примењују се посебне одредбе закона.²⁸

Више лица може деловати заједно као ко-руковаоци или заједнички руковаоци. У том случају, они могу заједно одредити сврху и начин обраде, али такође могу заједно одредити само одређене сврхе или начине обраде. Однос између заједничких руковалаца, укључујући питање одговорности и друга питања прописана законом, уређује се њиховим споразумом. Обрада података о личности врши се од стране обрађивача у име руковаоца и у складу са његовим упутствима. Обрађивач такође може бити физичко или правно лице, а руковалац може истовремено обављати и улогу обрађивача.²⁹

Подаци о личности који се обрађују у сврху успостављања друштвених мрежа или других облика комуникације путем интернета такође су предмет анализе. Уобичајено је да ова врста обраде није посебно регулисана законским одредбама, осим уколико се, узимајући у обзир специфичности конкретног случаја, утврди да је реч о обради која се не врши у личне сврхе, већ, на пример, има пословни карактер или се спроводи у оквиру професионалних активности субјекта обраде. У специфичним ситуацијама, надзор над стамбеним зградама, становима и кућама намењеним становању може се сматрати обрадом на коју се примењују одређене одредбе Закона.³⁰

5. Крађа података

Незаконито присвајање или задржавање информација поверљивог, личног или финансијског карактера, као што су лозинке, софтверски код, алгоритми, власнички подаци оријентисани на процес или технолошки детаљи, представља чин крађе података. Реперкусије за оштећену страну нису ограничене само на директне

²⁷Закон о заштити података о личности, чл. 4, ст. 1, тч. 8.

²⁸Гајин, С. (2019). нав. дело, стр. 9.

²⁹Исто.

³⁰Исто, стр. 10.

финансијске губитке, већ они обухватају спектар последица у распону од штете преко репутације и ерозије поверења купаца до финансијских казни, трошкова санације и потенцијалне појачане конкуренције која је резултат погрешно присвојених информација.³¹

Крађа података обухвата незаконито прибављање информација ускладиштених у корпоративним базама података, уређајима и серверима, што представља значајан ризик различитих размера. Порекло такве крађе може се пратити и у интерним и екстерним изворима. Док термин „крађа података“ подразумева намерно дело са злонамерним циљем, неопходно је напоменути да ова кршења нису искључиво вођена злонамерним мотивима; могу настати и ненамерним радњама.³²

Злонамерна ексфилтрација података се често дешава потајно, избегавајући свест жртава. Ово се дешава када хакери искористе рањивости као што су слабо управљање лозинкама или несигурне мреже да би компромитовали корисничке налоге или личне уређаје. Уљези, када једном уђу у системе компаније, могу прихватити маску легитимности, омогућавајући им да остану неоткривени у дужим периодима—у распону од дана до година. Ово тајно присуство пружа им прилику да постепено ескалирају своје привилегије приступа, добијајући приступ прогресивно осетљивим скуповима података и на тај начин представљају ескалирајућу претњу.³³

Подаци се манифестују у различитим облицима, носећи посебан значај и вредност зависну од природе. За предузећа, може попримити пословни или финансијски карактер, док се у области инжењеринга може манифестовати као софтверски програми, алгоритми, дизајни, прототипови, токови процеса, нацрти, симулације и подаци за тестирање, што све доприноси перформансама индустрије. Финансијске институције, као што су банке, сматрају да подаци обухватају акредитиве, информације о рачуну и осетљиве детаље о кредитној/дебитној картици. На нивоу националне државе, информације које се односе на спољну политику, унутрашњу безбедност и управљање одбраном, укључујући позиционирање и кретање оружаних снага, истраживачке податке и детаље о перформансама војног хардвера (подморнице, оружје, авиони, авиони носачи, фрегате), је инхерентно осетљив и сходно томе

³¹Sharma, M. (2017). Data Theft: Implications for Economic and National Security. *Journal of Defence Studies*,11(1), стр. 62.

³²Sham, S., What Is Data Theft?преузето са: <https://www.okta.com/blog/2020/07/data-theft/> (15.05.2024).

³³Исто.

ограничен на одабрану публику.³⁴ Чување таквих података може имати различите облике, било физичке или електронске, који се налазе у рачунарима, серверима или документовани графички или текстуално. Безбедносне импликације овог мноштва података су наглашене разноврсним низом потенцијалних актера претњи, укључујући стране обавештајне агенције, пословне ривале, транснационалне криминалне синдикате, хактивисте и интерне појединце или групе у дослуху. Ови актери представљају различите степене ризика како за економску тако и за националну безбедност.

Искоришћавање рањивости представља примарну могућност за актере претњи који траже приступ одређеним скуповима података или скуповима информација. Мотивације које покрећу ове актере су различите, у распону од политичких, безбедносних и монетарних добитака до конкурентског ривалства. Овај пејзаж злонамерних актера обухвата мноштво субјеката, укључујући инсајдере као што су незадовољни запослени, супротстављене националне државе које се баве економском или безбедносном шпијунажом и транснационално присутне криминалне синдикате. Свака категорија актера поседује различите капацитете и способности за извршење крађе података.³⁵

6. Заштита података о личности

6.1. Право на приватност

Право на приватност је основно људско право које игра кључну улогу у очувању индивидуалне слободе и интегритета у друштву. Њено постојање датира још од краја 19. века, настало као одговор на све веће изазове савременог доба, посебно у контексту развоја технологије и ширења јавне сфере. Иако је првенствено обликовано у правној доктрини Сједињених Америчких Држава, право на приватност је данас признато и заштићено у многим правним системима широм света.³⁶

³⁴ Sharma, M. (2017). нав. дело, стр. 64.

³⁵ Исто.

³⁶ Gondwe, M. (2011). *The Protection of Privacy in the Workplace: A Comparative Study - doctoral dissertation*. University of Stellenbosch, стр. 112.

Суштина права на приватност лежи у заштити различитих аспеката приватног живота појединца, укључујући просторну, емоционалну, информациону, комуникацијску и физичку сферу, од неовлашћених интервенција државних органа, корпорација и других појединаца. Појединцу даје право да контролише своје личне податке, одлучује о њиховој употреби и штити их од злоупотребе. У суштини, право на приватност штити појединца од задирања у приватност, што укључује неовлашћени физички контакт, како је првобитно дефинисано у пресуди судије Кулија. Касније је дефиниција права на приватност проширена у раду Ворена и Брандаиса, где је наглашен значај заштите појединца од неовлашћеног мешања и задирања у његов приватни живот.³⁷ Важно је напоменути да право на приватност није апсолутно, већ може бити ограничено у одређеним ситуацијама ради заштите јавног интереса или других права и слобода појединаца. Међутим, таква ограничења морају бити стриктно дефинисана и оправдана у складу са принципима владавине права и важећим прописима.

Заштита достојанства и интегритета сваког појединца обезбеђује се кроз различите аспекте људских права, од којих је једно од најважнијих право на приватност. Термин „*privatus*“ потиче од латинског језика што значи лично или незванично, и илуструје важност заштите приватности појединца. Право на приватност обезбеђује заштиту и личних и интимних аспеката личности, укључујући садржај права на приватност као и механизме за његову заштиту.³⁸ Да би се на адекватан начин одредио садржај концепта права на приватност, кључно је ослонити се на једну од најстаријих и најутицајнијих дефиниција овог права коју су формулисале енглеска и америчка правна традиција крајем 19. века. Ова дефиниција, позната као „право да се остане сам“ (енгл. „*right to be left alone*“), пружа дубок увид у суштину права на приватност и његову улогу у заштити индивидуалних слобода и аутономије.³⁹

Приватност је концепт који је у сржи наше личне и социјалне сфере, што је чини важним аспектом нашег постојања. Најпознатија дефиниција приватности коју су формулисали Семјуел Ворен и Луис Брандеис пре више од сто година, наглашава „право да се остане сам“, што је основа за заштиту наше личне аутономије и

³⁷Брковић, Р., Јовановић, З. И Тотић, М. (2019). Право на приватност и заштиту личних података запосленог као пацијента у праву Републике Србије. *Анали Правног факултета Универзитета у Зеници*, 13(24), стр. 206.

³⁸David, H. (2009). *The Right to Privacy*. Infobase Publishing, стр.13.

³⁹Clinton, L., Amit, S. (2008). Understanding Consumer Privacy: A Review and Future Directions. *Academy of Marketing Science Review*, 12(02), стр. 1-7.

интегритета.⁴⁰ Ово право обухвата избор начина живота, наше односе са другима и нашу слободу да обликујемо своје животе без непотребних ограничења. Међутим, приватност је више од само права на мир и непрекидност. Алан Вестин истиче да приватност обухвата и способност да контролишемо колико информација о себи откривамо другима, као и када то чинимо.⁴¹

Право на приватност је основни стуб демократског друштва и његово поштовање је од виталног значаја за очување слободе и интегритета појединца. Ово право није само производ борбе против тоталитарних режима, већ се континуирано суочава са изазовима у модерном дигиталном добу. У прошлости је право на приватност било угрожено диктаторским режимима који су се безобзирно мешали у приватне животе грађана, контролишући њихове активности и пратећи најинтимније аспекте њихових живота. Међутим, и у демократским друштвима суочавамо се са новим изазовима, посебно у контексту развоја науке и технологије. Дигитализација и компјутеризовани информациони системи отварају нове могућности за нарушавање духовног и моралног интегритета појединца, чиме се истиче значај прецизног дефинисања садржаја права на приватност и спровођења делотворних механизма за заштиту овог права. Приступ заштити права на приватност треба да буде свеобухватан и динамичан, у складу са еволуцијом технологије и друштвених норми. То подразумева успостављање јасних законских оквира који регулишу прикупљање, обраду и коришћење података о личности, као и јачање институција надлежних за заштиту приватности грађана. Такође је важно подизање свести грађана о њиховим правима и обавезама у дигиталном окружењу, као и промовисање транспарентности и одговорности међу корпорацијама и државним институцијама.⁴²

Право на приватност је од основне важности у савременом друштву, а та важност је потврђена и у бројним међународним инструментима за заштиту људских права. Ови инструменти, који су прихваћени на глобалном нивоу, истичу неопходност заштите приватног живота од произвољног мешања и напада. Њихов циљ је да осигурају да ниједна особа не буде изложена непоштовању свог приватног живота или нападима на свој углед и част.⁴³ Као основно људско право, право на приватност је

⁴⁰Warren, S.&Brandeis,L.(1890). TheRighttoprivity,*HarvardLawReview*,4(5),193-220.

⁴¹Westin,A. (1968).Privacyandfreedom. *WashigtonandLeeLawreview*,25(1).

⁴² Младенов, М. (2013). Заштита права на приватност у пракси Европског суда за људска права. *Зборник радова Правног факултета у Новом Саду*, 3, стр. 576.

⁴³Исто.

признато и загарантовано Конвенцијом за заштиту људских права и основних слобода (1950), Универзалном декларацијом о људским правима (1948), Повељи и основним правима у Европској унији (2007).

6.2. Право на заштиту података о личности

Заштита података о личности постала је кључна тема у правном свету, привлачећи све већу пажњу из неколико важних разлога. Са све већом употребом интернета, друштвених мрежа и других облика комуникације, количина личних података се драматично повећала. Ови подаци су све важнији у свакодневним активностима, од пословних до друштвених интеракција. Користе се не само у легитимне сврхе, већ и за анализу понашања корисника, праћење и разумевање људских активности, па чак и за надзор и прислушкивање.⁴⁴

Пре појаве информационо-комуникационих технологија и интернета, лични подаци нису имали велики значај. Државе су углавном имале информације о својим грађанима које се односе на њихову имовину и плаћање пореза. Међутим, све до Француске буржоаске револуције људска права су била занемарена, делом због недостатка глобализације и сложених информационих технологија. Један од кључних момената који се може сматрати почетком заштите података о личности је теоријско успостављање права на приватност 1890. године. Међутим, тек са глобализацијом и развојем информационо-комуникационих технологија, интересовање државе, привреде и друштва за обраду и заштиту података постаје све израженије, посебно током последње деценије 20. века.⁴⁵

Заштита података о личности, као грана права, представља кључни сегмент у регулисању начина на који организације манипулишу личним подацима. Настао је као одговор на забринутост у вези са све већом централизацијом личних података и стварањем огромних база података. Иако се често пореде са правом на приватност чија је примарна сврха заштита једног од основних људских права, заштита података о личности проистиче из другог мотива – економских интереса.⁴⁶ Право на приватност, иако се фокусира на заштиту приватности појединца, има своје корене у основним

⁴⁴Андоновић, С. (2019). *Заштита података у електронској јавној управи у Републици Србији – правни аспекти - докторска дисертација*. Београд: Правни факултет, стр. 134.

⁴⁵ Исто.

⁴⁶Carey,P.(2014). *DataProtection.ApracticalguidetoUKandEUlaw*. Oxford, стр. 1.

људским правима. С друге стране, заштита података о личности настаје као одговор на све израженију дигитализацију друштва и привреде. У том контексту, појединац све више постаје „роба“ која се може искористити у комерцијалне сврхе. Дакле, заштита података о личности није само питање права појединца на контролу над сопственим подацима, већ и питање економске сигурности и конкурентности. Концепт заштите података о личности посебно је важан у данашњем дигиталном добу, где се све већи број личних података користи у аналитичке, маркетиншке и профитне сврхе. Стога ефикасна заштита података о личности постаје витална за очување интегритета појединца, али и за очување поверења у дигиталне системе и тржиште у целини.

Међународна заједница је увек била кључни актер у расправама о заштити личних података и приватности. Тако су међународне организације попут Организација за економску сарадњу и развој(ОЕЦД) и Европске уније препознале значај регулативе у овој области. ОЕЦД-ов Приручник о приватности је важан документ који наглашава да је заштита података о личности неопходна не само за правосудна права појединца, већ и за унапређење економских и друштвених стандарда.⁴⁷ Он наглашава да подаци имају економску вредност, те да олакшавање протока података између земаља може донети политичке и технолошке предности. Слично, Европска унија је препознала потребу да се регулише заштита личних података. Директива 95/46/ЕЦ, позната као Директива о заштити података о личности, први је законодавни документ ЕУ који има за циљ заштиту приватности података.⁴⁸ Главни циљеви Директиве били су хармонизација закона држава чланица у вези са заштитом личних података и обезбеђивање слободног протока података између држава чланица. Данас се ова Директива сматра једном од најстрожих прописа у области заштите приватности података.⁴⁹

Заштита личних података постала је кључно питање у савременом дигиталном друштву, а академски приступ овој теми је од виталног значаја за разумевање њеног ширег контекста и импликација. Право на заштиту података о личности произилази из сложеног скупа правних норми које имају за циљ заштиту основних права, слобода и

⁴⁷Tzanou, M. (2013). Is data protection the same as privacy? An analysis of telecommunications' Metadata Retention Measures. *Journal of Internet Law*, 17(3), стр. 24.

⁴⁸Directive 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, OJ L 281, 23.11.1995, p. 31–50.

⁴⁹Cunningham, M. (2018). Complying with International Data Protection Law, *University of Cincinnati Law Review*, 84(2), 421–450.

интереса појединаца чији се подаци обрађују.⁵⁰ Овај концепт добија посебан значај доношењем Директиве Европске уније о заштити података о личности, која јасно дефинише заштиту података о личности као основно право појединца на приватност у контексту обраде његових података.

Да бисмо разумели концепт заштите података о личности, кључно је сагледати централне појмове као што су „обрада“ и „лични подаци“. Обрада података обухвата широк спектар операција, од прикупљања до брисања и уништавања, обезбеђујући да се лични подаци третирају на одговарајући начин у свакој фази њихове употребе. Подаци се сматрају личним подацима када постоји могућност да се могу директно или индиректно повезати са одређеним појединцем, чиме се наглашава важност заштите приватности и аутономије сваког појединца у дигиталном окружењу.

Централна тема заштите података о личности представља изазов који захтева постојану присутност и укљученост како законодаваца тако и руководиоца подацима. Широк спектар правила и принципа који је развијен у овој области наглашава неопходност укључивања различитих интереса и вредности.

У области заштите података о личности, еволуција је константна. Са сваким напретком у технологији појављују се нови изазови, захтевајући непрекидно усавршавање правних и етичких норми. Ово углавном илуструје разноликост интереса и вредности које се сукобљавају у овом контексту, укључујући аутономију, приватност, слободу информација и друштвени плурализам. Заштита података о личности не може се свести на пар реченица јер представља комплексан концепт са многим аспектима. Државе и регулаторна тела се труде да нађу баланс између различитих интереса кроз примену различитих стратегија, укључујући правну регулативу, али и етичке норме и стандарде. Стално развијање и унапређење правила и принципа у заштити података о личности је неопходно да би се осигурао одговарајући баланс између заштите приватности и потребе за слободним протоком информација, како у дигиталном тако и у реалном свету.

⁵⁰Hondius, F. (1975). *EmergingDataProtectioninEurope*. Amsterdam, стр. 16.

II ПРИНЦИПИ И ЗАШТИТА ПОДАТАКА О ЛИЧНОСТИ У ЕВРОПСКОМ КОНТИНЕНТАЛНОМ ПРАВУ

1. Право Европске Уније у области заштите података о личности

Европска унија је међувладина и наднационална унија (заједница) двадесет осам европских демократских држава.⁵¹ Политичке активности Европске уније се испољавају у многим сферама, од политике здравства и економске политике, до спољних послова и одбране. У зависности од развијености сваке државе понаособ, организација Европске уније се разликује у различитим областима. Како је наведено у основним одредбама Уговора из Мاستрихта, структура Европске уније која је њиме успостављена заснована је на три економска стуба: I – економска заједница; II – заједничка спољна и безбедносна политика и III – сарадња у области правосуђа и унутрашњих послова.⁵² Главна област на којој почива Европска унија је јединствено тржиште које се базира на царинској унији, јединственој валути, заједничкој агрокултурној политици и заједничкој политици у сфери рибарства.

Последњих деценија, Европска унија (ЕУ) је еволуирала у значајну интеграциону формацију у међународној политичкој и економској арени. Један од најзначајнијих аспеката ове еволуције је усвајање јединствене валуте – евра од стране 19 од 28 чланица ЕУ. Ово представља значајан корак ка економској интеграцији, при чему се националне валуте одбацују у корист јединствене европске валуте. Међутим, институционална структура ЕУ значајно се разликује од других регионалних трговинских споразума на нижем нивоу интеграције. Наравно, неке од основних институција ЕУ, као што су Европска комисија и Европски суд правде, имају широка овлашћења која их издвајају од уобичајених међународних институција. Овај

⁵¹ Француска, Немачка, Италија, Холандија, Белгија, Луксембург, Велика Британија, Данска, Република Ирска, Грчка, Шпанија, Португалија, Финска, Аустрија, Шведска, Естонија, Кипар, Летонија, Литванија, Мађарска, Малта, Пољска, Словачка, Словенија, Чешка, Бугарска, Румунија и Хрватска..

⁵²Džombić, I. J. (2010). *Evropska unija: prošlost, sadašnjost, budućnost*. Sarajevo: Friedrich-Ebert-Stiftung, стр. 41-42.

„наднационални“ карактер ЕУ говори о њеном високом степену аутономије и унапређености у односу на конвенционалне међународне институције.⁵³

Током 70-их година прошлог века многе европске земље, укључујући Шведску, Француску, Данску, Аустрију и Немачку, увеле су законе о заштити података. Ови закони нису укључивали само општи заштитни оквир, већ су укључивали и посебне законе за различите области као што су радно право, кривично право и здравствена заштита. На нивоу Европске уније, законодавство обухвата Конвенцију Савета Европе о заштити података из 1981. године⁵⁴, Повељу о основним правима Европске уније⁵⁵, Директиву о заштити података из 1995. године⁵⁶ и Општу уредбу о заштити података из 2016. године⁵⁷.

У контексту правних норми Европске уније, постоји принцип *lex specialis derogat legi generali*, што значи да посебни закони имају предност у односу на опште законе.⁵⁸ Овај принцип примењује се на низ директива које регулишу област приватности и електронских комуникација у ЕУ. Прво, Директива о приватности и електронским комуникацијама 2002/58⁵⁹ усвојена је да би се утврдили стандарди за заштиту личних података и приватности у контексту електронских комуникација. Затим, Директива 2006/24⁶⁰ је донесена са циљем да допуни претходну директиву у делу који се односи на задржавање и доступност трафика и информација о комуникацијама. Касније измене, као што је Директива 2009/136⁶¹, додатно су

⁵³Комшић Ј., (2013). *Принципи Европске уније*. Асоцијација мултиетничких градова југоисточне Европе, стр. 14.

⁵⁴Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.I.1981.

⁵⁵European Union, Charter of Fundamental Rights of the European Union, Official Journal of the European Communities, 2000/C364, 18.12.2000.

⁵⁶Directive 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, OJ L 281, 23.11.1995, p. 31–50.

⁵⁷Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L 119, 4.5.2016, p. 1–88.

⁵⁸Водинелић, В. (2007). Право заштите личних података. У: *Право информacionих технологија*, Београд: Правни факултет Универзитета „Унион“, Службени гласник, стр. 152.

⁵⁹Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37–47.

⁶⁰Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13.4.2006, p. 54–63.

⁶¹Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and

модификовале претходне законе у циљу адаптације на нове технолошке и друштвене изазове. Уз ове директиве, постоји и Директива ЕУ о телекомуникацијама 1997/66⁶² која је старија и обухвата опште одредбе о телекомуникационим услугама у ЕУ. Телеком пакет, у који спада и Директива 2009/140⁶³, представља комплекснију регулативу која обухвата аспекте управљања мрежама и услугама, укључујући и приступ мрежама.

Такође, треба напоменути и Директиву ЕУ 2016/680, познату и као Полицијска директива, усмерену на заштиту права физичких лица у контексту обраде њихових података од стране надлежних тела.⁶⁴ Циљ је спречавање, истраживање, откривање и гоњење кривичних дела или извршења казnenих санкција, и омогућава слободно кретање таквих података унутар Европске уније.

У развоју области заштите података о личности у ЕУ, значајни утицаји долазе од спољних и унутрашњих фактора. Напредак информационо-комуникационих технологија и широка примена интернета играли су кључну улогу, стварајући потребу за законском заштитом личних података. Исто тако, нарушење права на приватност додатно је убрзало потребу за усвајањем Повеље о основним правима ЕУ. Члан 8 ове Повеље посебно регулише заштиту података о личности, утврђујући право на њихову заштиту и неопходност њихове поштене обраде и предвиђајући потребу за пристанком или законским основом за обраду таквих података. Овакви правни оквири омогућавају уједињено регулисање питања заштите података о личности широм ЕУ. Затим, Директива 2002/58/ЕС, позната као Директива о приватности и електронској комуникацији, усмерена је на заштиту приватности и обраду личних података у контексту електронских комуникација. Она посебно регулише обраду података о

services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (Text with EEA relevance), OJ L 337, 18.12.2009, p. 11–36.

⁶²Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, OJ L 24, 30.1.1998, p. 1–8.

⁶³Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services (Text with EEA relevance), OJ L 337, 18.12.2009, p. 37–69.

⁶⁴Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89–131.

трафику и локацији, како би се осигурала приватност корисника електронских комуникационих услуга.⁶⁵ Осим ових, значајна је и Директива 2003/98/ЕС која се односи на поновну употребу информација јавног сектора, што укључује правила за поновну употребу информација које су у поседу јавних органа у циљу подршке иновацијама и развоју.⁶⁶ Ове директиве представљају важан правни оквир у Европској унији за заштиту података и уређење њихове обраде у различитим контекстима, од полицијских истрага до електронских комуникација и управљања јавним информацијама.

Регулативом ЕС/45/2001 утврђује се значај заштите података о личности у контексту обраде од стране институција и тела ЕУ, како би се осигурао слободан ток таквих података и заштитила приватност појединца. Ова регулатива поставља раме за обраду података о личности од стране институција и тела ЕУ, укључујући постојање Европског надзорника за заштиту података о личности и усвајање правила која гарантују поштовање принципа заштите података и права грађана ЕУ у вези са њиховим личним подацима.⁶⁷ Европски надзорник за заштиту података обавља детаљни надзор над применом Директиве, како од стране органа ЕУ, тако и од стране приватног сектора који обрађује податке. ЕУ је посебно ангажована на уређивању и заштити података о личности на интернету, а Суд правде игра активну улогу у тумачењу постојећих законских норми. Овај судски процес је од суштинског значаја за адресирање правних празнина које настају услед брзог развоја технологије које правни оквири нису успели да прате. Ово је главни мотив за реформу заштите података о личности коју ЕУ спроводи, укључујући и примену Регулативе за заштиту података о личности коју је Европска унија усвојила од 2018. године.

Европски надзорник за заштиту података о личности је независни орган у Европској унији који има за циљ да надгледа и обезбеди правилно обрађивање података о личности. Основан је Регулативом бр. 45/2001 и има улогу да прати да ли институције и тела ЕУ, као и приватни сектор, поштују правила о заштити података. Свака институција у ЕУ мора да именује повереника за заштиту података који сарађује са

⁶⁵Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37–47.

⁶⁶Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information, OJ L 345, 31/12/2003, p. 90–96.

⁶⁷ Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12.1.2001, p. 1–22.

Европским надзорником како би се осигурало да су права и слободе грађана у вези са њиховим подацима заштићени. Надзорник такође дели савете и прати технолошке развоје који могу утицати на обраду података о личности.

Европска комисија обавезна је да поднесе свој предлог закона Европском надзорнику за заштиту података ради консултације када предлог закона може утицати на заштиту података о личности. Надзорник анализира предлог закона узимајући у обзир различите аспекте који се односе на заштиту података, укључујући обим и сврху предложеног закона, ефикасност и пропорционалност правних мера за заштиту, обраду осетљивих података, период задржавања података, приступ подацима, информисање грађана о обради њихових података и начин на који грађани могу да остваре своја права у вези са њиховим подацима.

2. Општа уредба о заштити података о личности – GDPR

Европска унија је истакла своју улогу пионира у заштити личних података пре више од две деценије, када је први пут увела прописе у овој области. Недавно је завршила значајну ревизију свог законодавног оквира са циљем да унапреди заштиту појединаца, хармонизује правила за предузећа и олакша процесе преноса података изван ЕУ. Најважнији део овог законодавства је Општа уредба о заштити података о личности (GDPR)⁶⁸, која је почела да се примењује од 25. маја 2018. године. GDPR је усмерен на стандардизацију права и обавеза за обраду личних података у свих чланица Уније, како би се унапредила заштита права грађана и олакшало пословање предузећима која раде са подацима о личности.

Општа уредба о заштити података о личности (GDPR) представља значајан правни акт у Европској унији који је усвојен 27. априла 2016. године и ступио на снагу 25. маја 2018. године. GDPR је дизајниран да уједини и уједносмисли правила заштите података о личности у свим државама чланицама ЕУ, обезбеђујући виши ниво заштите и контроле над личним подацима. Главни циљ је био адаптација правних система држава чланица и усклађивање са новим стандардима, што је обезбедило конзистентност и једноставност у примени правила. Уводом GDPR је изазвао значајне

⁶⁸Regulation (EU) 2016/679 (General Data Protection Regulation) in the current version of the OJ L 119, 04.05.2016; cor. OJ L 127, 23.5.2018.

промене у начину како компаније обрађују и чувају податке о личности, пратећи све исказане стандарде и утицај на пословање унутар ЕУ.

Значај ове Уредбе је очигледан кроз дужину њеног уводног дела. Преамбула садржи преко 170 тачака и пружа опширну позадину која објашњава мотиве и циљеве аутора приликом израде нацрта. Она такође објашњава како је потребно применити материјалне одредбе.⁶⁹ За разлику од претходне Директиве која је била фокусирана на квалитет података, GDPR примењује принципе на обраду личних података.

Заштита личних података је основно право сваког грађанина ЕУ. Начела на којима почива GDPR укључују принцип законитости, поштене обраде и транспарентности, ограничења сврхе, минималне обраде података, тачности и заштите података. Концепт интегритета и поверљивости обухвата заштиту података кроз технолошке и организационе мере, као и обавештавање надзорног органа и лица којима подаци припадају у случају повреде података. Међутим, концепт одговорности је можда најважнији. Он захтева од оператера да докажу усклађеност са свим стандардима. Само они који успешно покажу поштовање и усклађеност са одредбама GDPR биће ослобођени одговорности за било какве недоследности у примени прописа.

GDPR је кључни пропис који је донет ради заштите приватности и обраде личних података. Уведен је као одговор на брзи технолошки напредак и свеprisутну дигитализацију у последњих 20 година. Ова уредба значајно мења начин на који се подаци обрађују у различитим секторима, од здравства до банкарства, не само унутар Европске уније, већ и глобално, где се лични подаци обрађују или користе.⁷⁰ Централни циљ GDPR -а је унапређење прописа о заштити података о личности и усклађивање са технолошким иновацијама, са посебним акцентом на поштовање основних људских права и слобода. Ово укључује праксу Европског суда за људска права и Суда Европске уније, која има за циљ да обезбеди да се сваки корак у обради личних података одвија у складу са високим стандардима заштите приватности и права појединаца.⁷¹

Ова регулатива дефинише личне податке као све информације које могу бити коришћене за идентификацију конкретног лица, укључујући основне податке као што су име и адреса, али и осетљивије информације као што су локација, физички и

⁶⁹ Преамбула Опште уредбе о заштити података о личности – GDPR.

⁷⁰ Беванда, М. и Чолаковић, М. (2016). Правни оквир за заштиту особних података у праву Европске Уније. *Зборник Правног факултета Универзитета у Ријеци*, 37(1), 125-154.

⁷¹ Ђукић, Д. (2017). Заштита података о личности са освртом на ново законодавство Европске Уније у овој области. *Правни записи*, 1, 49-60.

физиолошки подаци, како и друге карактеристике.⁷²Примарни циљ GDPR је да обезбеди већу контролу над личним подацима појединца. Организације које обрађују ове податке морају да затраже сагласност од особа чији се подаци користе, обавести их о сврси обраде и начину чувања података, као и да осигурају могућност појединцима да контролишу употребу својих података. Ова регулатива такође намеће строге захтеве за безбедност и заштиту података, што укључује мере за спречавање неправилног приступа и неовлаштеност обрађивања личних података. Све ове промене представљају значајан корак напред у обезбеђивању приватности и заштите података у дигиталном добу.

GDPR има екстериторијално важење, што значи да се примењује и на обраду података коју врше организације изван ЕУ, ако те организације обрађују податке грађана ЕУ или прате њихово понашање у ЕУ. Тиме се проширује обим примене GDPR-а и на земље које нису чланице ЕУ, али имају близак економски однос са ЕУ.

Уредба такође укључује процедуралне одредбе и захтева од Европске комисије да периодично подноси извештаје о примени GDPR-а и предлаже измене ако се укаже на потребу за њима. Ово је значајно не само за земље чланице ЕУ и кандидате за чланство, већ и за међународне организације које сарађују са ЕУ.

3. Начела заштите података о личности у европском праву

Општа уредба о заштити података (GDPR), усвојена 2016. године, представља значајно унапређење законодавства ЕУ у области заштите података. Ова уредба модернизује претходну Директиву о заштити података, постављајући нова правила која су директно применљива у свим државама чланицама ЕУ. Основни циљ GDPR-а је заштита основних права грађана у дигиталном добу, суочавајући се са изазовима које доноси дигитализација у економском и друштвеном контексту. GDPR чува и развија основне принципе заштите података, као и права субјеката података на приватност и контролу над њиховим подацима. Увођењем нових обавеза, као што су техничке и интегрисане мере заштите података, именовање службеника за заштиту података у

⁷²Бадовинац, Н. (2018). Осврт на GDPR уредбу и сугестије за развој апликативне подршке. *Инфо М*, 17(65), 11-16.

одређеним случајевима, право на преносивост података и принцип одговорности, GDPR ствара јединствен скуп правила који обезбеђује висок ниво заштите података широм ЕУ. Осим што обезбеђује доследна правила за заштиту података, GDPR такође успоставља окружење правне сигурности које користе и пословни субјекти и грађани, чинећи га кључним инструментом за регулисање података у савременом дигиталном окружењу.⁷³

Начела која регулишу правно поступање са подацима о личности представљају основне постулате на којима почива правилан поступак свих субјеката који обрађују или управљају овим подацима. Ови принципи су кључна смерница за сваког оператера или прерађивача, с обзиром да свака њихова активност мора да их поштује. Закон предвиђа обавезно поштовање ових принципа, а руковооци и прерађивачи могу бити санкционисани у случају њиховог кршења новчаном казном до 20 милиона евра или 4% укупног годишњег прихода компаније, у зависности од тога која је од ове две вредности већа.⁷⁴

Начела наведена у оквиру GDPR обухватају: 1) принцип законитости, поштења и транспарентности; 2) принцип сврхе обраде; 3) принцип минимизације; 4) принцип тачности; 5) принцип ограничења чувања; 6) принцип интегритета и поверљивости и 7) принцип друштвене одговорности.

Принципи законитости, поштења и транспарентности су суштински елементи правне регулативе за заштиту података, као што је дефинисано Општом уредбом о заштити података (GDPR). Законитост подразумева да се подаци могу прикупљати и обрађивати само у складу са јасно дефинисаним правним основама. Поштовање принципа поштења надограђује законитост, обавезујући руковооце података да поступају етички и пажљиво према личним подацима. Без поштовања принципа поштења, немогуће је испунити захтеве интегритета података. Транспарентност, као трећи принцип, директно повећава права појединаца чији се подаци прикупљају, омогућавајући им да буду обавештени о сврси, обиму, дужини чувања и приступу њиховим подацима на јасан и разумљив начин. Овај принцип не само да доприноси

⁷³Агенција Европске уније за основна права и Савет Европе (2018). *Приручник о европском праву заштите података*. Европска унија: Агенција Европске уније за основна права и Савет Европе, стр. 32.

⁷⁴Мајсторовић, М. (2020). Општа уредба Европског парламента и Савета Европске уније о заштити података (GDPR) – преглед и новине. *Библид*. XIX(73-74), стр. 106.

контроли над личним подацима, већ и унапређује поверљивост и безбедност тих података.⁷⁵

Приликом обраде података неопходно је поштовати принцип ограничења намене, што значи да се подаци могу прикупљати само за тачно дефинисану сврху. Пре прикупљања и обраде података, сврха мора бити јасно и недвосмислено одређена. Субјекат обраде података треба да буде обавештен о контексту прикупљања његових података и сврхама за које ће се они користити.⁷⁶

Принцип минимизације података проширује концепт сврхе обраде података увођењем захтева да се ограничи и број и обим прикупљених података. Према овом принципу, дозвољено је прикупљање само података који су неопходни за постизање дефинисане сврхе обраде података. С друге стране, сви подаци који нису неопходни за ову сврху представљају кршење права појединаца у складу са GDPR-ом. Овај принцип је директно подржан чланом 42 GDPR-а, који прописује мере заштите, укључујући концепте „приватност по дизајну“ и „приватност подразумевано“. Ови концепти захтевају да системи буду дизајнирани тако да интегришу заштиту безбедности и приватности, спречавајући прикупљање и обраду непотребних података.⁷⁷ Ограничење складиштења података директно је повезано са принципом сврхе обраде података, који захтева да се подаци чувају само онолико дуго колико је потребно за постизање те сврхе, уз транспарентно назначен период чувања.⁷⁸

Принцип тачности подразумева да подаци буду прецизни и ажурирани у складу са потребама. Поред тога, обрада података мора да обезбеди заштиту података и права на приватност субјеката чији се подаци прикупљају, применом одговарајућих законских, техничких и организационих мера за смањење ризика од повреде података, као и благовремене и адекватне реакције у случају инцидента, као што су губици, крађа или цурење података. Принципи поверљивости и интегритета су кључни у свим аспектима система заштите података, интегрисани у политике приватности, упозорења и обавештења о заштити података.⁷⁹ Сматрајући ове принципе основним за Општу

⁷⁵Исто, стр. 107.

⁷⁶Исто.

⁷⁷Кривокапић, Д., Адамовић, Ј., Тасић, Д., Петровски, А., Калезић, П., Кривокапић, Ђ. (2019). *Водич кроз Закон о заштити података о личности и GDPR – тумачење новог правног оквира*. Мисија ОЕБС-а у Србији и Share фондација, стр. 33.

⁷⁸Мајсторовић, М. (2020). нав. дело, стр. 108.

⁷⁹Исто.

уредбу о заштити података, циљ би требало да буде обезбеђивање и унапређење права субјеката чији се лични подаци прикупљају.

4. Заштита података о личности у Србији и поређење са регулативом ЕУ

У процесу развоја законодавства и правних прописа у Србији, заштита података о личности имала је своје корене у Уставу Краљевине Србије од 1888. године.⁸⁰ Члан 15. Устава гарантовао је неповредивост стана, док је члан 23. обезбедио заштиту тајности писама и телеграфских депеша, што можемо посматрати као ране облике заштите личних података у Србији. У периоду Социјалистичке Федеративне Републике Југославије (СФРЈ), заштита података о личности није била експлицитно регулисана, међутим, Уставом из 1974. године уређена су правила која су се односила на друштвени систем информисања.⁸¹ Потребно је споменути Закон из 1981. о основама друштвеног система информисања и информационом систему Федерације, који је успостављао одговорност грађана за осигуравање података неопходних за живот и рад у друштвеном систему информисања. Ипак, овај закон није детаљно разгледао заштиту личних података. Устав Републике Србије из 1990. године је укључивао формулацију која је гарантовала заштиту приватности података о личности, што је било значајно законодавство и суштински несрећно насупрот каснијим прописима.

У Србији је регулисање заштите података о личности почело доношењем Закона о заштити података о личности 1998. године, усклађивањем са Конвенцијом Савета Европе. Овај закон је, поред својих предности, имао и недостатке у регулисању процеса прикупљања, обраде и коришћења личних података. Током демократских промена ова питања су детаљније регулисана Повељом о људским и мањинским правима и грађанским слободама из 2003. године⁸². На даљи развој законодавства у области људских права и права на приватност значајно је утицао и Устав Републике Србије

⁸⁰Устав Краљевине Србије проглашен 22. децембра 1888. године на Великој Народној скупштини државној у Београду, преузето са: <https://ius.bg.ac.rs/wp-content/uploads/2020/11/USTAV-KRALJEVINE-SRBIJE-1888.pdf> (20.06.2024).

⁸¹Устав Социјалистичке Федеративне Републике Југославије из 1974. године, преузето са: https://www.yuhistorija.com/serbian/doc/Ustav_SFRJ_iz_1974.pdf (20.06.2024).

⁸²Повеља о људским и мањинским правима и грађанским слободама, Сл. лист СЦГ, бр. 6/2003.

усвојен 2006. године⁸³. Закон о заштити података о личности коначно је усвојен 2008. године, којим су успостављена системска правила за прикупљање, обраду и заштиту података о личности, што је Србију приближило правним стандардима Европске уније. Поред овог закона, унапређењу права на приватност и на ефективну заштиту допринели су и други закони, као што су Закон о парничном поступку⁸⁴ и Породични закон⁸⁵.

У стратегији усаглашавања са правним системима Европске уније и у циљу унапређења функционисања свог правног и надзорног система, Влада Републике Србије је 2010. године усвојила Стратегију за заштиту података о личности⁸⁶. Након тога, Министарство правде формирало је Радну групу 2013. године са задатком да развије нацрт новог закона. Група је укључивала представнике релевантних установа као што су Министарство одбране, Министарство правде и Министарство унутрашњих послова. Вођена моделом Закона о заштити података о личности⁸⁷, Радна група је радила пет година на састављању закона. Нови Закон је усвојен од стране Народне скупштине Србије 2018. године и почео је да се примењује девет месеци касније. Успостављањем овог закона, Србија је значајно усагласила свој регулативни оквир са европским стандардима, иако су се након његовог усвајања појавили неки изазови у погледу његове примене, укључујући нејасноће у домену судске праксе и ниског нивоа санкција. У сваком случају, овај закон је створио основу за даље унапређење законодавства и заштите личних података у земљи.

Закон о заштити података о личности (ЗЗПЛ) у складу је с уставним одредбама које регулишу законодавну делатност у области људских права и уређује питања повезана са заштитом података о личности. При изради закона, поштовани су општи стандарди за заштиту података, пре свега у складу са Општом уредбом о заштити података (GDPR) Европске уније. Ова иницијатива одраз је статуса кандидата за чланство у ЕУ, што је наша земља пратила усвајањем новог Закона о заштити података

⁸³Устав Републике Србије, Службени гласник РС, бр. 98/2006 и 115/2021.

⁸⁴Закон о парничном поступку, Службени гласник РС, бр. 72/2011, 49/2013 - одлука УС, 74/2013 - одлука УС, 55/2014, 87/2018, 18/2020 и 10/2023 - др. закон.

⁸⁵Породични закон, Службени гласник РС, бр. 18/2005, 72/2011 - др. закон и 6/2015.

⁸⁶Стратегија заштите података о личности из 2010. године, преузето са: <https://www.poverenik.rs/sr/%D0%BF%D0%BE%D0%B4%D0%B7%D0%B0%D0%BA%D0%BE%D0%BD%D1%81%D0%BA%D0%B8-%D0%B0%D0%BA%D1%82%D0%B84/942-strategija-zastite-podataka-o-licnosti.html> (20.06.2024).

⁸⁷Закон о заштити података о личности, Службени гласник РС, бр. 87/2018.

о личности.⁸⁸ Овде се истиче да су основна начела и принципи закона о заштити података у Републици Србији усклађени са Општом уредбом о заштити података (GDPR), која се односи на заштиту личних података у Европској унији. Закон о заштити података о личности у Републици Србији не само што усваја основне принципе GDPR-а, већ и захтева да сви посебни закони буду у складу са његовим одредбама.⁸⁹ Оваква законска регулатива осигурава конзистентност и заштиту личних података у свим аспектима обраде и управљања подацима.

⁸⁸Савовић, Д. и Савовић, М. (2020). Нормативно правни аспект заштите података о личности – упоредно правна анализа. У: *Зборник радова Заштита података о личности у Србији* (ур. Андоновић, С., Прља, Д. и Дилигенски, А.), Београд, стр. 158-159.

⁸⁹Закон о заштити података о личности, чл. 2, ст. 2.

III ПРИНЦИПИ И ЗАШТИТА ПОДАТАКА О ЛИЧНОСТИ У АНГЛОАМЕРИЧКОМ ПРАВУ

1. Англомеричко право у области заштите података о личности

У САД, за разлику од Европске уније, не постоји јединствен оквир или директива о заштити података. Уместо тога, закон о заштити података Сједињених Држава састоји се од мреже савезних и државних закона и прописа који регулишу руковање подацима у различитим индустријама и пословним операцијама. Да би се придржавале закона о заштити података САД, непрофитне организације које послују у Сједињеним Државама морају да се ослоне на савезне и државне законе и да их поштују. Генерално, савезни прописи регулишу прикупљање, складиштење и коришћење осетљивих личних података који нису јавно доступни. Државни закони, с друге стране, генерално регулишу захтеве за откривање података након кршења безбедности личних података који нису јавно доступни.⁹⁰

У контексту САД, процена заштите података у правосуђу представља изазов због сложеног федералног система власти. С обзиром на федерални систем владе САД, постоји више нивоа правосудних органа – савезни, државни и локални. Државна полиција и тужиоци, организовани на државном и локалном нивоу, врше независну власт и вођени су не само савезним законима, већ и државним законима, укључујући државне уставе и законе о приватности. Заштита података о личности суочава се са значајним изазовом због ограниченог уставног оквира који дефинише ову област политике, посебно у вези са правима грађана САД. За разлику од неких других домена, као што су слобода говора или законит процес где су уставне заштите јасније разграничене, право на приватност према Четвртом амандману није тумачено тако да свеобухватно обухвата заштиту личних података.⁹¹

Закони о приватности у САД се регулишу кроз мрежу савезних, државних и секторских закона и саморегулације. За разлику од Европске уније, која има Општу уредбу о заштити података (GDPR), у САД не постоји јединствени свеобухватни оквир заштите података. Међутим, Калифорнија је недавно усвојила Закон о приватности

⁹⁰Hasty, R., Nagel, T. W. & Subjally, M. (2013). *Data Protection Law in the USA*. Advocates for International Development, стр. 3.

⁹¹Bignami, F. (2015). *The US Legal System on Data Protection in the Field of Law Enforcement. Safeguards, Rights and Remedies for EU Citizens*. European Parliament, стр. 8.

потрошача из 2018. (ССРА), који је тренутно најсвеобухватнији закон о приватности у САД.⁹² У САД, законодавство о заштити података често је мета критика земаља које имају свеобухватније законе о заштити података. Аутори попут Бигнамија истичу сложену и, како се чини, непотпуну природу овог законодавства. У свом раду, Бигнами сугерише да су интереси који нису индивидуални често преовладавали у америчком законодавству о приватности⁹³, посебно оних трговинских и агенција за националну безбедност које су посвећене „свеједном“ приступу електронском надзору.⁹⁴

Од 1973. године, када је Министарство здравља, образовања и благостања САД (енгл. *US Department of Health, Education and Welfare*, HEW) објавило извештај под насловом „Компјутери и права грађана“, у САД се развио комплексан скуп правних инструмената за заштиту појединаца од „штетних последица које могу резултирати од аутоматизованих система личних података“.⁹⁵ Ови инструментикоји се у САД чешће називају заштитом приватности, а не заштитом података, укључују законе, преседане и уставна права. Ове друге надзире трипартитни систем провере и равнотеже, који стварају три одвојена, али подједнако важна огранка владе САД: законодавна, извршна и судска власт.⁹⁶

2. Правни акти која регулишу заштиту података о личности у англоамеричком праву

Прва америчка законодавна мера која се посебно бави штетним последицама личних информација похрањених у компјутеризованим базама података био је Закон о поштену кредитном извештавању из 1970. године. Често се помиње својим иницијалима – уобичајена пракса у америчком правном дискурсу – FCRA је донета да реформише индустрију извештавања о потрошачким кредитима, постављајући ограничења на дељење података и олакшавајући појединцима да исправе грешке, чије

⁹²Global Advertising Lawyers Alliance (GALA) (2020). *Privacy Law: A Global Legal Perspective on Data Protection Relating to Advertising and Marketing*. Volume 1, стр. 668.

⁹³Bignami, F. (2007). European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining. *Boston College Law Review*, 48, 609-698.

⁹⁴Robinson, J. (2014). The Snowden Disconnect: When the Ends Justify the Means. *SSRN*, 1-22.

⁹⁵Ware, W. H. (1973). *Records, Computers, and the Rights of Citizens*. RAND, стр. 1.

⁹⁶Swire, P. P. & Ahmad, K. (2012). *U.S. Private-sector Privacy*. Portsmouth, NH: International Association of Privacy Professionals, стр. 58.

последнице могу бити озбиљне. Многи Американци могу бити изненађени када сазнају да је први амерички председник који је истакао ова питања био Ричард Никсон 1974. године.⁹⁷ Овај историјски контекст показује колико је заштита приватности била важна чак и у раним фазама дигиталне ере у Сједињеним Државама.

Закон о поштену кредитном извештавању (енгл. *Fair Credit Reporting Act*, FCRA) из 1970. године представља кључни део закона у области заштите података, не само за Сједињене Државе већ и као модел са значајним утицајем на глобалном нивоу. Његови принципи и структура послужили су као нацрт за накнадне законе о заштити података, како на домаћем тако и на међународном нивоу. У својој сржи, FCRA оличава уравнотежен приступ који настоји да заштити интересе појединачних грађана, а истовремено се бави и потребама полиције и националне безбедности. Овај вишестрани приступ је од суштинског значаја за израду делотворног законодавства о заштити података у било којој јурисдикцији. Пре свега, FCRA наглашава важност индивидуалне сагласности и свести о прикупљању и коришћењу њихових личних података. Захтевајући обавештење и сагласност за прикупљање одређених врста личних података, FCRA овлашћује појединце да доносе информисане одлуке о својој приватности. Такође, FCRA успоставља снажан административни оквир за решавање притужби и осигуравање одговорности. Преко Федералне трговинске комисије (енгл. *Federal Trade Commission*, FTC) као одређене агенције, FCRA обезбеђује структурирани механизам за индивидуалну накнаду штете у случају злоупотребе података или неовлашћеног приступа. Ова административна процедура не само да нуди регрес за погођене појединце, већ служи и као одвраћање од повреда података и неправилног руковања личним информацијама.⁹⁸

Оно што је најважније, FCRA признаје легитимне потребе органа за спровођење закона и националних безбедносних агенција, истовремено намећући јасна ограничења и заштитне мере. Дефинисањем услова за приступ заштићеним подацима, FCRA успоставља деликатан баланс између права на приватност и јавних интереса. Било да се ради о налогу из четвртог амандмана који је подржан вероватним разлогом или судском позиву који је издало овлашћено особље, FCRA осигурава да приступ личним

⁹⁷Cobb, S. (2016). Data privacy and data protection: US law and legislation. An ESET White Paper (pp. 1-15), преузето са: https://www.researchgate.net/publication/309456653_Data_privacy_and_data_protection_US_law_and_legislation (20.05.2024).

⁹⁸Исто, стр. 2.

подацима подлеже ригорозној контроли и оправдању.⁹⁹ Утицај FCRA се протеже ван граница Сједињених Држава, обликујући оквире заштите података у другим земљама и међународним организацијама. Принципи артикулисани у FCRA, посебно они који се односе на праксу поштеност информисања, били су инструментални у развоју глобалних стандарда као што су ОЕЦД смернице о приватности података и Конвенција Савета Европе. Ови темељни документи, заузврат, представљају основне правне инструменте о заштити података у регионима попут Европске уније.¹⁰⁰

САД су историјски користиле нијансиран приступ заштити приватности података, што је пример њиховог законодавства које се бави одређеним категоријама информација. Ова стратегија се задржала до 1970-их година, посебно обележена доношењем Закона о породичним образовним правима и приватности из 1974. године (енгл. *Family Educational Rights and Privacy Act*, FERPA), кључног закона који има за циљ да заштити приватност евиденције о образовању ученика. Према FERPA-и, надзор над заштитом података поверен је Одељењу за образовање, што је представљало преседан за секторска регулаторна тела. Једна карактеристична карактеристика FERPA-е су њени строги захтеви за приступ заштићеним подацима органа за спровођење закона. За разлику од неких других америчких закона о приватности, FERPA налаже да је за такав приступ потребан или судски налог или законито издат судски позив, што одражава виши праг за упад.¹⁰¹ Међутим, вреди напоменути, као што је приметио Марфи, да корисност FERPA података у сврхе безбедности и спровођења закона може бити донекле ограничена, наглашавајући деликатну равнотежу између права на приватност и императива за спровођење закона.¹⁰²

Закон о праву на финансијску приватност из 1978. године (енгл. *Right to Financial Privacy Act*, RFPA) проширио је ову регулаторну парадигму на личне банкарске и рачуноводствене евиденције. Под управом америчког Министарства финансија, RFPA је увела мере за заштиту приватности финансијских информација, препознајући осетљивост таквих података. Током времена, RFPA је претрпео измене које имају за циљ да олакшају приступ заштићеним финансијским подацима органима за спровођење закона и промовишу извештавање банака регулаторним органима. RFPA

⁹⁹Gellman, R. (2014). Willis Ware's Lasting Contribution to Privacy: Fair Information Practices. *IEEE Security & Privacy*, 12(4), 51-54.

¹⁰⁰ Swire, P. P. & Ahmad, K. (2012). нав. дело, стр. 61.

¹⁰¹ Cobb, S. (2016). нав. дело, стр. 3-4.

¹⁰² Murphy, E. (2013). The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions. *Michigan Law Review*, 111(4), 485-546.

има посебан значај као претеча низа закона о приватности специфичних за сектор, подстакнутих значајним одлукама Врховног суда Сједињених Држава (енгл. *Supreme Court of the United States*, SCOTUS).¹⁰³

У недостатку америчког законодавства које експлицитно штити интересе субјеката података, секторском законодавству је додата заштита, посебно онима који су вођени новим технологијама. На пример, појава индустрије кабловске телевизије подстакла је доношење Закона о политици кабловских комуникација из 1984. године (енгл. *CableCommunications Policy Act*, CCPA). Посао са видео тркама подстакнут је доношењем Закона о заштити приватности у продаји видео записа из 1988. године (енгл. *Video Privacy Protection Act*, VPPA) када су представници Конгреса схватили да је срамота откривање података о изнајмљивању појединаца.¹⁰⁴

Закон *Gramm-Leach-Bliley* из 1999. године (енгл. *Gramm-Leach-Bliley Act*, GLBA) представља кључни закон који је настојао да преобликује пејзаж сектора банкарских и финансијских услуга у Сједињеним Државама. Првенствено усмерен ка дерегулацији, GLBA је имао за циљ да подстакне већу конкуренцију и иновације унутар индустрије. Међутим, усред овог притиска на дерегулацију, GLBA је такође препознао критичну потребу да се заштити приватност потрошача и обезбеди поштена пракса информисања, уводећи на тај начин Правило о финансијској приватности. Централни оквир GLBA-овог оквира била је заштита права на приватност појединаца, посебно у вези са њиховим финансијским подацима. У том циљу, уведене су строге мере за ограничавање неовлашћеног приступа таквим информацијама. Посебно, GLBA је изричито забранио употребу изговора, обмањујуће тактике коју користе приватни истражитељи да би добили поверљиве финансијске податке без пристанка или свести појединца. Ова забрана је имала за циљ сузбијање потенцијалних злоупотреба и очување интегритета права на приватност потрошача. Осим тога, законодавство је препознало важност заштите телекомуникационих записа појединаца, што је довело до доношења Закона о телефонским записима и заштити приватности из 2006. године (енгл. *Telephone Records and Privacy Protection Act*, TRPPA). Овај акт је посебно циљао на неовлашћено прибављање личних телефонских записа, чиме је ојачао шире циљеве заштите приватности наведене у GLBA.¹⁰⁵

¹⁰³ Cobb, S. (2016). нав. дело, стр. 4.

¹⁰⁴ Исто, стр. 5.

¹⁰⁵ Исто.

Ефикасно испитивање правних оквира као што је закон о заштити података значи разумевање њиховог порекла и развоја. Пример таквог извора је законодавство које штити посебно осетљиву врсту података - личне здравствене информације. У САД, ова врста података је заштићена Законом о преносивости и одговорности здравственог осигурања из 1996. године (енгл. *Health Insurance Portability and Accountability Act*, HIPAA). Осим наведених, постоји још три закона који допуњују законе о заштити података у САД: Закон о заштити приватности возача из 1994. године (енгл. *Driver's Privacy Protection Act*, DPPA), Закон о заштити приватности деце на интернету из 1998. године (енгл. *Children's Online Privacy Protection Act*, COPPA) и Закон о забрани дискриминације генетских информација из 2008. године (енгл. *Genetic Information Nondiscrimination Act*, GINA). Као и други закони, они омогућавају органима за спровођење закона приступ заштићеним подацима.¹⁰⁶Закон CAN-SPAM(енгл. *CAN-SPAM Act*), је још један кључни закон који утиче на већину непрофитних организација, који регулише слање комерцијалних порука е-поште. Од виталног је значаја за непрофитне организације да обезбеде да су њихове поруке са позивом у складу са захтевима овог закона, посебно када се обраћају појединцима који нису на њиховој листи чланова.¹⁰⁷

Федерални закони о заштити података у Сједињеним Државама се развијају како би одговорили на растућу забринутост око приватности података и заштите потрошача. Последњих година приметан је помак ка строжијем спровођењу ових закона од стране регулаторних тела. Очекује се да ће се овај тренд наставити у догледној будућности.Закон о Федералној трговинској комисији (енгл. *Federal Trade Commission Act*, FTCA) забрањује непоштене и обмањујуће праксе у трговини. Он обавезује организације, укључујући непрофитне, да се придржавају свих политика и процедура које су јавно објавиле. Ово наглашава важност транспарентности и одговорности у руковању подацима.Закон о Федералној трговинској комисији је донесен да забрани непоштене или обмањујуће радње или праксе у трговини или које утичу на трговину. Трговинска пракса је обмањујућа ако укључује „материјалну представу, пропуст или праксу која би у датим околностима могла довести у заблуду разумног потрошача на штету потрошача“. Федерална трговинска комисија је поднела тужбе против компанија, оптужујући их за обмањујуће поступке, када компанија није успела да адекватно

¹⁰⁶Исто, стр. 5-6.

¹⁰⁷ Hasty, R., Nagel, T. W. & Subjally, M. (2013). нав. дело, стр. 4.

заштити информације о потрошачима као што је обећано у њиховој политици приватности. FTC је такође подигао оптужбе према овом закону против компанија које су откриле информације о клијентима мимо одредби њихове политике приватности. Да би се придржавале FTCА, организације не би требало да обмањују потрошаче, купце или клијенте о коришћењу њихових личних података, и не би требало да прелазе обим својих политика приватности и обавештења датих својим клијентима.¹⁰⁸

Иако се чини да су у САД приватни интереси појединаца заштићени у многим ситуацијама, треба признати да ова заштита није универзална. На пример, не постоје експресне федералне заштите приватности за информације о резервацијама авио-компанија или информације о позајмици библиотеке. Читаве категорије података, као што су базе података о купцима и потенцијалним клијентима које се широко користе у продаји и маркетингу, немају експлицитну заштиту према савезном закону, иако неовлашћени приступ тим подацима може бити штетан за субјекте података. Такве празнине су навеле неке заговорнике приватности да направе неповољна поређења између закона о заштити података у САД и оних у европским земљама у којима су сви лични подаци аутоматски заштићени и где постоји национална канцеларија за заштиту података којој се појединци могу обратити за правну заштиту.¹⁰⁹ Иако такве критике могу бити оправдане, неки критичари имају тенденцију да потцене један или више аспеката америчке заштите приватности који још увек нису прегледани: закони савезне државе; улога Федералне трговинске комисије (енгл. *Federal Trade Commission*, FTC) као америчког чувара приватности и судска пракса.¹¹⁰ Државни закони често могу пружити додатни ниво заштите приватности који допуњује савезне прописе. FTC, иако није посебно дизајниран за заштиту приватности, има важну улогу у надгледању пракси компанија и организација у вези са прикупљањем и коришћењем личних података. Такође, судски преседани могу поставити границе и обликовати тумачење закона о приватности на начин који пружа додатну заштиту појединцима.

У Сједињеним Америчким Државама право на приватност је првенствено заштићено Првим амандманом који гарантује слободу говора и удруживања. Четврти амандман обезбеђује заштиту од неразумног претреса и одузимања личних докумената

¹⁰⁸ Исто, стр. 4-5.

¹⁰⁹ Bignami, F. (2007). нав. дело, стр. 651.

¹¹⁰ Bennett, C.J. (2011). In defense of privacy: the concept and the regime. *Surveillance & Society*, 8(4), 485-496.

или куће и гарантује поштовање закона.¹¹¹ Федерална трговинска комисија подржава саморегулацију индустрије у вези са приватношћу на мрежи. Иако се „поштене праксе информисања“ (енгл. *Fair Information Practices*, FIP) саме по себи не сматрају законодавством, оне представљају скуп принципа за законодавство и државни надзор.¹¹² На тај начин, слично Универзалној декларацији о људским правима у којој се у члану 12 наводи принцип да нико не сме бити подвргнут произвољном мешању у његову приватност, породицу, дом или преписку, нити нападима на његову части углед, свако има право на заштиту закона од таквог мешања или напада, али препушта конкретну правну примену тих идеала у рукама појединих нација.¹¹³ Пет FIP-ова које је усвојила FTC 1973. године - обавештење/свест, избор/пристанак, приступ/учешће, интегритет/безбедност и спровођење/задовољство – представљају подскуп од осам заштита садржаних у ОЕЦД-овим *Смерницама о приватности и прекограничним токовима – лични подаци*.¹¹⁴ Обавештења FIP-а су у основи идеје политике приватности у САД.

3. Начела заштите података о личности у англоамеричком праву

3.1. Први принцип заштите података о личности у англоамеричком праву – контрола приступа личним информацијама

Принципи су основа сваке гране права, формирајући апстрактне смернице које усмеравају стварање конкретних правила понашања. Они су као корени који хране стабло законодавства и правне праксе, обезбеђујући стабилност и доследност у примени закона. Принципи осликавају суштину и сврху закона или правне гране. Они

¹¹¹Bhasin, M. L. (2016). Privacy Protection Laws in Select Countries: Perspectives and Prospects. *International Journal of IT, Engineering and Applied Sciences Research (IJIEASR)*, 5(10), 7-21.

¹¹²Federal Trade Commission (2010). Protecting Consumer Privacy in an Era of Rapid Change: A proposed framework for business and policymakers, преузето са: <https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers> (21.05.2024).

¹¹³United Nations (2017). *The Universal Declaration Of Human Rights At 70: Still Working To Ensure Freedom, Equality And Dignity For All*. 30 Articles On The 30 Articles, United Nations, чл. 12.

¹¹⁴Organization for Economic Co-operation and Development (1980). OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, преузето са: https://www.oecd-ilibrary.org/science-and-technology/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_9789264196391-en (21.05.2024).

представљају суштину правног система, омогућавајући тумачење и примену норми у различитим ситуацијама. Управо због своје опште применљивости, принципи су кључно средство за разумевање права и правне праксе.¹¹⁵

Расправа о улози принципа у заштити података о личности је кључна за разумевање правног оквира који регулише ову област. Док се једни залажу за директно укључивање принципа у законске текстове, други сматрају да су они више декларативне природе и да њихово објашњење није неопходно у самим прописима.¹¹⁶ Међутим, постоји аргумент који подржава први приступ који тврди да принципи имају дубље значење него што су само набројани у законима. Они су заправо основа и темељ на коме почива сваки аспект законске регулативе о заштити података о личности. Принципи као што су транспарентност, ограничење сврхе, минимизирање података и одговорност не само да дефинишу како треба поступати са личним подацима, већ и постављају стандарде понашања за субјекте који их обрађују. Поред тога, принципи пружају флексибилност у тумачењу закона и прилагођавању различитим ситуацијама и технолошким променама. Без њих, закон би био ригидан и тешко применљив у пракси. Што се тиче аргумента да кршење принципа не доводи до санкција, то може бити тачно у неким правним системима. Међутим, то не умањује њихов значај. Принципи често служе као смернице за акцију, а њихово игнорисање може имати негативне последице у виду губитка поверења јавности, нарушавања репутације и могућих правних поступака.¹¹⁷

Последњих година дошло је до значајног пораста у прикупљању, коришћењу и откривању личних података. Овај тренд је подстакнут изузетном експанзијом *World Wide Web*-а који је постао саставни део савременог живота. Данас, електронска трговина игра кључну улогу у нашим свакодневним рутинама, са више појединаца који се ослањају на онлајн платформе за задатке који се крећу од куповине намирница до резервације авио карата. Пејзаж е-трговине у порасту је револуционисао начин на који спроводимо трансакције, чинећи га невероватно zgodним и приступачним за људе да извршавају задатке на даљину. Овај помак ка дигиталним платформама није само поједноставио процесе, већ је отворио и мноштво могућности за потрошаче и предузећа. Међутим, усред ове дигиталне револуције, забринутост у вези са

¹¹⁵ Vuković, M. (1953). *Interpretacija pravnih propisa*. Zagreb: Školska knjiga, стр. 128.

¹¹⁶ Андоновић, С. и Прља, Д. (2020). *Основи права заштите података о личности*. Београд: Институт за упоредно право, стр. 54.

¹¹⁷ Милков, Д. (2017). *Управно право II – управна делатност*. Нови Сад: Правни факултет, стр. 84-85.

приватношћу података постаје све израженија. Предузећа и организације у различитим секторима сада се боре са одговорношћу заштите личних података које су им поверили корисници. Сваког дана се суочавају са застрашујућим задатком безбедног и етичког управљања овим осетљивим подацима.¹¹⁸

Лични подаци су постали основа за модерне компаније и владе у обављању њихових услуга. Лични подаци се обрађују, чувају и откривају и често настају у процесу комерцијалне размене. Бројеви кредитних картица, појединачни идентификациони бројеви, евиденција о куповини, месечни приходи и сродни типови личних података играју важну улогу у овом комерцијалном информационом систему. Такве стране прикупљају, анализирају, чувају и деле више личних података. Информације о појединцима се тренутно одржавају у хиљадама база података, при чему се велики део тих информација реплицира у неколико база података. Процењује се да се информације о одређеној особи чувају у приближно 1000 различитих база података.¹¹⁹

Лакоћа са којом се личне информације могу креирати, приступити и користити изазива значајну забринутост не само за појединце већ и за организације. Једном када се лични подаци издају, контрола над њима често измиче, остављајући појединце подложним злоупотреби и експлоатацији. Ако размотримо сценарио где се лични подаци слободно деле на мрежи или их прикупљају различити субјекти без јасног пристанка или разумевања импликација, ово одустајање од контроле значи да појединци можда немају право гласа о томе како се њихови подаци користе или ко има приступ њима. У суштини, они губе власништво над нечим личним као што су њихове информације. Осим тога, како се открива више личних података, приватност се смањује. Ова ерозија приватности не погађа само појединце, већ представља изазове за организације које имају задатак да заштите осетљиве информације. Због тога језначајна чврста политика приватности и механизма за спровођење за заштиту од спољних и унутрашњих претњи.¹²⁰

Приватност на Интернету је веома важна, и зато се принцип контролисаног откривања личних информација често наглашава као најбољи начин за њену заштиту. Овај принцип нуди корисницима могућност да самостално одлучују о томе које

¹¹⁸Ghani, N. A. & Sidek, Z. M. (2009). Controlling and Disclosing your Personal Information. *Wseas Transactions on Information Science and Applications*, 3(6), стр. 397.

¹¹⁹Исто, стр. 397-398.

¹²⁰Исто, стр. 398.

информације желе да деле и са ким. За оне који желе још већу заштиту, могућност анонимног коришћења Интернета пружа додатни слој заштите. Коришћење анонимности омогућава корисницима да сурфују Интернетом без страха да ће њихове активности бити повезане са њиховим личним идентитетом. Ово је посебно корисно за особе које раде у осетљивим областима или које се просто брину за своју приватност. Ипак, важно је имати на уму да објављивање личних информација на Интернету може имати дугорочне последице. Чак и када се информације обришу, оне могу остати доступне на Интернету због праћења и архивирања. Због тога је од изузетне важности пазити на то које информације делимо на мрежи и сачувати своју приватност. На крају, један од најбољих начина да се заштити приватност на Интернету је комбиновање ових приступа.¹²¹

У савременом друштву, прикупљање личних података постало је неизбежно ради ефикасног функционисања разних система, од економије до безбедности. Међутим, појединци имају право на приватност и контролу над својим личним подацима. Овде настаје изазов - како балансирати ова два супротстављена интереса: право на приватност и право јавности на информације. Са једне стране, право на приватност је суштински елемент постојања демократског друштва. Оно обезбеђује појединцу слободу да контролише своје информације и да их не дели без њиховог одобрења. С друге стране, право на информације и доступност јавних информација је од суштинског значаја за функционисање друштва и демократије. Управо због тога, државе су пред изазовом да нађу равнотежу између ова два права. То подразумева усвајање законских и техничких механизма који ће штитити приватност грађана, али и омогућити потребне информације за функционисање друштва. Овде је од суштинског значаја прецизно дефинисање услова под којима се лични подаци могу користити, као и постојање независних тела која надгледају поштовање тих правила.¹²²

Подаци које делимо на мрежи и у офлајн окружењима могу бити изложени различитим опасностима, од злоупотребе од стране криминала или недобронамерних актера, до неконтролисане употребе од стране државе или приватних организација. Када размишљамо о заштити приватности података, треба узети у обзир неколико важних аспеката. Прво, ограничавање приступа одређеним врстама података је кључно. Овај принцип ограничава потенцијалну штету коју могу причинити неовлашћени

¹²¹Костић, М. и Вилић, В. (2013). Приватност корисника друштвених мрежа. *Зборник радова Правног факултета у Нишу*, LXIV, стр. 62.

¹²²Исто.

приступи и употребе података. Друго, обавеза да државни органи добију информације од недржавних субјеката уз поштовање приватности је битан елемент. Овај принцип осигурава баланс између безбедности и приватности грађана. Такође, једнако је важно да се грађани обавештавају о начину како се њихови подаци користе и обрађују. Транспарентност у овом процесу ствара поверење и омогућава људима да контролишу своје податке на адекватан начин. И на крају, примена техничких стандарда за заштиту података и стручно управљање су неопходни за осигуравање безбедности и приватности.¹²³ Централно за ово питање је недостатак контроле коју појединци имају над прикупљањем, употребом, складиштењем и откривањем њихових личних података од стране различитих субјеката, било да се ради о приватним компанијама или владиним агенцијама. Овај недостатак транспарентности и одговорности наглашава потребу за већим надзором и регулативом како би се подацима рукује одговорно и етички.

Док се безбедност података фокусира на спречавање неовлашћеног приступа подацима, питање приватности наглашава давање појединцима контроле над начином на који њиховим подацима управља и користи одређена организација. Повреде приватности личних података, које се називају и заштита података, настају када се лични подаци неправилно прикупљају, користе или откривају. Вестин је истакао три изјаве о томе како се људи слажу или не слажу са питањима приватности личних података:¹²⁴

- 1) потрошачи су изгубили сваку контролу над начином на који компаније прикупљају и користе личне податке,
- 2) већина предузећа поступа са личним подацима које прикупља о потрошачима на одговоран и поверљив начин и
- 3) постојећи закони и организациона пракса обезбеђују ниво заштите приватности потрошача који је данас разуман.

Важно је схватити да приватност није само питање индивидуалних права, већ и сложен концепт везан за друштвене, економске и политичке аспекте. Заштита приватности података захтева пажљиво балансирање између права појединаца да задрже контролу над својим личним подацима и потребе друштва да те информације

¹²³Cannataci, J. A. (1986). *Privacy and Data Protection Law: International Development and Maltese Perspectives*. Volume 87, Issue 1, CompLex (Series), Norwegian University Press.

¹²⁴Westin, A. (1967). *Privacy and Freedom*. New York: Atheneum, стр. 218.

користи у различите сврхе, као што су истраживање, маркетиншке активности или побољшање услуга. У потрази за решењима која омогућавају очување приватности података, истраживачи се све више ослањају на технике као што су шифровање података, анонимизација, диференцијална приватност и хомоморфно шифровање. Ове технике омогућавају приступ подацима без откривања осетљивих информација појединаца, чиме се постиже равнотежа између заштите приватности и коришћења података у сврхе које су корисне за друштво.¹²⁵

Идентификација сврхе, како је наведено у оквиру англо-америчког правног оквира заштите података, према FIP, служи као камен темељац у заштити личних података. У суштини, идентификација сврхе подразумева унапред информисање појединаца о намераваној употреби њихових личних података – пракса која је обично садржана у политици приватности. Примарна функција идентификације сврхе је да оснажи појединце да доносе информисане одлуке у вези са њиховим интеракцијама са организацијама, на основу тога како ће се њихови подаци користити. Давањем обавештења, организације омогућавају појединцима да врше контролу над приступом својим личним подацима. Ова контрола се манифестује у могућности да се одбије учешће ако се сматра да је предвиђено коришћење њихових података неприхватљиво.¹²⁶

Посебно, идентификација сврхе служи као механизам за контролу приступа, чиме се даје приоритет заштити приватности. Појединци могу остварити ову контролу одбијањем интеракција које могу угрозити њихову физичку или финансијску сигурност, као што је потенцијална изложеност прогонитељима или преварантима кроз неодговорно руковање подацима. Слично томе, појединци могу да одустану од ангажмана који укључују маркетиншке активности, тражећи предах од наметљивих наговарања или очување свог интегритета од неприкладне комодификације.¹²⁷

У контроли приступа личним информацијама, дискусија често почиње са два кључна принципа: знањем и сагласношћу. Принцип знања захтева да особе буду информисане о томе како ће њихове личне информације бити коришћене пре него што их поделе, док принцип сагласности подразумева да се особе морају сагласити са коришћењем њихових података на начин који је њима јасан и разуман. У светлу ових

¹²⁵Ghani, N. A. & Sidek, Z. M. (2009). нав. дело, стр. 398.

¹²⁶Harper, J. (2021). *Privacy and Fair Information Practices, The Struggle To Protect Threatened Values*. American Enterprise Institute, стр. 12.

¹²⁷Исто.

принципа, контрола приступа личним информацијама постаје кључна. Када особе имају знање о томе како ће њихови подаци бити коришћени и сагласност са тим коришћењем, то им пружа могућност да контролишу приступ својим информацијама. Ово није само питање поштовања приватности, већ и питање обезбеђивања других вредности као што су правда, безбедност, мир и тишина, аутономија, интегритет против комодификације и репутација. Међутим, постоје изазови у примени ових принципа у пракси. Један од њих је да је сазнање о коришћењу података субјективно и тешко доступно за особу која их прикупља, што може довести до проблема у обезбеђивању да људи буду довољно информисани, и да се њихов пристанак добије на јасан и разуман начин. Осим тога, истраживања показују да обавештења о приватности обично не доприносе значајно повећању нивоа знања људи, јер велики део људи једноставно пређе преко њих.¹²⁸

Како се наводи у оквиру FIP-а, овај принцип има значајан утицај на начин на који се подаци прикупљају и обрађују. Пре свега, он подстиче сервисне провајдере да ограниче прикупљање података на ону количину која је заиста неопходна за конкретну интеракцију. Овакав приступ не само што промовише приватност, већ и ограничава могућност злоупотребе података. На пример, ограничавање прикупљања података може да побољша безбедност како личних, тако и финансијских података, јер смањује доступност података за потенцијалне злоупотребе. Ограничавање времена задржавања података има директан утицај на контролу приступа другима кроз временску димензију. Када се подаци задржавају, постају доступни за дељење и коришћење, што може довести до губитка контроле над њима или изложености кроз кршење политика или безбедносне проблеме. Принцип задржавања података, као део FIP, има за циљ да ограничи ове ризике и тако обезбеди контролу приступа, што директно доприноси заштити приватности.¹²⁹

Приступ и исправка, као што је наведено у FIP, уводе сложену интеракцију, посебно у погледу заштите личних података у англо-америчким правним оквирима. Једна уочљива тензија која произилази из имплементације протокола приступа и корекције је њихова интеракција са мерама безбедности. Отварање приступа традиционално ограниченим подацима води ка рањивости, потенцијално излажући личне податке појединаца неовлашћеним странама. На пример, појединци који користе познате идентификаторе могу постати жртве лажног представљања, омогућавајући

¹²⁸Исто, стр. 13.

¹²⁹Исто, стр. 15-16.

варалицама да прикупе додатне податке или покрену нападе, чиме се проширује рањивост система, позната као његова „површина напада“. Ова динамика наглашава деликатну равнотежу између олакшавања приступа и заштите од кршења безбедности. Такође, давање права појединцима да исправе своје информације у базама података представља још један изазов за контролу приступа. С једне стране, овлашћивање појединаца да исправе нетачности повећава тачност података, али и повећава количину информација доступних другима. Супротно томе, допуштање права на исправку потенцијално би се могло искористити за фалсификовање информација, чиме се прикрива нечији прави идентитет и компликује напоре да се одржи тачна евиденција.¹³⁰

Препознајући ове сложености, принципи приватности АРЕС-а наглашавају важност провере идентитета пре одобравања приступа и сугеришу да одређени безбедносни захтеви могу захтевати ограничења директног приступа информацијама. Ово наглашава комплексност између омогућавања појединцима да управљају својим подацима и ублажавања ризика повезаних са неовлашћеним приступом и манипулацијом.

Ипак, треба нагласити да заштита личних података није само контрола приступа информацијама или осигурање поштеног третмана. Она обухвата шири спектар интереса који су замршено повезани са појмом контроле. Ови интереси се крећу од личне и финансијске сигурности до очувања аутономије. Ипак, у оквиру FIP -а, ови интереси се често третирају као деривати, а не као директно заштићени. То значи да иако су у оквиру FIP-а представљени као водећи принципи, они понекад не пружају свеобухватну визију заштите података. Недостаје им неопходна јасноћа и прецизност да би понудили практичне смернице у навигацији у сложености приватности података. Сходно томе, постављају више питања него што одговарају о томе како најбоље заштитити интересе потрошача. Потребно им је прецизирање како би се позабавили мноштвом интереса угрожених злоупотребом личних података. Проширујући свој обим изван пуке контроле приступа и нудећи јасније смернице, ови принципи могу боље да испуне своју предвиђену сврху заштите права на приватност података појединаца у дигиталном добу.

¹³⁰Исто, стр. 18.

3.2. Други принцип заштите података о личности у англоамеричком праву – правичност

У правној теорији до данас је задржано схватање правичности, које је формулисао Аристотел у Никомаховој етици. Према Аристотелу, правда подразумева да се свакоме да оно што му припада на основу заслуга или правичности. Ово схватање правичности истовремено укључује концепт правде, боље од одређене врсте праведности, али не боље од апсолутне правде. Правно право, с друге стране, често пропушта одређене ситуације због своје опште формулације, што може довести до недостатка правичности према Аристотеловом схватању.¹³¹

У праву САД-а, један од кључних аспеката права на приватност је принцип правичности, који се односи на фер третман личних података. То значи да организације које прикупљају, обрађују или користе личне податке морају осигурати да се ти подаци користе на етички и законит начин. Овај принцип се односи и на приватни сектор и на јавне институције које рукују личним подацима.¹³² Важно је да сваки појединац буде третиран праведно у погледу начина на који се његови подаци користе, да има право на приступ информацијама о томе како се његови подаци користе и да имају могућност да контролишу те податке колико год је то могуће. Ово укључује право на приступ, исправку и брисање података који се односе на ту особу. Законитост као део овог принципа наглашава да обрада података мора бити заснована на овлашћењу или сагласности, као и да се морају поштовати одредбе релевантних закона као што је Закон о заштити приватности података. Овај принцип поставља основна правила за прикупљање података пре него што се могу законски обрадити. С друге стране, правичност као део овог принципа је шири појам који захтева да се приликом обраде података поштују интереси и разумна очекивања лица чији се подаци обрађују. То значи да се лични подаци не смеју користити на штету појединаца, да се не сме злоупотребљавати монополски положај руковаоца подацима и да се обрада података увек мора вршити на транспарентан начин.¹³³

¹³¹Чавошки, К., Васић, Р. (2006). *Увод у право*. Београд: Правни факултет, стр. 91.

¹³²Нагрет, Ј. (2021). нав. дело, стр. 8.

¹³³Кривокапић, Д., Кривокапић, Ђ., Тодоровић, И., Комазец, С., Петровски, А., Ерцеговић, К. (2016). *Водич за органе власти – заштита податка о личности*. Америчка агенција за међународни развој и Share фондација, стр. 22.

Правичност или „поштење“ у контексту заштите података о личности у закону САД наглашава важност друштвених вредности поштовања интереса других. Неопходно је да обрада података о личности буде фер, што значи да се пристанак не сме добити обманом. Транспарентност је кључна компонента овог принципа јер се не односи само на обавештавање појединаца чији се подаци прикупљају о детаљима обраде, већ и на цео поступак. То подразумева да је увек јасно шта се дешава са подацима, зашто се то дешава, ко је одговоран за обраду тих података и како власници података могу да остваре своја права. Посебна пажња је посвећена језику који се користи у информисању о обради личних података. Требало би да буде сажет, транспарентан, разумљив и лако доступан, користећи јасне и једноставне речи. Ово је посебно важно ако су информације упућене малолетницима, осигуравајући да они јасно разумеју како се њихови подаци користе и шта то за њих значи.¹³⁴

Принцип поштене обраде у контексту заштите података о личности наглашава важност транспарентности и законитости у обради података. Према овом принципу, руковаоци подацима имају обавезу да јасно информишу субјекте и јавност о начину на који ће подаци бити обрађени и да покажу да је њихова пракса у складу са релевантним законима о заштити података. Обрада података се не сме вршити у тајности, а испитаници треба да буду свесни могућих ризика које таква обрада може да носи. Такође, руковаоци података морају поштовати жеље субјекта података, посебно када је сагласност носиоца података основа за правну обраду података.¹³⁵

У контексту интернет услуга и обраде података, према овом принципу, важно је да испитаници јасно разумеју како се њихови подаци обрађују, што превазилази само транспарентност. Принцип правичности наглашава важност етичке обраде личних података, посебно када се подаци не прикупљају директно од субјекта података.¹³⁶ У случају захтева за приступ подацима, руковалац података мора да пружи информације о извору података, ако су доступни, чиме се чува транспарентност и одговорност у обради података. Важно је напоменути да руковалац података не сме намерно да уништи информације о извору података како би их изузео од откривања, осим ако би

¹³⁴ Адамовић, Ј., Јовановић, М., Калезић, П., Кривокапић, Н., Перков, Б., Петровски, А. (2018). *Водич за медије: заштита личних података и новинарски изузетак*. Америчка агенција за међународни развој и Share фондација, стр. 19.

¹³⁵ Агенција Европске уније за основна права и Савет Европе (2018). нав. дело, стр. 120.

¹³⁶ Исто, стр. 121.

брисање било извршено пре пријема захтева за приступ, уз поштовање општих принципа одговорности.¹³⁷

3.3. Трећи принцип заштите података о личности у англоамеричком праву – приватност личних података

Један од ових принципа је концепт заштите приватности личних података, који је важан због потребе да се људима да контрола над својим личним подацима. Овај принцип се заснива на идеји да појединац треба да има право да контролише како се његови лични подаци прикупљају, користе и деле, чиме се штити приватност и аутономија сваког појединца.¹³⁸ У контексту америчког закона, приступ заштити приватности личних података је фрагментиран, јер САД немају општи закон о заштити података на националном нивоу, као што то имају неке друге земље попут земаља Европске уније. Уместо тога, САД имају вишеструке секторске законе и прописе који се баве заштитом одређених врста података или сектора, као што су здравствени подаци или финансијске информације.

Принцип приватности се односи на заштиту приватног интереса појединца или „приватног живота“, који покрива широк спектар ситуација. Судска пракса широко тумачи концепт „приватног живота“, укључујући интимне ситуације, осетљиве информације, као и информације које би могле да нашkode јавном мњењу и појединцу. Ово такође може укључивати аспекте нечијег професионалног живота и понашања у јавности. Међутим, утврђивање да ли је било мешања у „приватни живот“ зависи од специфичног контекста и околности сваког појединачног случаја.¹³⁹ Ако ове информације нису од јавног интереса и нема оправдања за њихову доступност широј јавности, приоритет би требало да буду заштита података и приватност. С друге стране, када су у питању јавне личности или информације од јавног значаја, приступ тим информацијама може бити оправдан, иако то може довести до задирања у основна права на заштиту података и приватност.¹⁴⁰

¹³⁷Исто, стр. 218.

¹³⁸Harper, J. (2021). нав. дело, стр. 8.

¹³⁹Агенција Европске уније за основна права и Савет Европе (2018). нав. дело, стр. 22.

¹⁴⁰Исто, стр. 58.

У контексту закона о заштити података о личности, неки подаци дубоко продиру у приватност грађана и стога захтевају строжу заштиту као основно људско право. На пример, информације као што су верска уверења или друге осетљиве информације заслужују већу заштиту у поређењу са мање осетљивим информацијама као што је број патика које носимо.¹⁴¹ У САД, примена закона о заштити личних података тумачи се у складу са овим принципом како би се обезбедило поштовање уставног права грађана на приватност у различитим контекстима обраде података. У зависности од врсте података које обрађују и размењују, надлежни су дужни да примењују одговарајуће мере техничке заштите. То укључује унутрашње пословање, као и комуникацију са другим органима власти и грађанима. Стандардизација безбедности података захтева утврђене процедуре, а анализом структуре информационог система уз помоћ техничких администратора могуће је усвојити одговарајуће стратегије заштите прилагођене сваком органу власти.¹⁴² Коришћењем посебне технологије за повећање приватности, као што је псеудонимизација, могуће је смањити могућност приписивања личних података испитанику. Ова технологија омогућава да подаци буду анонимизовани или да се користе псеудоними уместо правих имена или информација за идентификацију. Ово је посебно корисно у великим системима за обраду података где се обрађују велике количине информација, чиме се постиже повољно решење за заштиту приватности.¹⁴³ Псеудонимизација личних података игра кључну улогу у заштити приватности у различитим контекстима. Овај процес омогућава руковооцима подацима да сачувају поверљивост идентитета појединаца, што је посебно важно у истраживачким сценаријима или медицинским студијама. На пример, истраживачи могу да проучавају ток болести пацијената чији су идентитети скривени иза псеудонима, чиме се осигурава да руковооци подацима имају приступ само псеудонимизованим информацијама, а не и стварним идентитетима субјеката. Ова пракса чини псеудонимизацију кључним елементом у ланцу технологије заштите приватности, осигуравајући да заштита података буде саставни део система за обраду података.¹⁴⁴

Дужност је руковооца података да предузме одговарајуће мере заштите и смањи ризик од повреде права на заштиту података о личности, што произилази из уставних

¹⁴¹Кривокапић, Д., Кривокапић, Ђ., Тодоровић, И., Комазец, С., Петровски, А., Ерцеговић, К. (2016). нав. дело, стр. 15.

¹⁴²Исто, стр. 49.

¹⁴³Агенција Европске уније за основна права и Савет Европе (2018). нав. дело, стр. 128.

¹⁴⁴Исто, стр. 134.

гаранција приватности грађана и законских одредби. Приватност информација омогућава грађанима да сами одлуче када, како и у којој мери ће њихове информације бити саопштене другим лицима. То подразумева право на увид у њихове податке, на упознавање са начинима обраде, чувања и приступа овим подацима. Руковаоци података дужни су да у сваком тренутку контролишу цео циклус прикупљања, обраде и чувања података како би спречили кршење ових обавеза, до којих може доћи услед прекомерног прикупљања, неовлашћеног откривања или нестручног руковања подацима.¹⁴⁵

3.4. Четврти принцип заштите података о личности у англоамеричком праву – сигурност података

Четврти принцип у праву САД-а је заштита сигурности података појединаца. Сигурност је важна јер подаци могу бити злоупотребљени за бројне преваре, као што је крађа идентитета. Ова врста преваре укључује лажно представљање друге особе, отварање рачуна или накупљање дугова користећи податке жртве.¹⁴⁶ Крађа идентитета (енгл. *mobile phishing*) се дефинише као неовлашћено прибављање, пренос, поседовање или коришћење личних података који припадају физичком или правном лицу, са намером да се упусти у превару или друге криминалне активности.¹⁴⁷ Општи појам крађе идентитета обухвата различите моделе и манифестације крађе података о личности, као и различите методе и поступке њихове злоупотребе у извршењу нових кривичних дела. Такође, могу се уочити различити профили жртава, различити садржаји и вредности нанете штете, као и друге специфичности. Радња крађе података о личности најчешће има крајњи циљ који се постиже извршењем новог кривичног дела чије последице могу бити материјалне и нематеријалне природе. Крајњи циљеви крађе идентитета, поред финансијских и политичких, могу бити уцена, тероризам и слични облици злоупотребе.¹⁴⁸ Крађа идентитета представља праксу слања обмањујућих комуникација које се маскирају као легитимне и потичу из поузданог извора. Ова врста

¹⁴⁵Кривокапић, Д., Кривокапић, Ђ., Тодоровић, И., Комазец, С., Петровски, А., Ерцеговић, К. (2016). нав. дело, стр. 49.

¹⁴⁶Harper, J. (2021). нав. дело, стр. 8.

¹⁴⁷Organisation for Economic Co-Operation and Development (2008). *Scoping Paper on Online Identity Theft*, OECD Ministerial Meeting on The Future of Internet Economy, Seoul, стр. 3.

¹⁴⁸Ђукић, А. (2017). Крађа идентитета – облици, карактеристике и распрострањеност, *Војно дело*, 3/2017, стр. 101.

напада обично се остварује путем електронске поште, с циљем отуђења осетљивих информација, као што су подаци о кредитној картици и приступни подаци, или инсталације злонамерног софтвера на уређају жртве. Овакви компјутерски напади имају за циљ крађу информација, попут идентитета особе или финансијску добит. Чест облик ових напада је превара корисника да се преусмере на лажну веб локацију која изгледа доста слично оригиналној, чиме се добијају корисничка имена, лозинке, информације о банкама и кредитним картицама.¹⁴⁹

Финансијски сектор, укључујући банке и осигуравајућа друштва, у изазовној је позицији јер они не само да управљају личним подацима клијената, већ морају да обезбеде и сигурност њихових дигиталних трансакција. Иако је сектор значајно инвестирао у безбедносну инфраструктуру, недавни напади, попут оног на бразилску банку где су компромитовани подаци стотина хиљада клијената, показују да је и даље изложен значајним ризицима и губицима. Финансијски подаци захтевају посебне заштитне мере како би се обезбедила њихова тачност и сигурност. Системи електронског плаћања морају имати уграђене механизме за заштиту података, укључујући мере заштите приватности и техничке заштите. У овој области се често јављају специфични проблеми са заштитом података јер је неопходно применити одговарајуће механизме за аутентификацију и потврду.¹⁵⁰

Белгијско друштво за светске међубанкарске финансијске телекомуникације (SWIFT) је организација која олакшава глобалне трансфере новца између банака широм света. Већина европских банака користи SWIFT за ове трансакције, а подаци о овим трансакцијама често пролазе кроз центре за обраду података у САД. Амерички трезор је затражио приступ овим подацима за истраживање тероризма у оквиру свог програма праћења финансирања тероризма. ЕУ није сматрала да постоји адекватна правна основа за ову врсту размене података само зато што су подаци пролазили кроз центре у САД, посебно што се подаци односе на грађане ЕУ. Да би се овај проблем решио, 2010. године закључен је Споразум о SWIFT-у између ЕУ и САД. Овај споразум је успоставио јасне стандарде за заштиту података и правне основе за размену финансијских података у сврху спречавања, истраге, откривања или кривичног гоњења тероризма и финансирања терористичких активности. Према споразуму, Министарство финансија САД може да захтева финансијске податке од SWIFT-а под одређеним

¹⁴⁹Yu, W., Nargundkar, S., Tiruthani, N. (2008). A phishing vulnerability analysis of web-based systems. *Proceedings of the IEEE Symposium on Computers and Communications*, стр. 328.

¹⁵⁰Агенција Европске уније за основна права и Савет Европе (2018). нав. дело, стр. 343.

условима, као што су прецизност захтева и ограничење потребних података. Важно је напоменути да подаци који се односе на област јединственог плаћања у еврима нису обухваћени овим захтевом.¹⁵¹

Према Споразуму, Министарство финансија САД шаље захтеве Европолу, који затим проверава да ли се поштују одређени принципи. Ако пристану да се придржавају, SWIFT доставља финансијске податке директно Министарству финансија САД. Министарство чува ове податке у безбедном физичком окружењу, доступном само аналитичарима који истражују тероризам или његово финансирање. Подаци не смеју бити међусобно повезани са било којом другом базом података и морају бити избрисани најкасније пет година након пријема, осим ако је то неопходно за посебне истраге или кривично гоњење. Одељење може пренети информације из ових података органима за спровођење закона или агенцијама за борбу против тероризма, како унутар тако и ван Сједињених Држава, само у сврху истраге, откривања, спречавања или кривичног гоњења тероризма и његовог финансирања. За размену података са органима треће земље потребна је претходна сагласност надлежних органа државе чланице ЕУ, осим у случају непосредне и озбиљне опасности по јавну безбедност. Независна тела, укључујући она које је именовала Европска комисија, прате да ли се све ове процедуре спроводе у складу са SWIFT споразумом, укључујући право да прегледају претраге података у реалном времену или ретроактивно, да траже додатне информације и да блокирају претраге које крше заштитне мере мерама Споразума.¹⁵²

3.5. Пети принцип заштите података о личности у англоамеричком праву – транспарентност

Пети принцип заштите података о личности у праву САД-а односи се на транспарентност и информисање појединаца о томе шта се дешава са њиховим подацима. У модерним дигиталним контекстима, појединцима се често пружају превише сложена, правна и дуга обавештења о приватности која су ефективно бесмислена. Начело транспарентности у заштити података о личности је кључна

¹⁵¹Исто, стр. 268-269.

¹⁵²Исто, стр. 269.

компонента правних система који регулишу обраду података о личности. Основна сврха овог принципа је да грађанима омогући увид у све активности везане за њихове личне податке, укључујући прикупљање, обраду и доношење одлука. Тиме се обезбеђује да грађани могу да буду информисани о томе ко, када, на који начин и зашто користи њихове личне податке. Транспарентност такође промовише правичност у обради података, јер отворена пракса омогућава обављање законских активности без скривања или пропуштања информација.¹⁵³

Транспарентност у обради личних података је кључни принцип заштите приватности у правном оквиру Сједињених Америчких Држава. Иако не постоји јединствени савезни закон који регулише све аспекте заштите података, низом посебних закона и прописа обезбеђено је да грађани буду обавештени о обради својих података, да имају приступ овим подацима и да могу да захтевају исправке и брисање њихових информација. Ова транспарентност помаже у изградњи поверења између корисника и субјеката који обрађују њихове податке, што је неопходно у дигиталном добу.

Транспарентност наглашава отвореност у пракси руковања подацима, у супротности са идентификацијом сврхе, која се фокусира на специфицирање сврха за које се подаци прикупљају. Историјски гледано, концепт отворености у прописима о приватности може се пратити до утицајних докумената као што је HEW (енгл. *Health, Education, and Welfare*) извештај, који наглашава да не би требало да постоје системи за тајно вођење евиденције за личне податке. Ова препорука наглашава важност транспарентности у управљању подацима, са циљем да се оснаже надзорна тела и промовише равнотежа моћи између појединаца и организација које рукују личним подацима.¹⁵⁴ У суштини, док политике приватности детаљно наводе специфичне праксе, отвореност у FIP залаже се за ширу транспарентност, осигуравајући да постојање и рад система за руковање подацима не буду скривени од јавности или регулаторног надзора. Овај приступ је у складу са ширим напорима да се заштите права потрошача и приватност кроз законодавне оквире по узору на принципе који су слични поштеној радној пракси.

Транспарентност је мета-принцип заштите података, као што је и одговорност. У ствари, транспарентност је средство за постизање одговорности. Њена сврха је да

¹⁵³ Андоновић, С. и Прља, Д. (2020). нав. дело, стр. 56-57.

¹⁵⁴ Harper, J. (2021). нав. дело, стр. 17.

олакша примену других принципа заштите података, као што су приступ и исправка података. Када појединци желе да остваре таква права, требало би да буду у могућности да добију информације без неразумних напора у погледу времена, претходног знања, путовања и слично, као и без неразумних трошкова. Дизајнирање отворених или транспарентних друштвених система је изазов. То је проблем са две стране, јер мора постојати довољно информација или података изражених на одговарајући начин, али такође мора постојати и заједница мотивисана да обради те информације.¹⁵⁵

Ревизија америчког оквира за заштиту приватности пружа прилику за успостављање новог стандарда транспарентности који је усмерен на кориснике, контекстуалан и прилагођен специфичним употребама података и публици, укључујући оба модела, и активна (*push*) и пасивна (*pull*) обавештења, проактивна обавештења и информације на захтев. Требало би да постоји обавеза пружања основних информација појединцима када употреба података, примаоци и шири циљеви обраде можда нису очигледни појединцима, заједно са основним информацијама о било којим доступним опцијама избора, могућностима подношења жалби и правне заштите, контакт информацијама за додатне информације и сл. Организацијама мора бити дозвољена флексибилност да пруже додатну транспарентност на основу контекста планиране употребе података у слојевитом и кориснички оријентисаном формату.¹⁵⁶

Принцип транспарентности у односу на захтеве јавних власти за приступ личним подацима у праву САД-а подразумева да организације које учествују могу добровољно издавати периодичне извештаје о броју захтева за личним подацима које добијају од јавних власти ради спровођења закона или из разлога националне безбедности, у мери у којој су таква откривања дозвољена према важећем закону. Информације које пружају организације у овим извештајима, заједно са информацијама које је објавила обавештајна заједница, као и друге информације, могу се користити за информисање периодичног заједничког прегледа функционисања оквира ЕУ-САД заштите приватности (EU-U.S. DPF) у складу са принципима.

¹⁵⁵Исто.

¹⁵⁶Kurth, H. A. (2019). *Ten Principles for a Revised US Privacy Framework*. Center for Information Policy Leadership, стр. 2.

3.6. Шести принцип заштите података о личности у англоамеричком праву – ограничење сврхе и употребе података

Принцип ограничења сврхе је кључни аспект заштите података који има за циљ да обезбеди да се лични подаци обрађују на транспарентан и одговоран начин. Овај принцип подразумева да организације морају прецизно дефинисати сврху за коју прикупљају личне податке пре него што започну процес прикупљања. Овај приступ омогућава субјектима података да буду свесни разлога због којих се њихови подаци обрађују и дају свој пристанак на обраду у ту сврху. Примена овог принципа значи да организације не могу користити прикупљене податке за нове, некомпатибилне сврхе без додатног обавештавања субјекта података и добијања њиховог пристанка. На пример, ако компанија прикупља податке о клијентима ради обраде поруџбина, те податке не може касније користити за маркетиншке сврхе без претходног обавештења и пристанка клијената.

У контексту заштите података, овај принцип је такође важан јер омогућава појединцима да имају контролу над тим како и у коју сврху се њихови подаци користе, чиме се осигурава да се не осећају нападнуто или угрожено од стране компанија или организација које прикупљају њихове податке. Ово доприноси осећају сигурности и приватности, што је суштински део осећаја мирноће и одмора од спољног света. Примењен у пракси, овај принцип значи да компаније морају бити транспарентне и одговорне у свом приступу обради података, што доприноси грађењу поверења и поштовања према приватности појединаца, омогућавајући им да се повуку из света када то пожеље, без страха од злоупотребе њихових личних података.

Лични подаци треба да буду прикупљени у одређене, јасне и легитимне сврхе и не смеју се даље обрађивати на начин који није у складу са тим сврхама. Даља обрада у сврху архивирања у јавном интересу, за научно или историјско истраживање или у статистичке сврхе, у складу са Чланом 89(1), неће се сматрати неусклађеном са првобитним сврхама („ограничење сврхе“).¹⁵⁷ У складу са принципом ограничења сврхе, личне информације треба да буду ограничене на информације које су релевантне за циљеве обраде. Организација не сме обрађивати личне информације на начин који је несагласан са циљевима за које су прикупљене или касније одобрене од стране особе. У

¹⁵⁷Harper, J. (2021). нав. дело, стр. 6-7.

оквиру тих циљева, организација треба да предузме разумне кораке како би осигурала да су лични подаци поприлични за њихову намену, тачни, потпуни и актуелни. Организација треба да се придржава принципа ограничења сврхе док год чува такве информације. Информације које се могу идентификовати или идентификују могу се задржати само онолико дуго колико служе у сврхе обраде. Ова обавеза не спречава организације да обрађују личне податке на дужи период ако таква обрада разумно служи за сврхе архивирања у јавном интересу, новинарства, књижевности и уметности, научних или историјских истраживања и статистичких анализа. У овим случајевима, таква обрада мора бити у складу са другим принципима и одредбама. Организације морају предузети разумне и одговарајуће мере да би се придржавале ове одредбе. Прикупљање података без одређене сврхе је незаконито.

Када постоји потреба за обрадом података, оператер је дужан да јасно дефинише сврху овог прикупљања и обраде. Такође, лица чији се подаци обрађују морају бити на јасан и разумљив начин обавештена о сврси обраде, што подразумева забрану давања апстрактних или непрецизираних разлога за прикупљање података. Оправданост прикупљања података значи да постоји реална потреба за овим подацима, у складу са законским прописима.¹⁵⁸ Овде је транспарентност неопходна да би се спречила злоупотреба података од стране власти. Данас је уобичајено да се подаци користе на начине који нису првобитно били предвиђени или дозвољени законом, а те активности често остају непримећене. У пракси, органи власти морају да поштују законом прописане сврхе за које се подаци обрађују, а одступање од ових сврха може представљати озбиљан прекршај.¹⁵⁹

3.1. Седми принцип заштите података о личности у англоамеричком праву – одговорност

Да би систем правне заштите података о личности испунио своју заштитну улогу, неопходно је јасно дефинисати права и обавезе свих страна укључених у процес обраде података. У ове процесе најчешће су укључена физичка лица чији се подаци

¹⁵⁸ Андоновић, С. и Прља, Д. (2020). нав. дело, стр. 66-67.

¹⁵⁹ Кривокапић, Д., Кривокапић, Ђ., Тодоровић, И., Комазец, С., Петровски, А., Ерцеговић, К. (2016). нав. дело, стр. 22.

обрађују, као и субјекти који те податке обрађују, било да су физичка или правна лица, или државни органи. Друге стране, као што су примаоци података и трећа лица, могу бити укључени у обраду података, али је њихов значај мањи у односу на кључне учеснике.¹⁶⁰

С обзиром да оператер дефинише сврху обраде и управља личним подацима других људи, сноси одговорност за исправност и законитост обраде, као и за могуће последице. Овај принцип одговорности оператера за правилну обраду података о личности представља један од кључних принципа заштите података. Одговорност контролора се не односи само на лице чији су подаци предмет обраде, већ и на друштвену заједницу и очување јавног реда. На овај начин заштита података о личности доприноси очувању друштвених вредности и правног система у целини.¹⁶¹ Принцип одговорности подразумева преузимање одговорности за руковање личним подацима и за начин на који се руковаоци придржавају других принципа.¹⁶²

Одговорност за приватност подразумева прихватање обавезе заштите личних података. Одговорна организација треба да успостави одговарајуће политике и процедуре које подстичу добре праксе, које заједно чине програм управљања приватношћу. Циљ је да се постигне способност да се барем испуне захтеви релевантних закона о приватности. Када се примени на прави начин, требало би да ојача поверење потрошача и, као резултат, да донесе конкурентске и репутационе предности организацији.¹⁶³

Иако на први поглед делује једноставно, имплементација програма управљања приватношћу унутар организације захтева пажљиво планирање и укључивање различитих области и функција унутар компаније. Запослени у организацијама које теже одговорном пословању морају бити упознати са релевантним деловима програма управљања приватношћу. Поред тога, важно је да клијенти, партнери, као и пружаоци услуга буду информисани о кључним аспектима програма како би стекли поверење у његову ефикасност. Организације су, у случају инспекције или жалбе, дужне да повереницима за заштиту података презентују ажуриран и функционалан програм

¹⁶⁰ Андоновић, С. и Прља, Д. (2020). нав. дело, стр. 73.

¹⁶¹ Исто.

¹⁶² ICO, Accountability principle, преузето са: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/accountability-principle/> (20.09.2024).

¹⁶³ Office of the Information & Privacy Commissioner, Getting Accountability Right with a Privacy Management Program, преузето са: https://www.priv.gc.ca/media/2102/gl_acc_201204_e.pdf (20.09.2024).

управљања приватношћу. Такође, неопходно је да организације идентификују обавезе и ризике везане за приватност и да их интегришу у пословне моделе, технологије и праксе пре лансирања нових производа или услуга. Циљ је смањење ризика за саму организацију, запослене и кориснике, као и ефикасно управљање могућим кршењима приватности.¹⁶⁴

Појам одговорности у ширем смислу односи се на понашање у складу са друштвеним правилима и нормама. Употреба овог појма често имплицира да неко није испунио одређену обавезу.¹⁶⁵ Према најширем схватању, појам „одговорност“ може се разматрати из субјективне и објективне перспективе. Са субјективног аспекта, одговорност подразумева обавезу појединца да изврши одређену радњу, а уколико то није учинио, он осећа да треба да одговара за пропуст или неделовање. У објективном смислу, акценат није на осећајима појединца, већ на томе да ли је радња извршена или не.¹⁶⁶ Стога, одговорност укључује дужност појединца да обави одређени задатак, што подразумева полагање рачуна за поступке који су у супротности са законским нормама, правилима понашања, обичајима или моралним стандардима у друштву, због чега могу уследити одређене последице.¹⁶⁷ У правном контексту, одговорност се односи на поступање у складу са важећим законима и сношење последица за њихово кршење. Начело одговорности у односу на заштиту података подразумева обавезу лица које обрађује податке да поштује прописане норме и обезбеди исправност поступка обраде.¹⁶⁸

У Сједињеним Државама, Федерална трговинска комисија (FTC) примењује правило о заштитним мерама Закона о финансијским услугама (GLBA) на сву трговину. Овим законом, на основу принципа одговорности, утврђују се обавезе финансијских организација у вези са заштитом података о личности, али не прецизира конкретне начине на које те обавезе треба да се испуњавају.¹⁶⁹

¹⁶⁴Исто.

¹⁶⁵Илић Петковић, А. и Илић, М. (2017). Одговорност државних службеника и заштита њихових права. *Годишњак Педагошког факултета у Врању*, 1, (ур. Сунчица Денић), стр. 93.

¹⁶⁶Димитријевић, П. (2005). *Одговорност управе за нечињење - докторска дисертација*. Београд: Правни факултет, стр. 78-80.

¹⁶⁷Илић Петковић, А. и Илић, М. (2017). нав. дело, стр. 93.

¹⁶⁸Андоновић, С. и Прља, Д. (2020). нав. дело, стр. 74.

¹⁶⁹Federal Trade Commission, Data Protection Accountability: The Essential Elements A Document for Discussion, October 2009, преузето са: https://www.ftc.gov/sites/default/files/documents/public_comments/privacy-roundtables-comment-project-no.p095416-544506-00059/544506-00059.pdf(25.09.2024).

Приступ управљању подацима заснован на одговорности наглашава постављање циљева заштите приватности за организације, у складу са стандардима дефинисаним актуелним јавним политикама, док омогућава организацијама да саме одлуче о најприкладнијим мерама за постизање тих циљева. Овај приступ омогућава организацијама да примењују методе и праксе које су у складу са њиховим пословним моделима, технологијама и потребама корисника.¹⁷⁰

Приступ заснован на одговорности доноси директне користи појединцима, институцијама и регулаторима, јер је флексибилан и прилагодљив растућој количини података. Доприноси повезивању различитих регулаторних система, омогућавајући земљама да остваре заједничке циљеве заштите података кроз различите, али поуздане методе. Ово олакшава прекограничну размену података и обезбеђује једнаку заштиту података за појединце, без обзира на то где се њихови подаци налазе.¹⁷¹

Такође, овај приступ јача поверење појединаца да ће њихови подаци бити адекватно заштићени, смањујући њихову забринутост у вези са јурисдикцијама и локалним законима. Омогућава унапређење квалитета заштите података прилагођавањем алата специфичним ризицима и њихово брже ажурирање у складу са новим пословним моделима и технологијама. Организације не само да преузимају одговорност за податке којима рукују, већ се од њих тражи да покажу да имају одговарајуће системе, политике и обуку како би то доказали.¹⁷²

Већа флексибилност омогућава организацијама да ефикасније користе ограничене ресурсе намењене заштити приватности. Иако је за организације важно да се придржавају правила, ресурси који се троше на формалности, као што је обавештавање регулаторних тела, често нису доступни за друге, ефикасније мере заштите. Одговорност усмерава ресурсе на механизме који најефикасније обезбеђују заштиту података. Организације ће користити алате који на најбољи начин омогућавају постизање специфичних циљева заштите приватности и демонстрирати своју способност да их остваре.¹⁷³

Овај приступ не редефинише приватност нити замењује постојеће законе и прописе. Од организација се и даље тражи да се придржавају важећих закона, а

¹⁷⁰Исто.

¹⁷¹Исто.

¹⁷²Исто.

¹⁷³Исто.

регулаторни органи и организације ће и даље бити одговорни за постизање циљева заштите приватности. Међутим, приступ заснован на одговорности наглашава способност организације да покаже да може постићи дефинисане циљеве.¹⁷⁴

3.2. Осми принцип заштите података о личности у англоамеричком праву – минимизација

Принцип минимизације података налаже да они који прикупљају податке воде рачуна о врсти података које прикупљају и колико дуго се они чувају. Да би се испунио овај принцип, прикупљање података треба да буде ограничено само на оне информације које су неопходне и релевантне за постизање одређеног циља. У пракси, ово укључује процену да ли је потребно укључити личне информације у скуп података и колико дуго треба да се чувају пре него што се униште. Минимизација података такође укључује методе деидентификације, при чему се лични подаци уклањају из скупова података пре него што се поделе са другима или учине јавно доступним.¹⁷⁵

Овај принцип се примењује у већини фаза рада са подацима. Прикупљање најмање могуће количине података, њихово дељење само са онима којима су потребни и чување података само онолико колико је потребно доноси значајне предности приватности. Мање података смањује ризик од ненамерног откривања. Поред тога, минимизација података има финансијске користи јер организације троше мање времена и ресурса на прикупљање, обраду и складиштење сувишних података.¹⁷⁶

Принцип минимизације података подразумева да личне податке треба прикупљати и чувати у обиму који је пропорционалан, неопходан и ограничен искључиво на сврхе за које се обрађују.¹⁷⁷ Према овом принципу, лични подаци треба да буду: адекватни, релевантни и ограничени на оно што је неопходно у вези са сврхом обраде (минимизација података). Због тога је важно идентификовати минималну

¹⁷⁴Исто.

¹⁷⁵Elan, Data minimization, преузето са: <https://www.calpnetwork.org/wp-content/uploads/2020/09/Data-minimization-tip-sheet.pdf> (27.09.2024).

¹⁷⁶Исто.

¹⁷⁷Андоновић, С. и Прља, Д. (2020). нав. дело, стр. 81-82.

количину личних података неопходну за постизање одређеног циља. Требало би да чувате само те податке и ништа више.¹⁷⁸

Овај принцип укључује три основна елемента: 1) пропорционалност обраде података; 2) неопходност обраде података и 3) нужност обраде података. Пропорционалност се сматра задовољеном када је обим обраде података у равнотежи са циљевима који се желе постићи. У односу на неопходност, важно је размотрити да ли обрада података доприноси постизању легитимног циља. Када говоримо о нужности, то се односи на питање да ли је за постизање циља потребно обрадити одређену количину података или би мања количина могла бити довољна. Ово такође укључује ограничавање периода чувања података на минимум. Приликом процене неопходности треба узети у обзир да ли је могуће остварити сврху обраде на други начин, без обраде личних података.¹⁷⁹

Према принципима праксе поштеног информисања (енгл. *Fair Information Practices Principles*, FIPPS), организације треба да прикупљају личне информације (енгл. *Personally Identifiable Information*, ПИ) које су директно релевантне и неопходне за постизање дефинисаних циљева. Такође, ПИ треба да се задржи само онолико колико је неопходно за испуњавање те сврхе.¹⁸⁰

Да би се смањило прикупљање личних података (ПИ), кључно је прво разјаснити шта подразумева ПИ. У суштини, ПИ се дефинише као свака информација која директно или индиректно идентификује или се може користити за идентификацију живе особе. Међутим, ПИ такође може укључити различите комбинације података (понекад наизглед безазлених) које омогућавају идентификацију појединца. С обзиром да су електронски трансфери обично усмерени на појединце или домаћинства, програми електронских трансфера често захтевају ПИ како би се ефективно циљала помоћ и обезбедило да се помоћ додели правом кориснику.¹⁸¹

¹⁷⁸ICO, Principle (c): Data minimization, преузето са: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/data-minimisation/> (27.09.2024).

¹⁷⁹Андоновић, С. и Прља, Д. (2020). нав. дело, стр. 82.

¹⁸⁰Elan, Data minimization, преузето са: <https://www.calpnetwork.org/wp-content/uploads/2020/09/Data-minimization-tip-sheet.pdf> (27.09.2024).

¹⁸¹Исто.

3.3. Девети принцип заштите података о личности у англоамеричком праву – квалитет и интегритет

Треба предузети све разумне мере како би се обезбедио квалитет обрађених личних података, што је од суштинског значаја за испуњавање предвиђених циљева. Ова тема постаје посебно важна када се значајне одлуке о појединцима доносе на основу нетачних информација, посебно када су у питању аутоматизоване одлуке, алгоритми и вештачка интелигенција. Такве ситуације могу имати озбиљне последице по одлуке које се тичу финансија, истраживања и кривичних дела. Аутоматизоване одлуке се морају ослањати на тачне податке, а системи морају бити обучени користећи тачне и непристрасне информације. Интегритет укључује осигурање тачности личних података и спречавање неовлашћених промена од стране спољних страна. Ово укључује предузимање мера за заштиту система од потенцијалних покушаја хаковања.¹⁸²

Према америчком закону, принцип квалитета и интегритета података значи да савезне агенције, као што је Министарство за унутрашњу безбедност, имају одговорност да обезбеде тачност, релевантност, правовременост и потпуност информација које могу да идентификују личности (ПИ). Ова обавеза је од суштинског значаја за заштиту приватности појединаца, као и за јачање поверења јавности у институције власти.¹⁸³ Да би се постигао висок ниво квалитета података, требало би применити ригорозне процедуре прикупљања и верификације података. Ово укључује редовне провере и ажурирање података, као и механизме за идентификацију и исправљање грешака. Поред тога, важно је осигурати да се прикупљени подаци користе искључиво у сврхе за које су прикупљени, чиме се додатно штити интегритет информација. Овај принцип доприноси развоју одговорног и транспарентног управљања подацима, што је неопходно за очување грађанских права и слобода.

У америчком праву, принцип квалитета и интегритета приватности података наглашава потребу да се обрађују само оне информације које су релевантне за одређене сврхе. Овакав приступ не само да штити права појединаца, већ доприноси и поверењу у

¹⁸²Özkan, I. (2024). Data Protection Principles: The 7 Principles Of GDPR Explained, преузето са: <https://www.cyberpilot.io/cyberpilot-blog/data-protection-principles-the-7-principles-of-gdpr-explained/> (27.09.2024).

¹⁸³U.S. Department of Homeland Security, Privacy Policy Guidance Memorandum, преузето са: https://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf (27.09.2024).

систем обраде података. Поред тога, законодавни прописи, као што су Калифорнијски закон о заштити приватности потрошача (ССРА) и Закон о заштити приватности деце на мрежи (СОРРА), постављају посебне захтеве за прикупљање, задржавање и коришћење података, наглашавајући важност интегритета података и права појединаца на приступ и исправку информација. Ови закони доприносе стварању јасног оквира који осигурава да се подаци прикупљају и користе на начин који поштује приватност појединаца и истовремено подржава пословне потребе.¹⁸⁴

¹⁸⁴Gellman, R. (2024). Fair Information Practices: A Basic History, преузето са: <https://bobgellman.com/rg-docs/rg-FIPshistory.pdf> (28.09.2024).

IV ЗАКЉУЧАК

Поштовање права на приватни живот омогућава сваком појединцу да формира и развија одређене аспекте свог идентитета. Информације о овим аспектима су кључне јер значајно утичу на обликовање личности појединца. У доба интензивне комуникације заштита података о личности добија посебан значај, јер приватност се може схватити као супротност јавности која подразумева слободу избора и аутономију воље. Међутим, подела животних сфера на јавну и приватну није довољно јасна да би прецизно одредила границе уласка у нечију приватност, што чини ову тему сложенom и зависном од контекста.

Уставом гарантована права и слободе служе као заштита појединца од неовлашћеног уплитања државних власти у његову гарантовану сферу слободе. Приватност подразумева и независност у одређивању сопственог тела и изражавању личног идентитета. Овај концепт такође укључује ограничења приступа трећих лица личном простору појединца.

Приватност се може разматрати и у контексту обраде личних података. Права везана за обраду података укључују обраду у складу са законом и прилагођавање обраде циљевима за које су подаци прикупљени. Обрада личних података мора бити безбедна, а за то је потребно успоставити механизме одговорности за оне који обрађују податке, укључујући питања као што су зашто се подаци обрађују, под којим условима и коме се подаци преносе.

Тренутна правна ситуација у вези са заштитом података у Сједињеним Државама је сложена и технички захтевна, као и правна питања која се постављају у вези са предлозима за стварање јединствене федералне политике за заштиту података. Осим у екстремним случајевима и у случајевима приступа личним подацима од стране владе, "право на приватност" које се развило у општем праву и уставној доктрини пружа мало заштите просечном кориснику интернета. Иако је Конгрес усвојио неколико закона који имају за циљ повећање права појединаца у вези са заштитом података, тренутни мозаик федералних закона углавном је ограничен на одређене индустријске учеснике, одређене типове података или праксе које су непоштене или обмањујуће. Овај мозаик приступа се односи и на одређене државне законе. У настојању да се успостави свеобухватнији систем заштите података, неке државе, као

што је Калифорнија или сама Европска унија, усвојиле су широке законе који регулишу многе облике личних података. Неки тврде да би Конгрес требало да разматра стварање сличних заштита у федералном закону, али други критикују приступ Европске уније и Калифорније у погледу заштите података.

У Сједињеним Америчким Државама, заштита личних података је углавном фрагментирана и регулисана на федералном и државном нивоу, са бројним законима који се баве специфичним аспектима заштите података. Иако постоје снажни механизми заштите, потреба за свеобухватним федералним законом остаје значајна тема у правним и политичким дискусијама. Кључне карактеристике англо-америчког система укључују нагласак на престанку, права на приступ и исправку података, као и обавезе организација да осигурају адекватне мере заштите. Ови елементи су критични за изградњу поверења корисника и одржавање интегритета дигиталне економије.

Први принцип заштите личних података у англо-америчком праву, који се односи на контролу приступа личним информацијама, представља кључни елемент у обезбеђивању приватности и сигурности појединца у дигиталном добу. Овај принцип подразумева да субјекти података имају право да знају ко приступа њиховим подацима, у које сврхе и под којим условима. Контрола приступа личним информацијама није само правна обавеза, већ и морални императив који има за циљ заштиту достојанства и аутономије појединаца. С обзиром на брзи технолошки развој и све већи обим прикупљања и обраде података, неопходно је континуирано прилагођавати правне механизме како би се обезбедила адекватна заштита. Истовремено, појединци морају бити едуковани и оснажени да активно управљају својим подацима, што подразумева разумевање њихових права и начина на који могу да их остваре.

ЛИТЕРАТУРА

1. Адамовић, Ј., Јовановић, М., Калезић, П., Кривокапић, Н., Перков, Б., Петровски, А. (2018). *Водич за медије: заштита личних података и новинарски изузетак*. Америчка агенција за међународни развој и Shareфондација.
2. Агенција Европске уније за основна права и Савет Европе (2018). *Приручник о европском праву заштите података*. Европска унија: Агенција Европске уније за основна права и Савет Европе.
3. Андоновић, С. (2019). *Заштита података у електронској јавној управи у Републици Србији – правни аспекти - докторска дисертација*. Београд: Правни факултет.
4. Андоновић, С. и Прља, Д. (2020). *Основи права заштите података о личности*. Београд: Институт за упоредно право.
5. Bignami, F. (2007). European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining. *Boston College Law Review*, 48, 609-698.
6. Bignami, F. (2015). *The US Legal System on Data Protection in the Field of Law Enforcement. Safeguards, Rights and Remedies for EU Citizens*. European Parliament.
7. Bennett, C.J. (2011). In defense of privacy: the concept and the regime. *Surveillance & Society*, 8(4), 485-496.
8. Bhasin, M. L. (2016). Privacy Protection Laws in Select Countries: Perspectives and Prospects. *International Journal of IT, Engineering and Applied Sciences Research (IJEASR)*, 5(10), 7-21.
9. Беванда, М. и Чолаковић, М. (2016). Правни оквир за заштиту особних података у праву Европске Уније. *Зборник Правног факултета Универзитета у Ријеци*, 37(1), 125-154.
10. Бадовинац, Н. (2018). Осврт на GDPR уредбу и сугестије за развој апликативне подршке. *Инфо М*, 17(65), 11-16.
11. Брковић, Р., Јовановић, З. И Тотих, М. (2019). Право на приватност и заштиту личних података запосленог као пацијента у праву Републике Србије. *Анали Правног факултета Универзитета у Зеници*, 13(24), 205-224.
12. Cannataci, J. A. (1986). *Privacy and Data Protection Law: International Development and Maltese Perspectives*. Volume 87, Issue 1, CompLex (Series), Norwegian University Press.

13. Checkland, P., Holwell, S. (1998). *Information, Systems and information Systems: Making Sense of the Field*. New York: Wiley.
14. Clinton, L., Amit, S. (2008). Understanding Consumer Privacy: A Review and Future Directions. *Academy of Marketing Science Review*, 12(02), 1-7.
15. Carey, P. (2014). *Data Protection: A practical guide to UK and EU law*. Oxford.
16. Cunningham, M. (2018). Complying with International Data Protection Law, *University of Cincinnati Law Review*, 84(2), 421-450.
17. Чавошки, К., Васић, Р. (2006). *Увод у право*. Београд: Правни факултет.
18. Димитријевић, П. (2005). *Одговорност управе за нечињење - докторска дисертација*. Београд: Правни факултет.
19. David, H. (2009). *The Right to Privacy*. Infobase Publishing.
20. Ђукић, Д. (2017). Заштита података о личности са освртом на ново законодавство Европске Уније у овој области. *Правни записи*, 1, 49-60.
21. Ђукић, А. (2017). Крађа идентитета – облици, карактеристике и распрострањеност, *Војно дело*, 3/2017, 99-118.
22. Džombić, I. J. (2010). *Evropska unija: prošlost, sadašnjost, budućnost*. Sarajevo: Friedrich-Ebert-Stiftung.
23. Ghani, N. A. & Sidek, Z. M. (2009). Controlling and Disclosing your Personal Information. *Wseas Transactions on Information Science and Applications*, 3(6), 397-406.
24. Gondwe, M. (2011). *The Protection of Privacy in the Workplace: A Comparative Study - doctoral dissertation*. University of Stellenbosch.
25. Gellman, R. (2014). Willis Ware's Lasting Contribution to Privacy: Fair Information Practices. *IEEE Security & Privacy*, 12(4), 51-54.
26. Global Advertising Lawyers Alliance (GALA) (2020). *Privacy Law: A Global Legal Perspective on Data Protection Relating to Advertising and Marketing*. Volume 1.
27. Гајин, С. (2019). *Заштита података о личности у сектору безбедности, водич кроз законску регулативу*. Београд: Центар за унапређивање правних студија и Организација за европску безбедност и сарадњу.
28. Hondius, F. (1975). *Emerging Data Protection in Europe*. Amsterdam.
29. Hasty, R., Nagel, T. W. & Subjally, M. (2013). *Data Protection Law in the USA*. Advocates for International Development.
30. Harper, J. (2021). *Privacy and Fair Information Practices, The Struggle To Protect Threatened Values*. American Enterprise Institute.

31. Илић Петковић, А. и Илић, М. (2017). Одговорност државних службеника и заштита њихових права. *Годишњак Педагошког факултета у Врању*, 1, (ур. Сунчица Денић), 93-106.
32. Јовановић, С. (2014). Приватност и заштита података на интернету. *Твининг пројекат ЕУ – зборник Везе cyber криминала са ирегуларном миграцијом и трговином људима*, Министарство унутрашњих послова Републике Србије.
33. Kurth, H. A. (2019). *Ten Principles for a Revised US Privacy Framework*. Center for Information Policy Leadership.
34. Костић, М. и Вилић, В. (2013). Приватност корисника друштвених мрежа. *Зборник радова Правног факултета у Нишу*, LXIV, 53-78.
35. Комшић Ј., (2013). *Принципи Европске уније*. Асоцијација мултиетничких градова југоисточне Европе.
36. Кривокапић, Д., Кривокапић, Ђ., Тодоровић, И., Комазец, С., Петровски, А., Ерцеговић, К. (2016). *Водич за органе власти – заштита податка о личности*. Америчка агенција за међународни развој и Shareфондација.
37. Кривокапић, Д., Адамовић, Ј., Тасић, Д., Петровски, А., Калезић, П., Кривокапић, Ђ. (2019). *Водич кроз Закон о заштити података о личности и GDPR – тумачење новог правног оквира*. Мисија ОЕБС-а у Србији и Share фондација,
38. Murphy, E. (2013). The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions. *Michigan Law Review*, 111(4), 485-546.
39. Младенов, М. (2013). Заштита права на приватност у пракси Европског суда за људска права. *Зборник радова Правног факултета у Новом Саду*, 3, 575–593.
40. Милков, Д. (2017). *Управно право II – управна делатност*. Нови Сад: Правни факултет.
41. Мајсторовић, М. (2020). Општа уредба Европског парламента и Савета Европске уније о заштити података (GDPR) – преглед и новине. *Библид*. XIX(73-74), 99-117.
42. Organisation for Economic Co-Operation and Development (2008). *Scoping Paper on Online Identity Theft*, OECD Ministerial Meeting on The Future of Internet Economy, Seoul.
43. Robinson, J. (2014). The Snowden Disconnect: When the Ends Justify the Means. *SSRN*, 1-22.

44. Swire, P. P. & Ahmad, K. (2012) *U.S. Private-sector Privacy*. Portsmouth, NH: International Association of Privacy Professionals.
45. Sharma, M. (2017). Data Theft: Implications for Economic and National Security. *Journal of Defence Studies*, 11(1), 61-80.
46. Симовић, И., Лазић, М. (2014). Грађанско правна заштита права личности. *Зборник радова Правног факултета у Нишу*, 68, 269-290.
47. Савовић, Д. и Савовић, М. (2020). Нормативно правни аспект заштите података о личности – упоредно правна анализа. У: *Зборник радова Заштита података о личности у Србији* (ур. Андоновић, С., Прља, Д. и Дилигенски, А.), Београд, 153-168.
48. Tzanou, M. (2013). Is data protection the same as privacy? An analysis of telecommunications' Metadata Retention Measures. *Journal of Internet Law*, 17(3).
49. Vuković, M. (1953). *Interpretacija pravnih propisa*. Zagreb: Školska knjiga.
50. Водинелић, В. (2007). Право заштите личних података. У: *Право информационих технологија*, Београд: Правни факултет Универзитета „Унион“, Службени гласник.
51. Yu, W., Nargundkar, S., Tiruthani, N. (2008). A phishing vulnerability analysis of web-based systems. *Proceedings of the IEEE Symposium on Computers and Communications*, 326–331.
52. Warren, S. & Brandeis, L. (1890). The Right to privacy, *Harvard Law Review*, 4(5), 193-220.
53. Westin, A. (1967). *Privacy and Freedom*. New York: Atheneum.
54. Westin, A. (1968). Privacy and freedoms. *Washington and Lee Law Review*, 25(1).
55. Ware, W. H. (1973). *Records, Computers, and the Rights of Citizens*. RAND.

Правни извори

56. Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.1.1981.
57. 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, OJ L 281, 23.11.1995, p. 31–50.

58. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37–47.
59. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13.4.2006, p. 54–63.
60. Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (Text with EEA relevance), OJ L 337, 18.12.2009, p. 11–36.
61. Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, OJ L 24, 30.1.1998, p. 1–8.
62. Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services (Text with EEA relevance), OJ L 337, 18.12.2009, p. 37–69.
63. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89–131.
64. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37–47.

65. Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information, OJ L 345, 31/12/2003, p. 90–96.
66. European Union, Charter of Fundamental Rights of the European Union, Official Journal of the European Communities, 2000/C364, 18.12.2000.
67. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L 119, 4.5.2016, p. 1–88.
68. Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12.1.2001, p. 1–22.
69. Regulation (EU) 2016/679 (General Data Protection Regulation) in the current version of the OJ L 119, 04.05.2016; cor. OJ L 127, 23.5.2018.
70. United Nations (2017). *The Universal Declaration Of Human Rights At 70: Still Working To Ensure Freedom, Equality And Dignity For All*. 30 Articles On The 30 Articles, United Nations.
71. Закон о општем управном поступку, Службени гласник РС, бр. 18/2016, 95/2018 - аутентично тумачење и 2/2023 - одлука УС.
72. Закон о тајности података, Службени гласник РС, бр. 104/2009.
73. Закон о слободном приступу информацијама од јавног значаја, Службени гласник РС, бр. 120/2004, 54/2007, 104/2009, 36/2010 и 105/2021.
74. Закон о заштити података о личности, Службени гласник РС, бр. 87/2018.
75. Закон о парничном поступку, Службени гласник РС, бр. 72/2011, 49/2013 - одлука УС, 74/2013 - одлука УС, 55/2014, 87/2018, 18/2020 и 10/2023 - др. закон.
76. Повеља о људским и мањинским правима и грађанским слободама, Сл. лист СЦГ, бр. 6/2003.
77. Породични закон, Службени гласник РС, бр. 18/2005, 72/2011 - др. закон и 6/2015.
78. Стратегија заштите података о личности из 2010. године, преузето са: <https://www.poverenik.rs/sr/%D0%BF%D0%BE%D0%B4%D0%B7%D0%B0%D0%BA%D0%BE%D0%BD%D1%81%D0%BA%D0%B8->

[%D0%B0%D0%BA%D1%82%D0%B84/942-strategija-zastite-podataka-o-licnosti.html](#) (20.06.2024).

79. Устав Краљевине Србије проглашен 22. децембра 1888. године на Великој Народној скупштини држаној у Београду, преузето са: <https://ius.bg.ac.rs/wp-content/uploads/2020/11/USTAV-KRALJEVINE-SRBIJE-1888.pdf> (20.06.2024).
80. Устав Социјалистичке Федеративне Републике Југославије из 1974. године, преузето са: https://www.yuhistorija.com/serbian/doc/Ustav_SFRJ_iz_1974.pdf (20.06.2024).
81. Устав Републике Србије, Службени гласник РС, бр. 98/2006 и 115/2021.

Интернет извори

82. Cobb, S. (2016). Data privacy and data protection: US law and legislation. An ESET White Paper (pp. 1-15), преузето са: https://www.researchgate.net/publication/309456653_Data_privacy_and_data_protection_on_US_law_and_legislation (20.05.2024).
83. Elan, Data minimization, преузето са: <https://www.calpnetwork.org/wp-content/uploads/2020/09/Data-minimization-tip-sheet.pdf> (27.09.2024).
84. Federal Trade Commission (2010). Protecting Consumer Privacy in an Era of Rapid Change: A proposed framework for business and policymakers, преузето са: <https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers> (21.05.2024).
85. Federal Trade Commission, Data Protection Accountability: The Essential Elements A Document for Discussion, October 2009, преузето са: https://www.ftc.gov/sites/default/files/documents/public_comments/privacy-roundtables-comment-project-no.p095416-544506-00059/544506-00059.pdf (25.09.2024).
86. FPC, Fair Information Practice Principles (FIPPs), преузето са: <https://www.fpc.gov/resources/fipps/> (20.05.2024).
87. Gellman, R. (2024). Fair Information Practices: A Basic History, преузето са: <https://bobgellman.com/rg-docs/rg-FIPshistory.pdf> (28.09.2024).

88. ICO, Accountability principle, преузето са: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/accountability-principle/> (20.09.2024).
89. ICO, Principle (c): Data minimization, преузето са: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/data-minimisation/> (27.09.2024).
90. Organization for Economic Co-operation and Development (1980). OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, преузето са: https://www.oecd-ilibrary.org/science-and-technology/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_9789264196391-en (21.05.2024).
91. Office of the Information & Privacy Commissioner, Getting Accountability Right with a Privacy Management Program, преузето са: https://www.priv.gc.ca/media/2102/gl_acc_201204_e.pdf (20.09.2024).
92. Özkan, I. (2024). Data Protection Principles: The 7 Principles Of GDPR Explained, преузето са: <https://www.cyberpilot.io/cyberpilot-blog/data-protection-principles-the-7-principles-of-gdpr-explained/> (27.09.2024).
93. Sham, S., What Is Data Theft? преузето са: <https://www.okta.com/blog/2020/07/data-theft/> (15.05.2024).
94. U.S. Department of Homeland Security, Privacy Policy Guidance Memorandum, преузето са: https://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf (27.09.2024).

САЖЕТАК

Овај рад се бави америчким приступом заштити личних података, који је критикован због своје фрагментиране природе, што доводи до недоследности и празнина у заштити у различитим секторима и државама. Иако систем представља изазов за предузећа у навигацији кроз разнолике захтеве и за потрошаче који могу имати проблема са разумевањем својих права, дебата о потреби за свеобухватним савезним законом о приватности података је у току. Заговорници тврде да би такав закон ускладио заштиту и пружио јасније стандарде, док противници упозоравају на ризик од прекомерне регулативе. У контексту англоамеричког правног система, концепт контроле приступа личним информацијама је кључни аспект регулисања ових података, а принципи заштите података представљају основни оквир за разумевање те регулативе. Циљ овог рада је да истражи и анализира природу и дomet принципа заштите података у контексту англоамеричког права, укључујући еволуцију законских оквира и специфична правна решења усвојена за имплементацију ових принципа. Посебна пажња биће посвећена анализи регулаторних оквира који доприносе заштити права на приватност у дигиталном добу.

Кључне речи: податак, личност, заштита, САД, принцип

SUMMARY

Principles of Privacy Protection in United States Law

This paper examines the US approach to personal data protection, which has been criticized for its fragmented nature, leading to inconsistencies and gaps in protection across sectors and countries. Although the system presents a challenge for businesses to navigate the diverse requirements and for consumers who may have trouble understanding their rights, the debate over the need for a comprehensive federal data privacy law is ongoing. Proponents argue that such a law would harmonize protections and provide clearer standards, while opponents warn of the risk of overregulation. In the context of the Anglo-American legal system, the concept of controlling access to personal information is a key aspect of the regulation of this data, and the principles of data protection represent the basic framework for understanding that regulation. The aim of this paper is to explore and analyze the nature and scope of data protection principles in the context of Anglo-American law, including the evolution of legal frameworks and the specific legal solutions adopted to implement these principles. Special attention will be paid to the analysis of regulatory frameworks that contribute to the protection of the right to privacy in the digital age.

Keywords: data, personality, protection, USA, principle

БИОГРАФИЈА

Тијана Божић рођена је 30.04.1996. у Нишу. Завршила је Основну школу „Стефан Немања“, а затим је уписала Гимназију „Бора Станковић“ у Нишу коју је завршила 2015. године. Исте године уписала је Правни факултет Универзитета у Нишу, који је завршила са просечном оценом 8,77, 20. маја 2021. године. Током основних студија обављала је стручну праксу у адвокатској канцеларији Братислава Тодоровића у Нишу.

Након завршених основних студија, обављала је приправнички стаж у својству адвокатског приправника - волонтера у трајању од две године, у адвокатској канцеларији Снежане Станковић Цонић у Нишу. Мастер академске студије је уписала 2023/2024 године, смер Право и информационе технологије. У том периоду, обавила је стручну праксу у компанији „Better Collective“ доо у Нишу у трајању од десет радних дана.

Тренутно је запошљена у компанији „Better Collective“ доо у Нишу у правном тиму, на позицији асистента за правне операције.

Од страних језика говори енглески и немачки.

ИЗЈАВА О ИСТОВЕТНОСТИ

ШТАМПАНОГ И ЕЛЕКТРОНСКОГ ОБЛИКА МАСТЕР РАДА

Име и презиме аутора мастер рада: Тијана Божић

Наслов мастер рада: Принципи заштите приватности у праву Сједињених Америчких Држава

Ментор: Проф. др Милош Прица

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

У Нишу, _____

Потпис аутора

ИЗЈАВА О АУТОРСТВУ И ОДОБРАВАЊУ ОБЈАВЉИВАЊА МАСТЕР РАДА

Изјављујем да сам мастер рад, под насловом „Принципи заштите приватности у праву Сједињених Америчких Држава“ пријављен и објављен на Правном факултету Универзитета у Нишу:

- представља резултат сопственог истраживачког рада;
- није у целини, нити у деловима с моје стране пријављиван за одбрану на другим факултетима или универзитетима;
- не крши ауторска права или интелектуалну својину других лица.

Дозвољавам да се овај мастер рада чува у библиотеци и објави на сајту Правног факултета Универзитета у Нишу.

Аутор мастер рада: Тијана Божић

У Нишу, _____

Потпис аутора
