УНИВЕРЗИТЕТ У НИШУ
ПРАВНИ ФАКУЛТЕТ

Јавноправна заштита података о личности

(мастер рад)

Ментор:
Доц. др Дејан Вучетић

Студент:
Ивана Станковић
М 014/14 - О

Ниш, 2016

САДРЖАЈ

I УВОД

Предмет овог мастер рада је јавноправна заштита података о личности, са посебним освртом на међународне стандарде у пружању заштите овог права у савременом добу.

Право на приватност једно је од основних људских права чија је заштита загарантована у међународној заједници. У оквиру њега се развија и право на заштиту података о личности, које се данас се услед велике актуелности и важности полако одваја и све више јавља као самостално право.

Значај ове теме порастао је услед брзог развоја технологије и стварања нових начина за манипулацију подацима о личности. Право је неспремно дочекало ове промене, а постојећа законска регулатива која је штитила право на приватност није успела да одговори новим потребама савременог друштва и преплитањима нових технологија и приватности појединаца. То је довело до бројних злоупотреба података о личности и повреде права на приватност које право није могло да санкционише.

Ипак, ситуација се мења, па законодавци приступају детаљној правној регулацији ове области. У том циљу поступају и Уједињене нације, Европски суд за људска права као тело Савета Европе, Европска унија и Суд правде Европске уније и Сједињене Америчке Државе као предводници у стварању правила које касније прихвата и остатак света.

Како је у науци и пракси познат либералнији приступ који Сједињене Америчке Државе имају приликом заштите права на приватност, посебан изазов се јавља у начину регулисања трансфера података о личности из Европе у Сједињене Америчке Државе. Америчке компаније које послују у Европи често избегавају европске законе на тај начин што податке прикупљају у Европи, а обраду врше у Америци. Стога ће део рада обрадити постојећу регулативу у тој области, односно нови оквир „ЕУ-САД штит приватности“ који је 2016. године заменио до тада важеће принципе „Сигурне луке“.

Као битан орган у заштити података о личности, државе успостављају независтан државни орган – повереника за заштиту података о личности, који у оквиру управног поступка пружа заштиту грађанима чијим се подацима рукује. У нашој земљи

постоји Повереник за заштиту информација од јавног значаја и заштиту података о личности, који игра битну улогу како у заштити, тако и у едукацији јавности о њиховим правима везаним за приватност. Његова улога је регулисана Законом о заштити података о личности, који је уз Закон о општем управном поступку најважнији у процесном смислу.

Аутор ће се посебно осврнути на околност употребе нових информационих технологија путем којих се пружају услуге корисницима, а у ком циљу се користе њихови подаци о личности. У том процесу, пружаоци услуга рукују огромним количинама података који конкретно одређују лице, или великим броја података преко којих је лице одредиво, те стварно или потенцијално управљају приватношћу корисника. Јављају се у форми свеобухватних пружаоца услуга путем претраживача интернета, мобилних телефона и мобилних апликација, као и интернет сајтова који користе податке о личности, стваран свет селе „online“ и стварају велику заједницу у којој обавезе њених чланова нису истоветно регулисане као у стварном свету. Зато ће у раду бити обрађена и Гуглова политика у вези са заштитом приватности, као једног од највећих руковалаца подацима о личности, а којом се уређује начин на који се прикупљају и даље обрађују подаци о личности корисника Гуглових сервиса.

II О ПРАВУ ПРИВАТНОСТИ УОПШТЕ

Приватност је комплексан појам који је тренутно пред многим изазовима насталим услед развоја у науци и технологији. Као покретна мета, она временом еволуира, добија различите облике и вредности. Зато се и дефиниције приватности разликују, чинећи појам и културолошки различитим.[1]

Једна од најпознатијих дефиниција приватности је настала пре више од сто година, када су право на приватност Семјуел Ворен и Луис Брандеис назвали „правом да се буде остављен на миру“[2], што је подразумевало заштиту личне аутономије, моралног и физичког интегритета, право на избор животног стила и начина живота, интеракције са другим људима и сл. Алан Вестин је тврдио да је приватност више од

[1] A. Moore, Privacy rights: Moral and legal foundations, *The Pennsylvania State University Press, University Park, Pennsylvania*, 2010, pp 11.

[2] S. Warren and L. Brandeis, The Right to privacy, *Harvard Law Review*, Vol. 4, No. 5, pp. 193-220.

тога – то је способност да контролишемо колико информација о себи откривамо другима, како и када то чинимо.[3]

Данас се право на приватност сврстава у основна људска права, а услед комплексности и тешкоће дефинисања одређени аутори посматрају приватност кроз неколико аспеката:

1. приватност података – успостављање правила за прикупљање и поступање са подацима о личности,
2. приватност тела – заштита људског тела од инванзивних процедура,
3. приватност преписке – безбедност и приватност писама, телефонских разговора, електронске и друге комуникације,
4. приватност територије – која подразумева успостављање граница уласку трећих лица у лични простор појединаца. [4]

Као основно људско право, право на приватност је признато и загарантовано у Конвенцији за заштиту људских права и основних слобода (1950), Универзалној декларацији о људским правима (1948), Повељи и основним правима у Европској унији (2007).

III О ЗАШТИТИ ПОДАТАКА О ЛИЧНОСТИ

Заштита података о личности је грана права која се бави начином на који организације могу и треба да рукују личним подацима.[5] Као концепт настала је услед брига везаних за повећану централизацију података о личности и стварања огромних база података. Међутим, супротно од права на приватност, чији је примарни циљ заштита једног од основних људских права, заштита података о личности је створена из других разлога – економског интереса.

[3] A. Westin, Privacy and freedoms, *in: Washigton and Lee Law review*, Bodley Head, 1970.

[4] У. Мишљеновић, Б. Недић, А. Тоскић, *Заштита приватности у Србији – Анализа примене Закона о заштити података о личности*, Београд, 2013, страна 8.

(преузето дана 25.08.2016. године: http://partners-serbia.org/privatnost/wp-content/uploads/2013/07/Zastita-privatnosti-u-Srbiji.pdf)

[5] P. Carey, Data Protection, *A practical guide to UK and EU law,* Oxford, 2014, страна 1.

Пример за то је Приручник за приватност који је створила Организација за економску сарадњу и развој (ОЕЦД), а којим се као примарни циљ поставља политика која побољшава економски и социјални стандард[6] - заштита није повезана са људским правима, већ са олакшаним протоком података и информација између земаља. Информација има економску вредност, а могућност да једна земља чува и обрађује одређене податке даје тој земљи политичку и технолошку предност над другим земљама.[7]

Из сличних разлога је и Европска унија почела да регулише заштиту података о личности. Директива о заштити појединаца у вези са обрадом података о личности и слободном протоку таквих података 95/46/ЕЦ (у даљем тексту Директива, Директива о заштити података о личности), је била први документ у Европској унији усмерен на заштиту података о личности.[8] Директивом је требало остварити два циља:

1. Хармонизовати различите закона земаља чланица у вези са заштитом података о личности,
2. Обезбедити слободно кретања података између земаља чланица.[9]

Данас се Директива сматра једним од најстрожих регулатива у овој области.[10]

Од тада, право на заштиту података о личности у Европској унији заузима битно место, а о важности овог права говори и чињеница да је од ступања на снагу Лисабонског уговора из децембра 2009[11], право на заштиту података о личности постало самостално основно људско право у ЕУ. Тиме се чини разлика у односу на преостале међународне документе у којима се ово право, услед другачије регулативе,

[6] M.Tzanou, Is data protection the same as privacy? An analysis of telecommunications' Metadata Retention Measures, *Journal of Internet Law*, 2013, Вол. 17, Издање 3, страна 24.

[7] L. Joinet, као што је цитирано у J. Eger, *Emerging restrictions on transnational data flows: Privacy protections or non-tariff barriers?* 10 Law and Policy in International Business, 1978, страна 1065, 1066.

[8] Директива 95/46/ЕС Европског парламента и Савета од 24. октобра 1995. године о заштити појединаца у вези са обрадом података о личности и слободном кретању тих података, Службени гласник Европске уније Л 281 , 23/11/1995 П. 0031 – 0050.

[9] *Ibid*, Чл. 1.

[10] M. Cunningham, Complying with International Data Protection Law, *University of Cincinnati Law Review, Vol. 2, No. 84*, 2016.

[11] Чл. 16б, Лисабонски уговор којим се мења Уговор о Европској унији и Уговор о оснивању Европских заједница, потписан у Лисабону, 13. децембра 2007. Године, Службени гласник Европске уније, Ц 306, 17 December 2007.

углавном штити у оквиру права на приватност. Признато је као такво чланом 8. Повеље ЕУ, која данас има обавезујући карактер међу државама чланицама.

Право на заштиту података о личности се односи на сет правних норми насталих у циљу заштите права, слобода и интереса појединаца чији су подаци о личности сакупљани, чувани, обрађивани, дељени са трећим лицима, брисани и сл.[12]

Значајан допринос дефиницији овог права даје Директива Европске Уније о заштити података о личности, која заштиту података о личности дефинише као заштиту „фундаменталних права и слобода појединаца, и поготово њихово право на приватност у односу на обраду података о личности.” [13]

Централни појмови који доприносе разумевању концепта заштите података о личности су, стога, „обрада“ и „подаци о личности”. Под обрадом се подразумева било која операција која се врши над подацима, од њиховог прикупљања, снимања, чувања, употребе, до објављивања, дељења са трећим лицима, чињења јавно доступним, брисања и уништавања. Подаци се сматрају подацима о личности када могу бити повезани са конкретним појединцем.

Како произлази из Директиве о заштити података о личности – члан 1.1, циљ заштите је регулисање специфичне праксе, односно обраде података о личности. Стога заштита података о личности прихвата неминовност обраде података, али, због осетљивости и потенцијалне претеће природе тог процеса, ствара се неколико квалитативних цензуса и процедуралних гаранција које се сматрају довољним да заштите слободу појединаца чији се подаци о личности обрађују.

Субјекти чији се подаци обрађују не поседују своје податке, нити, у већини случајева, могу да спрече обраду својих података. Према тренутном стању ствари, руковаоци подацима имају право да обрађују податке који се тичу других. Стога је заштита података о личности врло прагматична – под њом се претпоставља да приватним и јавним установама мора бити омогућена употреба података о личности, јер је то често неопходно због друштвених разлога.

[12] F. Hondius, Emerging Data Protection in Europe, Амстердам, 1975, страна 16.
[13] Директива 95/46/EC, *op.cit.*

Зато нас право на заштиту података о личности не штити од обраде, већ од нелегалне и непропорционалне обраде података.

Како је заштита података о личности растући корпус правила и принципа, иста морају бити узета у обзир како од стране законодавца који ствара нове законе, тако и од стране руковаоца подацима о личности.

Као што је неминовно и са свим друштвеним областима, регулисање ове области никада неће бити готово. Нова правила и принципи настају сваки пут када нови изазови изникну услед континуираног развоја технологије. Стога није једноставно дефинисати преовлађујући интерес у заштити података о личности, јер је њих много, почевши од аутономије, информационе самоопредељености, баланса у снагама, поделе исти, до интегритета и достојанства, до демократије и плурализма.

Немогуће је сумирати заштиту података о личности у две или три реченице. То је свеобухватан термин за мноштво идеја у вези са заштитом података о личности. Примењујући те идеје, државе покушавају да помире основне, али супротстављене вредности, као што су приватност, слободан ток информација, потреба за надзором од стране владе, примена пореза и слично.

1. Однос права на приватност и права на заштиту података о личности

Право на заштиту података о личности је несумњиво у вези са правом на приватност, али је њихов однос тешко конкретно одредити и направити јасне разлике и сличности.

Оно се може описати и као шири појам у односу на приватност, али са друге стране и као конкретнији. Шири је, јер се поред права на приватност односи и на заштиту других права и интереса, као што су слобода изражавања, слобода вероисповести и мишљења, слободан проток информација и принцип недискриминације и јер уређује заштиту података о личности чак и када приватност тиме није повређена. Његова конкретност се огледа у константној примени – сваки пут када се обрађују лични подаци. Такође, примена правила о заштити података се не огледа у оцени да ли је дошло до кршења права на приватност, већ се врши увек када се испуне услови предвиђени законом за обраду података о личности. Осим тога,

законске норме о заштити података нису забрањујуће по природи, већ служе да усмеравају и контролишу начин на који су лични подаци обрађивани.[14]

Приватност је, такође, и шири и ужи појам у односу на заштиту података о личности – право на приватност може наћи примену и у случајевима када се не врши обрада података о личности, али та радња свеједно вређа нечију приватност, али се неће применити у случају обраде података о личности којом се не утиче на нечије право на приватност. Последице нелегалне обраде података о личности не морају имати последице само у смислу приватности, већ и у смислу осталих основних права и слобода, од којих је забрана дискриминације најочигледнија могућност за повреду.

Дакле, прва ствар на коју треба указати јесте да право на приватност и право на заштиту података о личности нису идентична права, али је њихово преплитање неминовно.[15]

Посматрајући право Европске уније, увиђа се да комунитарно право разликује формално два фундаментална права: право на приватност и право на заштиту података о личности.[16] Стога је јасно да се ова два права макар формално разликују. Ипак, посматрајући њихову садржину, нејасно је да ли су она у потпуности и суштински различита или се преклапају.

Иако Европски суд за људска права разликује право на заштиту података о личности и право на приватност и формално и суштински, ова два права имају преклапања. Суд под приватношћу обухвата ту обраду уколико закључи да се том

[14] M. Friedwald, D. Wright, S. Guzwirght and E. Mordini, Privacy, data protection and emerging sciences and technologies: Towards a common framework; in: *Innovation – The European Journal of Social Science Research, Vol. 23, No. 1,* 2010, страна 63.

[15] J. Kokott and C. Sobotta, The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR, *International Data Privacy Law*, 2013, Vol. 3, No. 4, pp. 223.

[16] Повеља Европске уније о основним слободама, *op.cit.*,

Члан. 7.

1. Свако има право на поштовање свог приватног и породичног живота, дома и преписке.

Члан 8.

1. Свако има право на заштиту података о својој личности.

2. Такви подаци морају бити обрађени поштено за (унапред) одређену сврху и на основу информисаног пристанка особе или на неком другом легитимном основу уређеном законом. Свако има право да приступи прикупљеним подацима о својој личности и има право да затражи њихову исправку.

3. Поступање по овим правилима је под контролом независног органа.

обрадом меша у право на приватност појединца загарантовано чл. 8. Европске конвенције. Штавише, представке које су се односиле на заштиту података о личности су биле подношене суду, али како Конвенција не садржи одредбе које се односе на њихову заштиту, Суд је у тим случајевима морао да пресуђује у оквиру чл. 8. Зато је Европски суд развио низ критеријума за одлучивање да ли се обрада података о личности може обухватити правом на приватност или не.

Европски суд прави разлику између ова два права користећи два критеријума: природу података који се обрађују и опсег обраде. Уколико су подаци суштински везани за приватност особе, онда ће њихова обрада пасти под заштиту чл. 8. Конвенције без даљег разматрања. Ипак, уколико подаци нису суштински приватни, суд ће посматрати опсег обраде, односно: да ли су подаци аутоматски складиштени; да ли се подаци складиште са фокусом на субјекта обраде, независно од тога да ли се то чини аутоматски или не; да ли је субјект обраде имао разумна очекивања да се подаци неће обрађивати. У великом броју случајева, Суд је пронашао да је обрада података о личности условила повреду права на приватност, зато што обрада вршена у мери у којој се вређало право на приватност,[17] али не у свим случајевима.[18]. Тиме је суд закључио да свака обрада података о личности не подразумева и повреду права на приватност, иако је покривена законском регулативом заштите података о личности.

Са једне стране, чини се да заштита података о личности спада у аспект приватности који је данас познат и усвојен, односно као контрола над подацима о личности. Међутим, оно што приватност штити се не може свести само на податке о личности. [19]

Са друге стране, нису сви подаци о личности (као информације које се односе на одређену или одредиву особу) обавезно „приватни“, односно не могу сви ти подаци утицати на приватну сферу индивидуе. Надаље, заштита података о личности се не односи само на приватност у оквиру технологија, јер она служи заштити и других

[17] Application no 27798/95*, Amann vs Switzerland,* para 65, Application no. 28341/95, *Rotaru vs Romania*, para 43; Application no 44787/98, *P.G. & J.H. vs U.K,* para 57.

[18] S. Gutwirth, Y. Poullet, P. De Hert, C. de Terwangne and S. Nouwt (eds.), *Reinventing data protection?*, Springer**,** Dordrecht, 2009, pp. 20-26.

[19] A. Rouvroy and Y. Poullet, The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy цитирано као у S. Gutwirth, Y. Poullet, P. De Hert, C. de Terwangne and S. Nouwt (eds.), Reinventing data protection?, Springer, Dordrecht, 2009, pp 70.

вредности и права поред приватности. Коначно, док је приватност право које има различито значење у различитим контекстима и јурисдикцијама, заштита података о личности са својим принципима фер обраде, има есенцијалну процедуралну природу која га чини објективнијим правом.[20]

Крајњи циљ заштите података о личности је да омогући "поштовање правила о обради података, и, до неке мере, и фер приступ у вези са исходом те обраде."[21] Принципи фер обраде имају циљ да достигну сет вредности и интереса као што су приватност, транспарентност у обради, загарантована права на заштиту тог права судским путем, квалитет и сигурност података, одговорност контролора података, недискриминацију и пропорционалност.[22]

Суштина је да је право на заштиту података о личности природно преклапа са осталим правима, јер уместо гарантовања суштинске слободе (као што је тајност кореспонденције, слобода говора, право на слободан избор религије), ово право је ограничено на процену до које границе у кршењу наших слобода се може ићи – у овом случају пракса која се састоји у обради података о личности. Оно се у многоме припаја осталим правима који такође гарантују неку суштинску слободу, а пружају и начине да се те слободе ограниче.

IV МЕЂУНАРОДНОПРАВНА РЕГУЛАТИВА ЗАШТИТЕ ПОДАТАКА О ЛИЧНОСТИ

1. Заштита података о личности у оквиру Уједињених нација

Уједињене нације право на заштиту података о личности развијају под окриљем Универзалне декларације и чл. 12 којим се штити право на приватност, и чл. 17 Међународног пакта о цивилним и политичким правима.

Иако у овим универзалним документима нема помена заштите података о личности, Комитет за људска права Уједињених нација је у Генералном коментару бр. 16 од 23.03.1988. године навео да чл. 17 Међународне повеље такође намеће правило

[20] M. Tzanou, Is data protection the same as privacy? An analysis of telecommunications' Metadata Retention Measures in: *Journal of Internet Law*, 2013, Vol. 17, 3, pp. 24.

[21] L. Bygrave, *Data Protection Law: Approaching Its Rationale, Logic, and Limits*, 2002, The Hague, pp. 168.

[22] M. Tzanou, Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right, in: *International Data Privacy Law,* pp. 88, 91.

да обрада података о личности у оквиру јавног и приватног сектора мора бити регулисана у складу са фундаменталним принципима заштите података о личности.[23]

Поред наведених правила која оквирно уређују приватност и промовишу право и на заштиту података о личности, Уједињене нације су 1990. године усвојиле и Смернице за регулисање компјутеризованих база података о личности[24].

Њима су успостављени Правични принципи у вези са обрадом података, и препоручено је усвајање националних смерница за заштиту приватности. Као и у осталим међународним документима, смернице успостављају могућност за ограничење ових принципа, уколико је циљ заштита људских права и основних слобода појединаца, или хуманитарна помоћ.

1.1. Специјални известилац о приватности у дигиталном добу

Проблему значајнијег бављења правом на приватност и заштитом података о личности, Уједињене нације приступају и кроз постављање специјалног известиоца за право на приватност у дигиталном добу. Иако је његова обавеза окренута посматрању целокупног концепта приватности, а не само података о личности, посебан значај постојању овог органа аутор рада даје услед чињенице да се приватност посматра са аспекта дигиталног доба и утицаја нових технологија на њу, те је у том смислу значајна и за тему која је у овом мастер раду обрађивана.

У јулу 2015, Савет за људска права поставио је Др Џозефа Канатација са Малте као првог специјалног известиоца за право на приватност, именованог на период од три године. Специјални известилац је мандат добио Резолуцијом 28/16 Савета за људска права[25], у оквиру ког је добио следећа овлашћења да:

а) прикупи релевантне информације, укључујући међународне и националне оквире, националне праксе и искуства, да проучава трендове, развој и изазове у вези са

[23] UN Human Rights Committee (HRC), CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988, преузето 18.08.2016. године са: http://www.refworld.org/docid/453883f922.html.

[24] Смернице за регулисање компјутеризованих података о личности, усвојене на 68. Седници Уједињених нација дана 14. Децембра 1990. Године, A/RES/45/95

[25] The right to privacy in the digital age, no. A/HRC/28/L.27, 26 March 2015

правом на приватност и да даје препоруке како би се осигурала њихова промоција и заштита, укључујући и изазове који произилазе из нових технологија;

б) тражи и прима информације, као и да даје одговоре на питања, избегавајући дуплирање, од држава, Уједињених нација и њених агенција, програма и фондова, регионалних механизама за заштиту људских права, националних институција за људска права, организација цивилног друштва, приватног сектора, укључујући предузећа, и било који други релевантне актере или стране;

в) идентификује могуће препреке за промоцију и заштиту права на приватност, да идентификује размењује и промовише принципе и најбољу праксу на националном, регионалном и међународном нивоу, као и да подноси предлоге и препоруке Савету за људска права у том смислу, укључујући и изазове који нарочито настају дигиталном добу;

г) учествује и доприноси релевантним међународним конференцијама и догађајима са циљем промовисања систематског и кохерентног приступа питањима која произлазе из његовог мандата;

д) подиже свест о важности промовисања и заштите права на приватност, укључујући и поглед на одређене изазове који су настали у дигиталном добу, као и значај пружања права на делотворан правни лек појединцима чије је право на приватност угрожено, у складу са међународним обавезама;

ђ) током рада мандата интегрише аспект равноправности полова;

е) извештава о наводним кршењима, где год да се десе, права на приватност, као што је наведено у члану 12 Универзалне декларације о људским правима и члану 17. Међународног пакта о грађанским и политичким правима, укључујући и она у вези са изазовима које произилазе из нових технологија, и да скрене пажњу Савету и Високом комесару Уједињених нација за људска права на ситуације које су од посебног значаја;

ж) подноси годишњи извештај Савету за људска права и Генералној скупштини, почевши од тридесет прве односно седамдесет прве седнице.

2. Заштита података о личности у комунитарном праву

Европска унија је једна од првих организација која је спровела свеобухватно регулисање заштите приватности и заштите података о личности. Повељом о основним правима у Европској унији (чланом 8) први пут је право на заштиту података о личности индивидуализовано загарантовано као основно људско право, што је допринело лакшем препознавању значаја података о личности у савременом свету. Ово право је детаљно регулисано и Директивом о заштити појединаца у вези са обрадом података о личности и слободном кретању таквих података, о којој је већ било речи у деловима II 1. и II 2. овог рада.

Регулативом (ЕЦ) бр. 45/2001 од 18. децембра 2000. године о заштити појединаца у погледу обраде података о личности од стране институција и тела Заједнице и о слободном току таквих података, ЕУ потврђује значај који даје заштити података о личности, те детаљно уређује начине обраде података о личности од стране ЕУ институција и тела. Њом је постављен Европски надзорник за заштиту података о личности, и установљена су правила која гарантују да ће подаци о личности које користе ЕУ институције и начела за њихову заштиту бити поштована, па се у том смислу и дефинишу права грађана ЕУ.

Европски надзорник врши свеобухватну контролу над применом Директиве, како од стране органа ЕУ, тако и од стране приватног сектора који рукује подацима. ЕУ посебно уређује и заштиту података о личности на интернету, а Суд правде овде игра активну улогу у тумачењу постојећих законских норми и на тај начин допуњује правне празнине које услед брзог развоја технологије право не успева да испрати. Ова околност је и најважнији разлог за реформу заштитите података о личности коју ЕУ спроводи, те ће се од 2018. године примењивати Регулатива за заштиту података о личности коју је Европска унија ове године усвојила.

2.1.Европски надзорник за заштиту података о личности

Европски надзорник за заштиту података о личности је независтан орган који се бави заштитом података о личности у Европској унији, установљен Регулативом бр.

45/2001[26]. Његова примарна улога је надгледање примене правила о заштити података о личности од стране институција и тела Европске уније и приватног сектора.

Регулативом бр. 45/2001 је одређено да свака европска институција и тело морају именовати барем једног повереника за заштиту података о личности са задатком да сарађује са Европским надзорником за заштиту података о личности, ради сигурности да права и слободе субјеката чији се подаци обрађују нису компромитовани.

Надзорник се стара о томе да су подаци о личности:

- обрађени на поштен и законит начин,

- за специфичне, експлицитне и легитимне сврхе и да не постоји даља повреда која је несагласна са тим сврхама,

- адекватно, релевантно и непрекомерно обрађивани,

- тачни и ажурни,

- држани у форми која не идентификује субјекта дуже него што је то потребно.[27]

Европски надзорник за заштиту података о личности има бројне задатке и овлашћења.

Европски надзорник пре свега саветује институције и органе Европске уније о свим питањима која се односе на обраду података о личности. Он прати релевантне промене које могу имати утицај на заштиту података о личности, поготово када се ради о развоју технологије и комуникација.

Када предлог закона може имати утицај на заштиту података о личности, Европска комисија мора да га поднесе Европском надзорнику ради консултација.[28] Надзорник анализира предлог узимајући у обзир основне елементе који утичу на заштиту података, питања као што су: који је обим и сврха предлога закона, да ли су

[26] Regulation (Ec) No 45/2001 of The European Parliament and of The Council of 18 December2000 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, *Official Journal of the European Communities*, no L 8/1

[27] *Ibid*, чл. 4.

[28] *Ibid,* чл. 28.

правни лекови за заштиту ефикасни и пропорционални, да ли закон подразумева обраду осетљивих података, колико дуго се подаци чувају, ко ће имати приступ подацима, да ли ће грађани бити обавештени о томе, и на који начин ће грађани Европске уније моћи да остваре своја права.

Велики број задатака прате и овлашћења које Надзорник има, као што су:

а) давање савета субјектима чији се подаци обрађују у остваривању њихових права,

б) обраћање руковаоцу података у случају наводног кршења одредби које регулишу обраду података о личности, и, где је то могуће, подношење предлога за отклањање тих повреда и унапређења заштите носиоца права;

в) налагање институцијама да поступе по захтеву грађана за заштиту података о личности;

г) упозоравање или укор руковаоца;

д) наређивање исправљања, блокирања, брисања или уништавања свих података када су обрађени уз кршење одредби које регулишу обраду података о личности или без обавештавања о таквим радњама трећих лица чији су подаци у питању;

ђ) изрицање привремене мере или дефинитивне забране обраде;

е) упућивање случаја одговарајућим институцијама Заједнице илиорганимаи, ако је потребно, Европском парламенту, Савету и Комисији;

ж) упућивање случаја Суду правде Европске уније под условима предвиђеним споразумима о оснивању ЕУ;

з) интервенисање у поступцима који се воде пред Судом правде Европске уније.[29]

Надзорник може још и:

а) добити од руковаоца или институције Заједнице или другог тела, приступ свим подацима о личности и свим информацијама потребним за своје упите;

б) добити приступ свим просторијама у којима руковалац или институција или тело Заједнице спроводи своје активности, када постоје оправдани разлози да верује да су те активности регулисане овом Регулативом.[30]

[29] Regulation (EC) No 45/2001 , *op.cit,* чл. 47.

Канцеларија Надзорника је 2015. године усвојила стратегију развоја за период 2015-2019. године, под називом „Поведи својим примером“.[31]

Циљ Надзорника је да помогне Европској унији да предводи примером у глобалном дијалогу о заштити права на приватност у дигиталном добу. У том циљу, Надзорник је утврдио три циља, која ће спровести кроз 10 акција, и то:

1. Заштита података постаје дигитална

1) Промовисање технологије за побољшање приватности и заштите података;

2) Идентификација интердисциплинарних решења;

3) Повећање транспарентности, корисничке контроле и одговорности у обради тзв. великих података (енг. Big data).

2. Напредовање у глобалним партнерствима

4) Развој етичке димензије заштите података;

5) Укључивање заштите података у редовне токове међународних политика;

6) Стварање јединственог ЕУ гласа у међународној арени.

3. Отварање новог поглавља за заштиту података о личности у ЕУ

7) Усвајање и спровођење актуелних правила о заштити података о личности;

8) Повећање одговорности тела ЕУ која прикупљају, користе и задржавају податке о личности;

9) Омогућавање одговорног и информисаног креирања политика;

10) Промовисање зрелог разговора о безбедности и приватности.[32]

На овај начин, Европска унија показује да има јасне циљеве у заштити података о личности, и да се њен најважнији орган тиме организовано и усмерено бави, те са правом очекује развој и напредак у наведеној области.

---

[30] Regulation (EC) No 45/2001, *op.cit,* чл. 47(2).

[31]The European Data Protection Supervisor, *Leading by example - The European data protection supervisor strategy 2015-2019*, Luxembourg, Publications Office of the European Union, 2015.

Преузето 05.09.2016.

https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Strategy/15-07-30_Strategy_2015_2019_Update_EN.pdf.

[32] *Ibid, с*трана 3.

Из изнете стратегије се може закључити да је потребна сарадња свих – од креатора политике, инжењера, преко привредника, државника и свих осталих грађана – да заједнички раде на задатку заштите података о личности. Једино се на тај начин може утицати на развој технологије и њену примену, али још битније је што хитније разматрање етике и очувања људског достојанства у технологији у будућности.

2.2.Директива о приватности и електронским комуникацијама

Европски парламент и Европски савет су дана 12.07.2002. године усвојили Директиву о обради података о личности и заштити приватности у подручју електронских комуникација (Директива о приватности и електронским комуникацијама). [33]

Циљ ове директиве је уређивање информација које се размењују кроз јавне електронске комуникационе услуге, као што су интернет и мобилна и фиксна телефонија, те преко њихових припадајућих мрежа. Те услуге и мреже захтевају посебна правила и заштитне механизме како би се осигурало право корисника на приватност и поверљивост.

Пружаоци електронских комуникационих услуга морају осигурати своје услуге тако да барем:

- осигурају да подацима о личности приступају само овлашћене особе;

- штите податке од уништења, губитка или случајне измене, те од осталих незаконитих или неовлашћених облика обраде;

- осигурају примену сигурносне политике о обради података о личности.

Државе Европске уније морају осигурати поверљивост комуникација објављених преко јавних мрежа. Посебно морају:

- забранити слушање, прислушкивање, задржавање или друге облике пресретања, односно надзора над комуникацијама и с тиме повезаним подацима о промету, без пристанка корисника, осим у случају када особа има законско допуштење да то учини и делује у складу с посебним захтевима;

[33] 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), *Official Journal of the European Communities* L 201, 31/07/2002 P. 0037 – 0047.

- јемчити да је чување информација о приступу информацијама сачуваним на посебној опреми корисника допуштена само ако је корисник јасно и потпуно обавештен, између осталог, о сврси, те ако му је било дато право да то одбије.

Када подаци о промету више нису потребни за комуникацију или наплаћивање услуге, морају се обрисати или учинити анонимним. Међутим, пружаоци услуга могу обрађивати те податке у сврхе маркетинга, све док корисници на које се подаци односе дају свој пристанак. Тај се пристанак може повући у сваком тренутку.

Пристанак корисника потребан је и у бројним другим ситуацијама, укључујући:

- пре него што им се могу послати нежељене комуникације (енг. spam). То се односи и на СМС и на остале електронске начине слања порука;

- пре него што се информације (колачићи – енг.cookies) сачувају на њихове рачунаре или уређаје, или пре него што се добије приступ тим информацијама, корисник мора добити јасне и потпуне информације, између осталог, о сврси чувања или приступа;

- пре објаве телефонских бројева, е-маил адреса или поштанских адреса у јавним телефонским именицима.

- државе Европске уније морају имати систем казни, укључујући правне санкције за кршење директиве.

Поред наведених ограничења, ЕУ прописује генералну могућност за дерогацију права, сличну оној која постоји међународним документима у вези са заштитом људских права. Опсег права и обвеза може се ограничити само националним законским мерама када су таква ограничења нужна и сразмерна за заштиту одређених јавних интереса, као што су спровођење кривичних истрага, или заштите националне сигурности, одбране или јавне сигурности.

Ова директива једна је од пет директива које заједно чине Пакет о телекомуникацијама, законодавни оквир којим се уређује сектор електронских комуникација. Остале директиве обухватају општи оквир, приступ и међусобно повезивање, овлашћење, лиценцирање и универзалну услугу.

Пакет је измењен и допуњен 2009. године двема директивама о бољем законодавству и правима грађана, као и уредбом о оснивању тела европских регулатора за електронске комуникације.

2.3. Пракса Суда правде Европске уније у вези са заштитом података о личности. Право на заборав – порекло, одлука Суда правде и развој

Дана 3. маја 2014. године, Суд правде Европске уније је донео одлуку у поступку који је покренуо шпански Народни виши суд (Audencia Nacional) ради доношења претходне одлуке о појединим питањима која се односе на примену Директиве. Поступак пред шпанским судом је започет 2010. године, када је Шпанац, господин Марио Костеја Гонзалез, поднео жалбу Шпанској агенцији за заштиту података о личности (Agencia Española de Protección de Datos) против, између осталог, Гугла Шпанија (Google Spain) и компаније Гугл са седиштем у Сједињеним Америчким Државама (Google Inc.) ради заштите права на приватност.[34]

Случај се тицао странице у интернет издању каталонске новине Ла Вангуардиа (La Vanguardia), до које претрага путем Гугла може одвести, а путем које се пружало обавештење о аукцији некретнина господина Гонзалеса ради наплате његових дугова за социјално осигурање.

Жалба је поднета јер је пружањем обавештења о аукцији његове куће на Гугл резултатима претраге повређено право на приватност господина Гонзалеса, будући да је поступак у вези са тим у потпуности решен пре више година, па је референца на те податке сасвим непотребна и ирелевантна. Он је затражио, прво, да новине уклоне или измене странице у питању, тако да његови лични подаци више не појављују, и друго, да Гугл Шпанија или Google Inc. уклоне личне податке који се односе на њега, тако да се исти више не појављују у резултатима претраге.

Шпанска агенција за заштиту података о личности је жалбу против новина одбила, будући да су исте имале легитиман разлог за објављивање тих информација, објављене су у оквиру налога Министарства и ради омогућавања што већег броја понуђача на аукцији. Ипак, Агенција је уважила жалбу у односу на Гугл Шпанија и Google Inc,и наложила им да онемогуће приступ до спорне странице у новинама Ла Вангуардија насталих Гугл претрагом имена господина Гонзалеса.

И један и други Гугл су поднели одвојене тужбе шпанском суду против оваквих одлука, када је суд застао са поступком и обратио се Суду правде Европске уније затраживши одговор на питања:

[34] Case C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González.*

а) да ли се Директива из '95 примењује на сервисе за претраживање података као што је Гугл;

б) да ли се европско право (Директива) примењује на Гугл Шпанија, будући да се компанијин сервер за обраду података налази у Америци;

в) да ли појединац има право да захтева да његови подаци о личности не буду доступни преко сервиса за претрагу (право на заборав).

У одговору на захтев за тумачење, Европски суд правде је заузео важна становишта у погледу Директиве, и појаснио конкретну примену Директиве на ову ситуацију.

- пре свега, сервиси за претрагу података врше обраду података о личности уређену чл. 2(б) Директиве, будући да њихове радње подразумевају прикупљање, бележење, организацију, складиштење, добијање натраг, обелодањивање, и чињење доступним података о личности, што све спада под дефиницију "обраде“ а чињеница што се ти подаци већ налазе на интернету нема утицаја на класификацију.

- друго, сервис за претрагу се сматра „руковаоцем“ обраде у смислу члана 2(д) Директиве, будући да сервиси за претрагу одређују сврху и средства за остваривање својих активности, а која је различита од оне коју имају власници интернет-страница, чак независно од тога што власници интернет страница користе „robot.txt“ фајлове, „nonindex“ или „nonarchive“ мета тагове да би садржај страница држали ван индекса које користи сервис за претрагу. И ово оставља последице на сервисе за претрагу, јер су руковаоци они који су одговорни за усаглашеност са већином захтева Директиве.

- треће, територијални досег Директиве је проширен у овом случају, па иако Гугл Шпанија, као привредно друштво које је основано и послује у Европској унији, није вршило обраду података о личности, већ је то чињено у седишту компаније у Калифорнији, суд је нашао да су активности Гугловог огранка у Шпанији неодвојиво повезане са активностима обраде будући да се иста обрада финансира новцем од рекламирања путем Гугла Шпанија. Суд је нашао да: „… података о личности за сврху сервиса за претрагу као што је Гугл, који функционишу са седиштем у трећој држави - али имају огранак у земљи Европске уније, "у контексту активности“ огранка, уколико огранак намерава да рекламира и прода простор за рекламу у Европској унији који је понуђен од стране сервиса за претрагу који чини услугу коју тај сервис чини доступном – профитабилном.“

- четврто, физичко лице на кога се податак односи има право да, у случајевима када су основи за легитимност обраде података базирани на члану 7(ф) директиве, да приговори таквој обради у било ком тренутку на бази необоривих легитимних основа који се односе на конкретну ситуацију обраде података који се односе на њега. Уколико је приговор лица оправдан, обрађивач података више не сме да укључи ове податке. [35] Уколико руковалац података не поступи у складу са захтевом лица, исто има право да поднесе жалбу телу које се бави заштитом података о личности или суду, ради прибављања налога којим се руковаоцу налаже чинидба. У оцени основа за обраду података о личности, право на заштиту података о личности лица надмашује економски интерес сервиса.

У погледу успостављања равнотеже између права на приступ информацијама интернет корисника и права физичких лица гарантованих директивом, то је потребно одредити од случаја до случаја, и зависиће од улоге коју физичко лице има у јавном животу.

Коначно, утицај питања на живот лица на ког се подаци односе, чињеница да су подаци објављени пре 16 година и недостатак преваге у интересу јавности за приступ овим подацима, захтевају да ти линкови буду уклоњени из резултата претраге.

Након ове одлуке, Гугл је створио онлајн форму коју субјекти чији се подаци обрађују могу да користе да би затражили уклањање линка или садржаја, уз идентификацију фотографијом. Линкови се уклањају у оквиру претрага које се врше из земаља Европске уније, Норвешке, Исланда, Швајцарске и Лихтенштајна, али је линк и даље доступан путем сајта ,,google.com“ и из било ког дела света. Такође, линкови ће бити уклањани из резултата претраге у којима се употребљава име конкретног физичког лица, док уклањање неће важити за остале резултате претраге којима се претражују друге теме.

Иако је ,право на заборав“ све време постојало у Директиви, овом пресудом је Суд правде први пут применио наведене одредбе, и притом појаснио важна питања у вези са територијалним аспектом Директиве и њеним дефиницијама. Појашњено је да су интернет сервиси за претрагу података одвојени руковаоци од власника интернет страница чији садржај индексирају. Оснивање компанија у ЕУ није нужно штит од примене комунитарног права, уколико је обрада података вршена у контексту

[35] Директива '95, *op.cit,* чл. 14.

активности огранка основаног у Европској унији, па се стога и право Европске уније у вези са обрадом података о личности мора поштовати.[36]

Будући да је пресуда донета у време велике реформе заштите података о личности и стварања нове Генералне регулативе за заштиту података о личности, право на заборав у будућој Регулативи заузима битно место, о чему ће бити више речи у наредном делу рада.

2.4. Трансфер података о личности из ЕУ у Сједињене Америчке Државе

У Европској унији послују бројне компаније чија се седишта налазе у Сједињеним Америчким Државама. Подаци које прикупљају европски огранци, од података о запосленима за потребе кадровских питања, до података које прикупљају интернет странице и мобилне апликације, се шаљу на обраду у САД. Зато је створена брига код грађана Европске уније о томе како ће се са подацима који се обрађују ван Европске уније поступати, као и да ли ће различито место прикупљања и обраде података о личности постати правна празнина која искључује примену детаљних правила за руковање која важе у Европској унији.

2.4.1. Принципи „Сигурне луке“ и „ЕУ-САД штит приватности“

До 2015. године више од 5000 америчких компанија са огранцима у Европи се ослањало на принципе „Сигурне луке“ – како су названа правила у вези са преносом података о личности из Европске уније у Сједињене Америчке Државе. Правила су настала Одлуком комисије 2000/520 од 26.07.2000. године о адекватности заштите коју принципи „сигурне луке“ пружају у погледу трансфера података из ЕУ у САД.[37]

Правила „Сигурне луке“ су подразумевали обавезивање америчких компанија које складиште или обрађују податке грађана ЕУ и Швајцарске да ће поштовати седам принципа (обавештавање, могућност избора, даљи пренос података, безбедност,

[36] B. Van Alsenoy and M. Koekkoek, *The extra-territorial reach of the EU's "right to be forgotten",* Working Paper No. 152 – March 2015, преузето 20.09.2016. године са https://ghum.kuleuven.be/ggs/publications/working_papers/new_series/wp151-160/wp152-alsenoy-koekkoek.pdf.

[37] Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, *Official Journal L 215* , 25/08/2000 P. 0007 – 0047.

интегритет података, приступ и извршење) приликом руковања тим подацима. Приступ овим правилима је био на добровољној бази, а америчке компаније би то чиниле путем сертификације код америчког Министарства трговине, чиме би се обавезале на поштовање принципа који испуњавају услове заштите података о личности који одговарају онима у ЕУ.

Ипак, одлуком Суда правде Европске уније од 06.10.2015. године[38], ови принципи су проглашени неважећим. До пресуде је дошло након што је Аустријанац, Максимилијан Шремс, поднео приговор код ирског повереника за заштиту података о личности, тврдећи да САД не пружају довољну заштиту против присмотре од стране америчке владе.

Господин Шремс је корисник друштвене мреже Фејсбук. Као што је случај и са осталим корисницима ове друштвене мреже који живе у ЕУ, неки од података су из огранка Фејсбука у Ирској слати на обраду у Сједињене Америчке Државе. У светлу Сноуденових открића из 2013. године, Шремс је тврдио да закони и пракса Сједињених Америчких Држава не нуде довољну заштиту података о личности од надзора који врше америчке власти. Ирски повереник је жалбу одбацио, са образложењем да се путем принципа „Сигурне луке“ обезбеђује довољан ниво заштите.

Након тога се случај нашао пред Вишим судом Ирске, који је испитивао да ли одлука Комисије о правилима „Сигурне луке“ спречава националне повереника за заштиту података о личности да поступају по жалбама грађана којима се тврди да трећа земља не осигурава адекватан ниво заштите и, по потреби, суспензију спорног преноса података.

Пресудом од 06.10.2015. године, Суд правде је заузео правни став да Комисија својом одлуком, сматрајући да трећа земља у коју су пренети подаци треба да обезбеђује адекватан ниво истих, не може да елиминише или пак смањи овлашћења којима је располагао национални повереник за заштиту података о личности базираних на Повељи о основним правима Европске уније и Директиви. Суд је тиме нагласио право на заштиту података о личности, гарантовано Повељом, и задатак који је националним органима који се баве заштитом тог права поверен Повељом.

[38] Case C-362/14 *Maximillian Schrems v Data Protection Commissioner joined party: Digital Rights Ireland Ltd.*

Суд истиче, пре свега, да ниједна одредба Директиве не спречава националне поверенике да надзиру трансфере личних података грађана трећим земљама, иако су ти трансфери претходно били предмет одлуке Комисије. Према томе, чак и ако је Комисија усвојила одлуку, национални надзорни органи морају бити у стању да одлуче о жалби грађана, и да испитају, потпуно независно, да ли је пренос података неке особе у трећу земљу у складу са Захтевима које прописује Директива.

Ипак, Суд истиче да он сам има надлежност да утврди да је акт ЕУ, као што су одлуке Комисије, неважећи. Сходно томе, где национални орган или лице које се том националном органу обратило, сматра да је одлука Комисије неважећа, тај орган или особа морају бити у стању да покрену поступак пред домаћим судовима како би они могли да, уколико сумњају у исправност одлуке Комисије, упуте предмет Суду правде ради добијања одговора. Стога је Суд правде тај који има задатак да одлучи да ли је Одлука Комисије је важећа или неважећа.

У вези са валидношћу принципа ,,Сигурне луке" суд је извео следећи закључак:

Суд наводи да је Комисија била у обавези да успостави такав режим са Сједињеним Америчким Државама, који, путем домаћег права или обавеза преузетих у оквиру међународне заједнице, омогућава ниво заштите људских права који је суштински истоветан оном који гарантују Директива и Повеља. Суд налази да Комисија није успела да омогући наведено, већ да је просто испитала шему правила ,,Сигурне луке".

Суд не улази у утврђивање чињенице да ли правила ,,Сигурне луке" омогућавају ниво заштите који је суштински истоветан оном који гарантује Европска унија, али суд запажа да су та правила примењива само на компаније у Сједињеним Америчким Државама које се са њима сагласе, али да америчке јавне власти не подлежу истим.

Осим тога, захтеви националне безбедности, јавног интереса и спровођење закона у Сједињеним Америчким Државама, преовлађују над правилима ,,Сигурне луке", тако да су компаније из САД-а дужне да, без ограничења, занемаре правила утврђена овом шемом, уколико су иста у супротности са горе наведеним захтевима и интересима САД-а. Тиме ова шема омогућава мешање јавних власти у Сједињеним државама у основна права појединаца. Штавише, одлука Комисије не садржи никакву могућност за ограничење било таквог мешања од стране америчких јавних власти, нити постојање ефективне правне заштите против таквог мешања.

Што се тиче нивоа заштите суштински еквивалентног основним правима и слободама загарантованим у Европској унији, Суд сматра да није могуће само на основу генералних правила омогућити складиштење свих података о личности свих лица чији подаци се преносе из ЕУ у САД без икакве разлике, ограничавања или изузетка које је направљен у светлу циља коме се тежи, и без објективног критеријума који се прописује за одређивање границе приступа јавних власти подацима и њихову каснију употребу. Суд сматра да се закон који омогућава приступ јавних власти садржају електронских комуникација на генералној основи, мора посматрати као суштинско угрожавање права на приватност.

Исто тако, Суд примећује да закон не предвиђа било какве могућности за појединца да искористи правне лекове како би имао приступ личним подацима који се односе на њега, или да му се омогући исправљање или брисање тих података, што доводи у питање суштину основног права на делотворну судску заштиту, и јер је постојање таквих могућности садржано у принципу владавине права.

Коначно, Суд сматра да правила „Сигурне луке“ негирају овлашћења националних органа за заштиту података о личности у ситуацијама када лице доведе у питање да ли је одлука у складу са заштитом приватности и основним правима и слободама појединаца. Суд сматра да Комисија није имала надлежност да ограничи овлашћења националних органа који се баве заштитом података о личности на тај начин. [39]

Услед свега наведеног, Суд је прогласио Одлуку „Сигурне луке“ неважећом. Ова пресуда има за последицу и налог ирском надзорном органу да са дужном пажњом размотри жалбу господина Шремса, и да, након спроведеног поступка, одлучи да ли, у складу са Директивом, пренос података европских корисника Фејсбука у Сједињене Америчке Државе треба да буде суспендован на основу тога да та држава не даје адекватан ниво заштите података о личности.

Пресуда Суда правде Европске уније којом су укинута правила „Сигурне луке“ изазвале су бурне реакције међу америчким компанијама, будући да велики број њих оснива огранке у земљама ЕУ, а обраду података врши у Америци. Покренуто је и

[39] Case C-362/14 Maximillian Schrems v Data Protection Commissioner joined party: Digital Rights Ireland Ltd, пара 56.

питање широког досега који Шремс пресуда може да има на будући правни поредак и праксе које уређују информациону приватност у САД-у и остатку света.[40]

Будући да су правила сигурне луке проглашена неважећим, Европска унија и Сједињене Америчке државе су дошле до новог решења, те је 12. јула 2016. године донета нова одлука којом се регулише трансфер података о личности, назван „ЕУ – САД штит приватности“[41]

Нова регулатива доноси нове обавезе за руковаоце подацима о личности, и има за циљ испуњавање обавеза које поставља ЕУ у руковању подацима. Што је најбитније, омогућава несметано функционисање компанија са седиштем у ЕУ које податке шаљу у Сједињене Америчке Државе на обраду, без опасности од ускраћивања пословања.

„ЕУ – САД штит приватности“ доноси следеће новине:

- строге обавезе према компанијама које рукују подацима: према новом споразуму, Министарство трговине Сједињених Америчких Држава ће вршити редовна ажурирања и преглед компанија које су се обавезале на примену споразума, да би осигурала да компаније пошују правила на која су се обавезале. Уколико компаније не поштују правила, суочавају се са санкцијама и бришу се са листе. Пооштравање услова за даљи трансфер података трећим земљама ће гарантовати исти ниво заштите у случају уколико трансфер врши компанија у оквиру "Штита приватности“:

- јасне гаранције и транспарентне обавезе у случају приступа подацима од стране америчке владе: Сједињене Америчке Државе су пружиле уверење Европској унији да ће приступ подацима о личности од стране јавних власти, а у циљу спровођења закона и националне безбедности, бити јасно ограничен и под механизмом надзора. Свако у Европској унији ће, по први пут, имати могућност преиспитивања и накнаде штете услед непоступања у складу са „Штитом приватности“. Сједињене Америчке Државе су искључиле масовни неселективни надзор података о личности. Директор Националне обавештајне службе је објаснио да ће до масивне обраде података доћи само уколико су испуњени специјални предуслови и биће што фокусираније и циљано усмерено. Државни секретар САД-а је успоставио могућност

[40] N. Ni Loidean The End of Safe Harbor: Implications for EU Digital Privacy and Data Protection Law, Journal of internet law, voume 19, no. 8, 2016, pp.11-12.

[41] Commission implementing decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, *Official Journal of the European Union* L 207/1.

за накнаду штете за Европљане чији се подаци о личности користе у раду обавештајних служби, и то путем механизма Омбудсмана у оквиру Министарстца спољних послова, тј. Државног секретаријата (Department of State).

- ефективна заштита индивидуалних права: грађанин који сматра да су његови подаци злоупотребљени у оквиру шеме „Штит приватности“ имаће неколико доступних и приступачних механизама за решавање спорова**.** У идеалној ситуацији, по жалби ће решити сама компанија, или ће потпуно бесплатно бити понуђене могућности за алтернативно решавање спорова. Појединац ће моћи да добије заштиту и директно код свог националног Повереника за заштиту података о личности, који ће се, у сарадњи са америчким Министарством трговине, постарати да су жалбе грађана Европске уније испитане и решене. Уколико случај не буде решен ниједном од набројаних мера, последња мера биће механизам арбитраже. Могућност накнаде штете у сфери употребе података од стране националних обавештајних служби, биће решен од стране Омбудсмана, независног од америчких јавних власти.

- годишњи заједнички преглед: постојаће посебан механизам праћења функционисања „Штита приватности“, укључујући обавезе и гаранције у вези са подацима који се користе у сврхе спровођења закона и заштите националне безбедности. Европска комисија и Министарство трговине САД-а ће спроводити праћење и удружити националне обавештајне експерте из САД-а и европске органе за заштиту података о личности. Комисија ће користити и све остале изворе информација, и саставити извештај за Европски парламент и Савет.

Одлука о усклађености у вези са принципима „Штита приватности" је донета 12. јула2016. године, а након што компаније буду ускладиле своје пословање са одлуком, моћи ће да се сертификују код Министарства трговине од 01. августа, од ког момента су се компаније обавезале да ће пословати у складу са новоусвојеним правилима.

2.5. Реформа заштите података о личности у ЕУ

Крајем 2015. године Европски парламент и Савет Европске уније постигли су споразум о реформи коју је предложила Комисија. Реформа је кључан корак за јачање основних права грађана у дигиталном добу и олакшавање пословања кроз поједностављење правила за компаније у јединственом дигиталном тржишту Европске уније.

Пакет реформи за заштиту података састоји се из Генералне регулативе за заштиту података о личности и Директиве о заштити података за полицијски и кривично-правни сектор.

Иако комунитарно право уређује заштиту података о личности још од 1995. године путем Директиве, разлике у начину на који свака држава чланица спроводи Директиву су довеле до недоследности које стварају комплексност, правну несигурност и административне трошкове. Ово утиче на поверење појединаца и конкурентност привреде ЕУ. Тренутна правила такође захтевају модернизацију, будући да су уведена у време када многе од данашњих интернет услуга и изазова који постоје за заштиту података још увек нису ни постојали. Преко друштвених мрежа, рачунарства преко облака, услуга базираних на локацијама и смарт картицама, обрада података о личности је експоненцијално порасла. Стога је Унија створила скуп правила како би право грађана на заштиту података о личности, загарантованих чланом 8. Повеље ЕУ о основним правима, остало делотворно и у дигиталном добу. Ово ће уједно бити корисно и за развој дигиталне економије.[42]

Регулатива ажурира и модернизује принципе садржане у Директиви из 1995. године која гарантује право на приватност. Она се фокусира на: јачање права појединаца, јачање унутрашњег тржишта ЕУ, обезбеђујући темељније поштовање и примену правила, поједностављење међународног трансфера података о личности и успостављање глобалних стандарда заштите података.

Промене ће дати грађанима већу контролу над својим личним подацима и лакши приступ. Оне су настале да би се осигурало да су подаци о личности грађана Европске уније заштићени - без обзира где су послати, прерађивани или складиштени - чак и изван ЕУ, што често може бити случај на интернету.

Реформа предвиђа алате за стицање контроле над подацима појединаца, а која се испоставила као једно од права око чије заштите Европљани имају бригу. Стога би реформа требало да поврати поверење грађана кроз:

• „Право на заборав": када појединац више не жели да се његови/њени подаци о личности складиште, и под условом да не постоје оправдани разлози за то задржавање,

[42] Појашњења Европске комисије у вези са реформом заштите података о личности – питања и одговори, 2015.
Преузето 15.08.2016. године са: http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm.

подаци ће бити избрисани. Ради се о заштити приватности појединаца, а не о брисању прошлих догађаја или ограничавању слободе штампе.

• Лакши приступ нечијим подацима: појединци ће имати више информација о томе како се обрађују њихови подаци и те информације треба да буду доступне на јасан и разумљив начин. Право на преносивост података ће олакшати појединцима пренос личних података између пружаоца услуга.

• Право појединца на сазнање када су његови подаци хаковани: компаније и организације морају да обавесте национални надзорни орган о незаконитом приступу који појединце ставља у ризик, као и да обавесте појединца чији су подаци у питању о свим приступима великих размера, тако да корисници могу предузети одговарајуће мере.

• Заштита података по дизајну (by design) и по стандарду (by default): "заштита података по дизајну" и "заштита података по стандарду" су сада битни елементи у правилима ЕУ о заштити података. Гаранције за заштиту података ће бити уграђене у производе и услуге у најранијој фази развоја, а стандардна подешавања која штите приватност ће бити норма - на пример, на друштвеним мрежама и у мобилним апликацијама.

• Правила ће бити примењивана строже: повереници за заштиту података ће моћи да казне компаније које не поступају у складу са правилима ЕУ износима до 4% од њиховог глобалног годишњег промета.

Дана 15. децембра 2015. године, Европски парламент, Савет и Комисија постигли су договор о новим правилима о заштити података о личности, успостављању модерног и усклађеног оквира за заштиту података широм Европске уније. Комитет Европског парламента за грађанске слободе и Комитет сталних представника Савета (COREPER) је одобрио споразум са веома великом већином. Споразуми су поздрављени од стране Европског савета 17-18. децембра као велики корак напред у реализацији дигиталне стратегије јединственог тржишта.

Дана 8. априла 2016. године Савет је усвојио Регулативу, а 14. априла 2016. године је усвојио и Европски парламент.

Дана 4. маја 2016. године, званични текст Регулативе је објављен у Службеном гласнику Европске уније на свим службеним језицима. Генерална регулатива за заштиту података о личности ступила је на снагу 24. маја 2016. године, примењиваће се

од 25. маја 2018. године[43], те компаније убрзано проучавају нова решења и усаглашавају пословање са наступајућим одредбама.

Будући да Србија, као земља кандидат за приступ Европској унији, има обавезу да у целости прихвати правне тековине Заједнице пре приступа истој, то је приказивање решења у ЕУ од великог значаја и за домаћи правни поредак. Кроз отварање поглавља ће и законодавство Европске уније у вези са заштитом података о личности бити уврштено у наше право, и биће спровођено од тренутка приступања, те је и из тог разлога аутор велики део рада посветио управо законодавству Европске уније.

3. Заштита података о личности у оквиру права Савета Европе

Заштита података о личности у оквиру Савета Европе се првенствено врши према одредбама Конвенције о заштити лица у односу на аутоматску обраду података о личности[44] и Конвенције о основним људским правима и слободама[45].

Конвенција о заштити лица у односу на аутоматску обраду података о личности је позната као први међународни документ који се експлицитно бави заштитом података о личности, и истовремено настоји да регулише прекогранични проток личних података. Такође, она је једини обавезујући документ у међународном праву који се бави заштитом података о личности. Сама Конвенција је усвојена 28. јануара 1981, а ступила је на снагу 1. октобра 1985. године, након пет потребних ратификација од стране држава чланица. Данас је Турска једина чланица Савета Европе која није ратификовала Конвенцију 108, а 2013. је и Уругвај ратификовао ову Конвенцију.

Поред пружања гаранција у вези са прикупљањем и обрадом података о личности, Конвенција 108 обезакоњује обраду "осетљивих" података о раси особе, политичкој припадности, здравственом стању, религији, сексуалном опредељењу,

[43]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), *Official Journal of the European Union* L 119/1.

[44]Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ETS No.108, *European Treaty Series - No. 108*.

[45]Европска конвенција за заштиту људских права и основних слобода, Рим, 4. новембар1950, CETS бр:005.

кривичним евиденцијама, итд, у одсуству правилне правне заштите. Конвенција такође гарантује право појединца да зна да се подаци о њему или њој чувају, и, ако је потребно, да те податке исправи.

Према Конвенцији о заштити лица у односу на аутоматску обраду података о личности, "подаци о личности" се дефинишу као свака информација која се односи на идентификованог појединца, или она на основу које се појединац може идентификовати.

Заштита и задржавање података о личности јасно потпада под обим приватног живота који је заштићен чланом 8 Конвенције о основним људским правима и слободама. Члан 8 обухвата широк спектар интересовања и штити приватан и породичан живот, дом и преписку. Овај став је Европски суд за људска права касније потврдио и кроз праксу, те у својим пресудама наводи да је заштита података о личности од кључне важности за комплетно уживање права на поштовање личног и породичног живота.[46]

Даље је Суд, у контексту права на заштиту података о личности, проналазио да се чланом 8 Конвенције штити легитимно право појединца да његови подаци о личности не буду објављени без његовог пристанка,[47] као што је на пример адреса пребивалишта.[48]

Објављивање информације о особи помињући пуно име и презиме те особе представља мешање у право на приватност[49]. Употреба само имена особе може такође представљати повреду, уколико је то име поменуто у контексту који чини једноставним идентификацију те особе, и када се употребљава у сврхе маркетинга[50].

Право на приватност у смислу права на заштиту података о личности, укључује и приватност комуникација, која подразумева сигурност и приватност поште, електронске поште, телефона, и осталих видова комуникације, укључујући и информатичку приватност као и информације које се налазе на интернету.[51]

---

[46] Application no. 30562/04 and 30566/04, *S. and Marper v. the United Kingdom*, para 41.

[47] Application no. 25576/04, *Flinkkilä and Others v. Finland*, para 75, Application no. 184/06, *Saaristo and Others v. Finland*, para, 12.

[48] Application no. 42811/06, *Alkaya v. Turkey.*

[49] Application no. 1593/06*, Kurier Zeitungsverlag und Druckerei GmbH v. Austria(no. 2).*

[50] Application no. no. 53495/09, *Bohlen v. Germany*, para 45.

[51] Application no. 62617/00, *Copland v. the United Kingdom*.

Под овај концепт спада и право на фотографију и контролу употребе те фотографије, и одбијања да се исте објаве[52]. Овај принцип је релевантан и за задржавање слика на социјалним мрежама, а од великог значаја је и за заштиту репутације и права других, јер слике могу садржати изузетно личне и чак приватне информације о појединцу и његовој породици. У случају да су слике направљене уз сагласност подносиоца представке, али не и уз сагласност за дељење истих са другима, суд је сматрао да је право на приватност превагнуло над правом на информисаност, будући да фотографије нису представљале најбитнији део новинског чланка.[53]

Чак и објављивање материјала насталог на јавним местима у ситуацијама које превазилазе нормално предвидљиве околности, могу такође да представљају повреду права на приватност. Тако је Суд пронашао да је чињење доступним медијима видео снимка подносиоца представке насталог на јавном месту није био предвидљиво и представљало је повреду очекиваног права на приватност.[54]

Када је у питању задржавање података о личности, Суд је у неколико предмета дефинисао обавезе државе да усвоји мере које ће осигурати поштовање права на приватност чак и када се ради о односу између два физичка лица или појединаца у чијем односу држава нема утицаја. То се, на пример, односи на однос корисника интернета и оног ко омогућава приступ одређеној интернет презентацији. У том смислу постоји позитивна обавеза државе да омогући ефективну заштиту против тешких злоупотреба нечијих података о личности, некада чак прописивањем ефикасне кривичноправне мере.[55]

Када је у питању интернет, обавеза државе се огледа у позитивној обавези да омогући приговор или правни лек[56]. Чак и када податке о личности задржава држава, уколико се исто чини у интересу националне безбедности или неког другог легитимног циља прописаног ст.2.чл.8 Конвенције[57], држава има обавезу да обезбеди адекватне и

[52] Application no. 40660/08 and 60641/08, *Von Hannover v. Germany (no. 2)*, para. 96.

[53] Application no. 59631/09, *The Verlagsgruppe News GmbH and Bobi v. Austria.*

[54] Application no. 44647/98, *Peck v. the United Kingdom*, para 60-63.

[55] Application Series A no. 91, *X and Y v. the Netherlands*, para 23-24, 27; Application no. 36505/02, *August v. the United Kingdom*; Application no. 39272/98, *M.C. v. Bulgaria*, para. 150.

[56]Application no. 2872/02, *K.U. v. Finland*, para 43.

[57] Чл. 8.ст.2 Конвенције за заштиту људских права и основних слобода, *op.cit.*

Јавне власти неће се мешати у вршење овог права сем ако то није у складу са законом и неопходно у демократском друштву у интересу националне безбедности, јавне безбедности или економске добробити земље, ради спречавања нереда или криминала, заштите здравља или морала, или ради заштите права и слобода других.

ефективне гаранције против сопствене злоупотребе. Уколико такве гаранције постоје, суд у већини случајева неће наћи повреду права на приватност, јер су телекомуникациони подаци о личности у широкој употреби од стране државних власти за потребе надзора, јер исти подаци могу бити чувани и приступати им се без скоро икаквог трошка.[58]

Чак и случајевима када податке задржава држава, закон којим се то дозвољава мора објаснити довољно јасно, и успоставити оквир и услове под којим ће држава користити то своје право.

Стога је заштита коју суд пружа широка, и редовно се подводи под чл. 8 Конвенције, будући да суд у оквиру тренутно постављених људских права нема другу могућност да заштити право на заштиту података о личности. Ипак, и сам суд је развио одређене критеријуме за прављење разлике између тога када је повређена приватност а када право на заштиту података о личности, што је подробније објашњено у делу 2.2. овог рада.

4. Обрада података о личности од стране интернет претраживача - Гуглова политика заштите приватности

Гугл је данас најпосећенији сајт и најпопуларнији интернет сервис, са око милијарду и шестстотина милиона претрага месечно, што представља око 70% укупних претрага[59]. Распрострањеност коју Гуглове услуге заузимају на интернету створила је од Гугла руковаоца огромним бројем података о личности.

Зато је његова улога у свету заштите података о личности врло битна, па је тако и под будним оком повереника за заштиту података о личности, а са Гуглом и одлуком Суда правде ЕУ је кренула и нова ера брисања података које Гугл претрага чини доступним остатку света.

Гугл има тежак задатак успостављања равнотеже између сопствених комерцијалних интереса за прикупљање и обраду података о личности, и интереса заштите истих које намећу, како Европска унија, тако и остале државе света. У својим

[58] Application no. 35623/05, Uzun v. Germany, para 69.

[59] Извор: http://www.ecloudbuzz.com/top-10-best-search-engines-in-the-world/ , https://searchenginewatch.com/2016/08/08/what-are-the-top-10-most-popular-search-engines/

„правилима о приватности“[60] детаљно је описано које податке Гугл прикупља и зашто, начин на који употребљава те податке, и опције које су пружене корисницима ради приступа и ажурирања тих података.

Иако однос између Гугла и корисника његових услуга представља приватноправни однос, те је саглашавање корисника са Правилима о приватности израз слободне воље, на иста је и јавно право извршило велики утицај. Досадашњи ток рада указује управо на велику уплетеност јавног права у овај приватноправни однос, будући да је он увелико регулисан правилима јавног права којима се руковаоцима података намећу обавезе у односу на поштовање права грађана. Тако и ова правила са једне стране омогућавају пружање услуга, а са друге стране осигуравају права и слободе грађана.

Додатно, имајући у виду убрзани развој технологија и њихову широку употребу, основни принципи заштите података о личности су већ заузели своје место у међународном јавном поретку, па исте у своје пословање и однос са становништвом уносе и компаније које тим подацима рукују.

На почетку је важно знати да се целокупно прикупљање, задржавање, обрада и остали начини коришћења наших података, заснивају на нашем пристанку. Приликом отварања Гугл налога, вршења претраге, коришћења било које услуге, ми се саглашавамо са употребом тих података од стране Гугла.

4.1.Информације које Гугл сакупља

1. информације које сами дајемо – креирањем Гугл налога, корисници се саглашавају да Гугл може користити њихове податке о личности, као што су име, е-маил адреса, број телефона или број кредитне картице. Уколико корисник креира и Гугл профил, дозвола се шири и на име и фотографију које у те сврхе користимо.

2. информације које пружамо приликом коришћења Гуглових услуга

Гугл прикупља податке о томе које услуге користимо, и на који начин – приликом гледања видеа на „You tube“-у, посећивања интернет презентације која користи Гуглове услуге оглашавања, прегледа и интеракције са огласима и садржајима. Те информације укључују:

[60] Доступно на: https://www.google.com/policies/privacy/, датум приступа: септембар 2016.

Информације о уређају са ког се врши приступ – модела хардвера, верзије оперативног система, јединствене идентификаторе конкретног мобилног уређаја, информације о мобилној мрежи као и број телефона. Гугл може да повеже идентификаторе уређаја или број телефона са Гугл налогом.

Лог информације – Гугл аутоматски прикупља и складишти одређене информације који се налазе у евиденцији сервера. Ово укључује: детаље о томе како користимо Гуглове услуге, као што су упити претраге, лог информације настале телефонирањем – корисников број телефона, број телефона саговорника, време и датум позива, трајање позива, усмеравање СМС-ова и врсте позива.

Адресе интернет протокола – информације о догађајима на уређају, као што су отказивања, активности система, поставке хардвера, тип прегледача, језик, датум и време захтева и упућивање УРЛ, колачићи који могу јединствено да идентификују интернет прегледач или Гугл налог.

Информације о локацији – Гугл прикупља и обрађује податке о стварној локацији користећи разне технологије за одређивање локације, укључујући ИП адресу, ГПС и друге сензоре који могу, на пример, обезбедити Гуглу информације о оближњим уређајима, приступним тачкама бежичног интернета и базних станица.

Јединствени бројеви апликација - овај број и подаци о инсталацији (на пример, тип оперативног система и број верзије апликације) могу бити послати Гуглу приликом инсталирања или деинсталирања услуга, или када та услуга повремено контактира Гуглове сервере, нпр. ради аутоматског ажурирања.

Локално складиштење – Гугл прикупља и складишти локалне информације на уређају (укључујући и податке о личности) помоћу механизама као што су складиштење података интернет читача (укључујући ХТМЛ 5) и скровишта апликација података.

Колачићи[61] и сличне технологије - коришћење колачића или сличних технологија и циљу идентификације прегледача или уређаја. Информације се

[61] Интернет колачићи (или само колачићи) представљају малу количину података које интернет странице шаљу својим посетиоцима на чување. Чување ових података на корисничкој страни обавља интернет прегледач.Сваки интернет корисник може чувати више колачића са одговарајућих интернет страница које је претходно посећивао. Колачић садржи податке о активностима корисника на основу којих

прикупљају и складиште и у току интеракције са рекламама или другим облицима Гуглових услуга које се могу појавити на другим сајтовима. ***Гугл аналитика*** помаже предузећима и власницима сајтова да анализирају саобраћај на њиховим сајтовима и апликацијама. Када се користи у комбинацији са Гугловим услугама оглашавања, као што су они користећи double click[62] колачић, Гугл аналитика је повезана са информацијама о посетама већем броју интернет презентација.

4.2. Како се користе прикупљене информације

Гугл користи информације које прикупља из употребе својих сервиса у циљу обезбеђивања, одржавања, заштите и унапређења истих услуга, или ради развоја нових. Исти се употребљавају ради представљања садржаја по мери - релевантнијих резултата претраге и огласа. Гугл користи информације ради повезивања налога на различитим Гугл услугама, ажурирања истих и Г+ налога – показивање имена, јавног профила, коментара и осталих информација које су јавно доступне на нашем профилу.

Уколико корисник контактира Гугл услед неког проблема, Гугл води евиденцију о комуникацији да би помогао у решавању будућих проблема са којима се корисник можда сусреће. Гугл може користити адресу електронске поште да би

интернет страница поспешује своје корисничко искуство, а самим тим и своју употребљиву вредност. На пример, Гугл као интернет претраживач користи колачиће како би пратио колико резултата претраживања корисник жели да види на једној страници. На пример, интернет страница Амазон користи колачиће да чува податке о томе које производе корисници стављају у ,,корпу" пре него што их купе. Коначно, једна од најбитнијих употреба је провера идентитета корисника. Интернер странице које захтевају од својих корисника да се пријаве путем корисничког имена и лозинке, могу након успешне пријаве да пошаљу колачић који садржи јединствену информацију која га може идентификовати. Приликом следећег приступа сајту, корисников интернет прегледач може директно послати интернет страници ову информацију, без потребе да се корисник опет пријављује. Механизам колачића за проверу идентитета и праћење активности корисника се може злоупотребити, па се регулисање ове области ефикасним законским решењима сматра једним од битних циљева информационе приватности.

[62] Већина колачића садрже такозвани јединствени идентификатор који се зове ИД колачића - то је низ знакова који интернет странице користе да препознају интернет прегледач на коме се налази колачић. Ово омогућава интернет страницама да прилагоде садржај странице конкретном претраживачу. Компанија ДаблКлик (DoubleClick) користи колачиће у циљу побољшања оглашавања. Уобичајене примене су циљно оглашавање на основу онога што је релевантно за корисника, ради побољшања перформанси рекламне кампање и избегавање приказивање огласа које корисник већ видео. Идентификатор колачића у сваком DoubleClick колачићу је од суштинског значаја за ову примену. На пример, идентификатор колачића се користи да би се водила евиденција о томе који се огласи приказују на којем интернет прегледачу. Тако ДаблКлик избегава приказивање огласа које је корисник већ видео. Слично, идентификатор колачића омогућава да се прате тзв. конверзије, односно ситуације када корисник посети оглас па касније користећи исти прегледач посети интернет страницу оглашавача и евентуално обави куповину. Оваква примена праћења, иако није персонализована (оглашавач једино може да разликује интернет прегледаче, али не и кориснике) ипак изазива проблеме када је у питању приватност података.

обавестио корисника о својим услугама, ради упознавања корисника са предстојећим променама или побољшањима.

Путем кеша[63], Гугл чува наше преференције, као на пример у погледу језика, што омогућава пружање релевантних услуга (реклама). Осетљиве категорије података о личности као што су раса, вера, сексуална оријентација или здравље, Гугл не користи ради прилагођавања услуга.

Гуглови аутоматизовани системи анализирају садржај (укључујући е-маилове) како би обезбедили лично релевантне карактеристике производа, као што су прилагођени резултати претраге, прилагођено оглашавање и детекција спам и малициозних софтвера. У зависности од подешавања налога, активност корисника на другим сајтовима и апликацијама може бити повезана са подацима о личности у побољшању пружања Гугл услуга и огласа.

Гугл мора тражити пристанак корисника пре употребе информација за неке друге сврхе осим оних које су наведене у Политици приватности.

Гугл обрађује личне податке на серверима у многим земљама широм света, па су кроз Политику приватности корисници обавештени да подаци о личности корисника могу бити обрађени и на серверу који се налази изван земље у којој корисник живи. Ово је битно из разлога што се сви подаци обрађују у Америци која има другачија правила за обраду података, што, као што се из одлуке Суда правде Европске уније види, може довести до слабије заштите у односу на заштиту коју корисник у земљи у којој користи услуге има.

[63] Веб-кеш меморија (или само веб-кеш) је механизам привременог складиштења поадтака интернет страница, како би се смањило коришћење преноса података преко интернета, оптерећење сервера као и кашњење приликом отварања интернет страница опажено из угла корисника. Идеја да се складиште копије података којима се често приступа, тако да се наредни приступи могу остваривати много брже, директно из веб-кеш меморије. Постоје две врсте веб-кеш меморије: 1) прокси (proxy) веб-кеш меморија која се налази са посебном серверу, коме типично корисник има бежи приступ, него оригиналном серверу интернет странице; 2) веб-кеш интернет прегледача који се налази ан корисничком рачунару. Пример прокси веб-кеша је кеш линк у Гугловим резултатима претраге, који пружа бржи начин прикупљања података од самог клика на директни линк, јер Гуглов прокси механизам функционише тако да корисник увек приступа серверу са најбржим приступом. Такође, чињеница да су веб-кеш подаци копије оригиналног садржаја интернет страница је очигледно када преко Гугловог веб-кеша можемо приступити интернет страницама које су давно угашене. Веб-кеш интернет прегледач се обично користи да чува садржај који се ретко мења (попут заглавља или менија интернет страница), па није оптимално преносити их преко интернета при сваком приступу. Иако је веб-кеш мотивисан техничким проблемима ограниченог интернет протока, постоји низ правних питаеа које оно отвара, укључујући ауторска праа на кеширани садржај.

Транспарентност и избор

Гуглова правила о приватности се заснивају на транспарентности и избору, и циљ њиховог постојања је пружање јасне информације о томе које податке Гугл прикупља како би корисник могао да направи избор о томе које услуге жели да користи.

Тако Гугл корисник може да прегледа и ажурира активност на Гугловим сервисима и да контролише и одлучи које врсте података, као што су видео снимци или прошле претраге, жели да сачува уз сопствени налог. Корисник може контролисати да ли се његова активност задржава у "колачићима“ или сличним техонологијама, а може се и одјавити са налога. Корисник може вршити преглед и контролу одређених врста информација повезаних са Гугл налогом помоћу Гугл контролне табле. Постоји могућности измене подешавања за Гугл огласе, ради приказивања релевантнијег садржаја или престанка са оглашавањем одређених призвода.

Корисник може подесити прегледач да блокира све колачиће, укључујући и колачиће у вези са Гугловим услугама. Ипак, иако оваква могућност постоји, многе услуге како Гугла, тако и осталих интернет презентација, неће правилно фукционисати уколико су "колачићи“ искључени, а неки чак условљавају да се ова могућност експлицитно дозволи ради уласка на одређени сајт.

Приступ и ажурирање личних информација[64]

Гугл омогућава приступ личним подацима, и уколико је тај податак погрешан, Гугл пружа начине за ажурирање и брзо брисање података – уколико исте Гугл не мора да држи зарад легитимних пословних или правних разлога. Пре извршене промене, Гугл може затражити проверу идентитета подносиоца захтева.

Захтев може бити одбијен уколико се нерационално понавља без ваљаних разлога, захтева несразмерни технички напор (на пример, развој новог система или из корена мењање постојеће праксе), ризикује приватност других, или уколико би за Гугл било врло непрактично да изврши промену (на пример, захтеви везани за информације које бораве на резервним системима за подршку).

Информација које Гугл дели

[64] Изворни текст на енглеском гласи „ Accessing and updating your personal information“. Гугл не прави јасну разлику, већ употребљава различите изразе – подаци о личности, личне информације..., те различитом терминологијом може унети забуну у тачно значење правила.

Гугл не дели податке о личности корисника са компанијама, организацијама и појединцима ван Гугла, осим у следећим околностима:

Уз пристанак корисника

Гугл ће делити податке о личности са компанијама, организацијама или појединцима изван Гугла када постоји пристанак корисника за тако нешто. Посебна сагласност се мора дати за дељење било ког осетљивог податка о личности.

Са администраторима домена

Уколико Гугл налогом корисника управља његов администратор домена (на пример, за кориснике Гугл апликација), онда ће тај домен администратор и дистрибутери који пружају корисничку подршку организацији корисника, моћи да имају приступ корисниковом Гугл налогу (укључујући е-пошту и друге податке). Администратор домена може бити у стању да:

- види статистику која се тиче корисниковог рачуна, као и статистике у вези са апликацијама које корисник инсталира,

- промени лозинку за корисников налог,

- онемогући или прекине приступ налогу,

- приступи или задржи податке који се налазе у оквиру корисниковог налога,

- преузме податке о налогу у циљу задовољења важећих закона, прописа, правних процеса или захтева извршне власти,

- ограничити могућност кориснику да избрише или измени информације или подешавања приватности.

За спољну обраду

Гугл пружа податке о личности својим партнерима или другим предузећима од поверења или особама који обрађују податке за Гугл, на основу Гугловог упутства и у складу са Гугловом политиком приватности и било које друге одговарајуће мере поверљивости и сигурности.

Из правних разлога

Уколико је то неопходно ради испуњавања законских обавеза, прописа, правних прописа или правноснажног захтева државе, Гул ће податке о личности корисника

поделити и са компанијама, организацијама или појединцима ван Гугла; ради спровођења услова коришћења, укључујући истрагу о потенцијалним повредама; ради откривања, спречавања или реаговања на други начин на преваре, безбедност или техничка питања; ради заштите права, власништва или сигурност Гугла, његових корисника или јавности, а на начин који је дозвољено и у складу са законом.

Гугл предвиђа да податке које не идентификују директно или индиректно корисника може делити са својим партнерима - издавачима, оглашивачима или повезаним сајтовима. Као пример, Гугл наводи дељење информација којима показује трендове у општој употреби наших услуга.

Наведеном политиком Гугл испуњава своју обавезу обавештавања корисника о начину и обиму коришћења података о личности, са којом се корисници пре коришћења услуга морају сагласити. Поред обавештавања, кроз политику се објашњавају и разлози коришћења података о личности, којима Гугл жели да испуни обавезу сразмерности и оправданости коришћења података.

Гугл поступа по захтевима корисника за брисање података које контролише, а чији број се, након одлуке Суда правде у случају Гонзалес многоструко увећао. Док се са једне стране ово сматра победом права на приватност и заштиту података о личности, из Гугла и других организација се чује о негативним аспектима пресуде, из разлога угрожавања права јавности да зна, те се стога се сматра да ће ова одлука бити коришћена противно сврси којој је успостављена.

V ЗАШТИТА ПОДАТАКА О ЛИЧНОСТИ У ПРАВНОМ СИСТЕМУ РЕПУБЛИКЕ СРБИЈЕ

1. Уставноправна заштита података о личности у Србији

Устав Републике Србије препознаје заштиту података о личности као самостално право. Чланом 42. Устава зајемчена је заштита података о личности, па Устав одређује да се прикупљање, држање, обрада и коришћење података о личности уређују законом, да је забрањена је и кажњива употреба података о личности изван сврхе за коју су прикупљени, у складу са законом, осим за потребе вођења кривичног поступка или заштите безбедности Републике Србије, на начин предвиђен законом, као

и да свако има право да буде обавештен о прикупљеним подацима о својој личности, у складу са законом, и право на судску заштиту због њихове злоупотребе.[65]

Уставни суд још увек није развио праксу у вези са повредом права на заштиту података о личности. Ипак, Уставни суд је допринос дао кроз оцену уставности закона који имају везе са заштитом података о личности.[66]

2. Управноправна заштита података о личности у Србији

Заштита приватности, а са њом и право на заштиту података о личности, још увек представља релативно нов концепт у Србији. Иако је право на заштиту података о личности једно од основних људских права загарантованих Уставом, основни правни оквир у Републици Србији установљен је тек октобра 2008. године, усвајањем Закона о заштити података о личности (у даљем тексту ЗЗЛП, Закон)[67]. Поред овог, донети су и подзаконски акти, и то Уредба о обрасцу за вођење евиденције и начину вођења евиденције о обради података о личности ("Сл. гласник РС", бр. 50/2009), Правилник о начину претходне провере радњи обраде података о личности ("Сл. гласник РС", бр. 35/2009), Правилник о обрасцу легитимације овлашћеног лица за вршење надзора по Закону о заштити података о личности ("Сл. гласник РС", бр. 35/2009).

Заштита података о личности се примарно остварује кроз контролу Повереника за заштиту података о личности над спровођењем Закона. Сам грађанин може руковаоцу захтева поднети захтев за брисање, исправку, приступ својим подацима о личности, или на други начин искористити права загарантована Законом, уколико за то постоји законски основ. Ако руковалац неосновано не поступи по захтеву, процедура се наставља кроз управни поступак у ком Повереник има главну улогу, будући да се

[65] Чл. 42 Устава Републике Србије, *Службени гласник РС* бр. 98/2006.

[66] Уставност законске обавезе обавештавања Републичког фонда за здравствено осигурање о подацима који се односе на здравствено стање пацијента - Одлука Уставног суда, I Уз број 421/2013 од 5. јуна 2014. године, објављена у "*Сл. гласнику РС"*, бр. 73/2014 од 16. јула 2014. године; Неуставност одредаба Закона о безбедносно-информативној агенцији којима се ограничава начело неповредивости тајности писама и других средстава општења - Одлука Уставног суда, IУз број 252/2002 од 26. децембра 2013. године, објављена у "*Сл. гласнику РС*", бр. 65/2014 од 27. јуна 2014. године; Непостојање уставног основа да се прикупљање, држање, обрада и коришћење података о личности уређује актом ниже правне снаге од закона - Одлука Уставног суда, I Уз број 41/2010 од 30. маја 2012. године, објављена у "*Сл. гласнику РС",* бр. 68/2012 од 18. јула 2012. године

[67] Закон о заштити података о личности, *Службени гласник РС* бр. 97/2008, 104/2009 - др. закон, 68/2012 - одлука УС и 107/2012.

јавља у улози другостепеног органа који решава по жалби грађанина, а касније и надзирањем да руковалац поступи по одлуци Повереника.

2.1. Закон о заштити података о личности у Србији

Истини за вољу, у Србији је и раније постојао закон под истим именом. Још 1998. године, у време постојања Савезне Републике Југославије, донет је Закон о заштити података о личности[68], који је касније остао део правног система Републике Србије. Настао је ради испуњења обавеза које је Србија имала као потписница Конвенције Савета Европе бр. 108 о заштити лица у односу на аутоматску обраду личних података из 1981. године[69]. Нажалост, овај закон се у Србији мало примењивао.

Доношењем новог Закона 2008. године, законодавац је настојао да постави свеобухватнија правила, да одговори на бројна отворена питања у вези са заштитом података о личности, али и да усклади домаће стандарде са онима постављеним у Директиви ЕУ о заштити података о личности.

ЗЗПЛ не покрива комплетан спектар права на приватност појединца, већ само онај део који се односи на његове податке о личности. Тако Закон уређује услове за прикупљање и обраду података о личности, права лица и заштиту права лица чији се подаци прикупљају и обрађују, ограничења заштите података о личности, поступак пред надлежним органом за заштиту података о личности, обезбеђење података, евиденције, изношење података из Републике Србије и надзор над извршавањем ових норми. У члану 2 Закона стоји да је циљ, у вези са обрадом заштите података о личности, да се сваком лицу обезбеди остваривање и заштита права на приватност и осталих права и слобода, те главни субјект заштите нису сами подаци о личности, већ појединци на које се ти подаци односе.

2.1.1. Шта су то подаци о личности

Податак о личности је, према чл.3. ст.1. Закона, свака информација која се односи на физичко лице, без обзира на облик у ком је изражена и на носач информације (папир, трака, филм, електронски медијум и сл.), без обзира на околности чувања информација, без обзира на начин прибављања информације (слушањем,

[68] Закон о заштити података о личности, *Службени лист СРЈ бр.* 24/98.

[69] Потврђена усвајањен Закона о потврђивању Конвенције у односу на аутоматску обраду личних података, *Службени лист СРЈ* бр. 1/92.

гледањем, путем увида у документ и сл.) и без обзира на друга својства те информације.

Физичко лице је, према чл.3. ст.1 Закона, човек на кога се односи податак, чији је идентитет одређен или одредив на основу личног имена, јединственог матичног броја грађана, адресног кода или другог обележја његовог физичког, психолошког, духовног, економског, културног или друштвеног идентитета. Физичко лице је овим путем одређено, односно одредиво, уз помоћ његових идентификационих бројева као што су већ поменути јединствени матични број грађана, такође и порески број, број здравственог осигурања, број телефона, број личне карте или пасоша или пак број студентског индекса.

Одредбом "или другог обележја“ законодавац оставља могућност да и неки подаци који нису примарно набројани у Закону, добију квалитет података о личности.

Такође, наш Закон поред података које воде директној идентификацији, у податке о личности сврстава и податке на основу којих се посредно може доћи до идентитета лица. Оваква формулација води бољој заштити појединаца, јер постоји реална могућност да се одређивање лица изврши повезивањем и комбинацијом података који га наизглед не идентификују. Тиме је наш законодавац учинио усаглашавање са Директивом ЕУ, која на сличан начин одређује појам података о личности (одредба члана 2).

Други фактори помоћу којих физичко лице може бити одређено или одредиво, између осталог, су: старост, запослење, друге функције које лице обавља, положај и статус у одређеном субјекту и сл. Такође, податке представљају и слика, глас, отисци прстију, те све друге биометријске карактеристике физичког лица. Биометријске карактеристике су телесне, физиолошке, и карактеристике понашања, које поседују сви појединци, које су јединствене и сталне за сваког појединца посебно и уз чију помоћ га је могуће идентификовати, нарочито у случају употребе отисака прстију, дужица ока, мрежњаче ока, образа, ушију, дезоксирибонуклеинске киселине (ДНК), као и различитости положаја.

Податак о личности је зато сваки податак који се односи на физичко лице ако је оно одређено или одредиво. Подаци, који су непрепознатљиви, изманипулисани или на неки други начин измењени, нису подаци о личности уколико на основу њих није могуће одредити особу на коју се односе.

Међутим, подаци о стварима, животињама и о правним лицима не спадају под заштиту коју пружа овај Закон. Мало је сложенија ситуација у случају самосталних предузетника и треба скренути пажњу да у случају када појединац наступа као предузетник (приватни предузетник), ради заштите правног промета, право на заштиту података о личности је сужено и појединац у својству предузетника не може уживати толико права као појединац у својству физичког лица. Дакле, у ситуацијама где се подаци односе на предузетника, не може се говорити о заштићеним подацима о личности када се ради о подацима појединца повезаним са обављањем функције самосталног предузетника. Порески број или на пример број текућег рачуна самосталног предузетника су у непосредној вези са обављањем његове делатности, те стога у том случају не представљају заштићене податке, док би за исти порески број односно исти текући рачун то били заштићени подаци у случају када их користи појединац као физичко лице.[70]

Намера законодавца није била надзирање и регулисање апсолутно сваке обраде података о личности, те су у члану 5. ЗЗПЛ прецизирани изузеци од примене закона, и то:

1) Подаци који су доступни свакоме и објављени су у јавним гласилима и публикацијама или приступачни у архивама, музејима и другим сличним организацијама,
2) Подаци који се обрађују за породичне и друге личне потребе и нису доступни трећим лицима,
3) Подаци који се о члановима различитих политичких странака, удружења, синдиката, као и других облика удруживања, обрађују од стране тих организација, под условом да члан да писмену изјаву да одређене одредбе овог закона не важе за обраду података о њему за одређено време, али не дуже од времена трајања његовог чланства,
4) Подаци које је лице, способно да се стара о својим интересима, објавило о себи.

[70] Н. Пирц Мусар, *Водич кроз Закон о заштити података о личности*, Повереник за информације од јавног значаја и заштиту података о личности, Београд, 2009, страна 16.

2.1.2. Чување и обрада података о личности

Подаци о личности се чувају у збиркама података. Збирка података, према члану 3, став 6. ЗЗПЛ, представља скуп података који се аутоматизовано (коришћењем информационе технологије) или неаутоматизовано воде и доступни су по личном, предметном или другом основу, независно од начина на који су сачувани и места где се чувају. У збирку података могуће је убројати разне базе, евиденције, регистре, уписнике, спискове, као и друге облике информација које одговарају дефиницији низа података о личности, као на пример разни уговори, записници, здравствени картони, видео снимци и сл. Ако систем управљања збиркама омогућава приступ подацима о личности појединца на основу његовог имена, или његових других идентификационих знакова (нпр. јединствени матични број грађана, датум рођења, адреса итд.) онда се ради о збирци података о личности. Ручно вођене збирке представљају збирку података уколико је могуће на основу, односно уз помоћ одређених мерила, приступити подацима о личности и неког појединца на тај начин идентификовати. Са друге стране, уколико непосредна доступност, односно претрага података појединаца, који се налазе у некој збирци, није могућа и уколико се њихови подаци само случајно, несистемски појављују у збирци (нпр. збирци техничких података), таква збирка не представља збирку података у смислу ЗЗПЛ.[71]

Обрада података је свака радња предузета у вези са подацима као што су: прикупљање, бележење, преписивање, умножавање, копирање, преношење, претраживање, разврставање, чување, раздвајање, укрштање, обједињавање, уподобљавање (прилагођавање), мењање, обезбеђивање, коришћење, стављање на увид, откривање, објављивање, ширење, снимање, организовање, чување, прилагођавање, откривање путем преноса или на други начин чињење доступним, прикривање, измештање и на други начин чињење недоступним, као и спровођење других радњи у вези са наведеним подацима, без обзира да ли се врши аутоматски, полуаутоматски или на други начин (чл. 3. ст.3. ЗЗЛП). Законодавац овим набрајањем не врши исцрпљивање могућих начина обраде, чиме наведене облике не треба сматрати за *numerus clausus* већ као одређене примере руковања подацима, а да се у пракси може јавити још начина на који се обрађују подаци о личности.

[71] Н. Пирц Мусар, *op.cit.* страна 17-18.

2.1.3. Заштита података о личности – права субјекта чији се подаци обрађују

ЗЗЛП као кровни закон који уређује област обраде података о личности одређује скуп права појединца у погледу остварења заштите података о личности.

Та права обухватају:

1) Право на давање/недавање пристанка за обраду – свако физичко лице има право да руковаоцу да или одбије да да пристанак за обраду података о себи, ако руковалац не врши обраду на основу законског овлашћења (чланови 10–12 и 15–18);

2) Право на обавештење о обради – лице има право да захтева да га руковалац потпуно и истинито обавести о томе да ли обрађује податке о њему, које и у коју сврху и по ком правном основу и од кога их прикупља; у којим збиркама података се налазе подаци о њему, ко су корисници и којих података и у које сврхе и по ком правном основу; коме и који подаци се преносе, у коју сврху и по ком правном основу, као и свим осталим питањима из члана 19. Закона;

3) Право на увид – лице има право да захтева да му се ставе на увид подаци који се на њега односе. Право на увид обухвата право на преглед, читање и слушање података, као и прављење бележака (члан 20);

4) Право на копију – лице има право да од руковаоца захтева копију података који се на њега односе, при чему је дужан да сноси само нужне трошкове израде и предаје копије (члан 21);

5) Права поводом извршеног увида – лице има и право да од руковаоца захтева исправку, допуну, ажурирање или брисање података, као и прекид и привремену обуставу обраде, ако су испуњени услови предвиђени чланом 22. Закона.

Права на обавештење, увид, исправку и брисање су битан институт и заштита који лицу пружа могућност остваривања његових права у односу на руковаоца збирки података. Та права су део Уставом опредељене заштите података о личности, као што их дефинише члан 42. Устава Републике Србије, који одређује да свако има право да буде обавештен о прикупљању података о личности у складу са законом, те право на судску заштиту у случају њихове злоупотребе.

Наведена права представљају један од облика права лица на информисано одлучивање док истовремено обезбеђују транспарентност обраде података. Сврха тих права је да обезбеде поштену и закониту обраду података о личности, тако да лице

увек може имати увид у то који подаци о њему се обрађују, те може захтевати брисање незаконито сакупљених података, односно уложити приговор због незаконите обраде података. [72]

Ова права се остварују упућивањем одговарајућег захтева руковаоцу. Чланом 24. ЗЗПЛ дефинисано је да Захтев за остваривање права у вези са обрадом података о личности мора да садржи:

1. податке о идентитету подносиоца (име и презиме, име једног родитеља, датум и место рођења, јединствени матични број грађана),

2. адресу пребивалишта, односно боравишта, као и друге податке неопходне за контакт,

3. што прецизнији опис у вези са обрадом података, пре свега појашњење контекста који је претходио прикупљању података од стране руковаоца, како би руковалац могао да одговори на захтев у случају да се подаци налазе у неаутоматизованим збиркама података о личности.

Достављање захтева се може вршити поштом, електронском поштом или предати на писарници руковаоца. Чланом 25. ЗЗПЛ предвиђа се да руковалац, након што је примио Захтев, мора издати обавештење о обради без одлагања, а најкасније у року од 15 дана од дана подношења. Истим чланом Закона предвиђа се да, ако руковалац одбије захтев, о томе доноси решење са поуком о правном средству. Уколико руковалац не обрађује никакве податке о подносиоцу, о томе ће обавестити подносиоца, а чланом 32. ЗЗПЛ предвиђено је да у том случају прослеђује захтев Поверенику за заштиту информација од јавног значаја и заштиту података о личности (у даљем тексту Повереник), осим ако се подносилац захтева томе противи. После тога Повереник проверава да ли руковалац обрађује тражени податак.

Повереник за информације од јавног значаја и заштиту података о личности обавља послове заштите података о личности као самосталан државни орган, независан у вршењу своје надлежности, а судски поступак заштите података о личности води се пред Управним судом. Функција Повереника произлази из захтева ЕУ Директиве о заштити података о личности у погледу обавезе држава да обезбеде независан орган за заштиту података о личности (Члан 4 Директиве).

[72] Н. Пирц Мусар, о*p.cit,* страна 42.

У случају да захтев буде прослеђен Поверенику, он врши проверу да ли руковалац обрађује тражени податак и у случају да утврди да га не обрађује, Повереник ће доставити захтев руковаоцу за ког утврди да тражени податак обрађује и о томе обавестити подносиоца захтева или ће га упутити на руковаоца који обрађује податак, у зависности од тога на који ће се начин ефикасније остварити захтев. Руковалац у том случају мора одлучити у року од 15 дана од уручења прослеђеног захтева. Ако у тој фази Повереник утврди да руковалац коме је првобитно био поднет захтев, заиста обрађује захтеване податке, решењем ће наложити руковаоцу да одлучи о захтеву. У овом случају руковалац мора да одлучи о достављеном захтеву у року 7 дана од дана достављања решења Повереника (чл. 33. ЗЗЛП)

У пракси ово представља гаранцију лицу да је деловање руковаоца у вези са захтевом стварно подвргнуто провери другостепеног органа, без сумње да ће такав однос повећати и поверење појединаца у одлуке, односно одговоре руковаоца, с обзиром да ће руковалац знати да не може да избегне надзор.[73]

2.1.4. Поступак повереника по жалби

У вези са остваривањем права на обавештење, увид, копију, исправке и брисање, као и на прекид и привремено обуставу обраде по ЗЗПЛ лице увек има могућност изјављивања жалбе Поверенику. Закон у четвртом поглављу уређује поступак по жалби у погледу извршавања захтева за обавештење, увид, копију, исправку и брисање (члан 38–43 ЗЗЛП).

Подносилац захтева може у року од 15 дана (по уручењу одлуке о одбацивању, односно одбијању захтева, односно по истеку утврђеног рока), изјавити жалбу Поверенику:

1. против одлуке руковаоца којом је одбијен или одбачен захтев;

2. када руковалац не одлучи о захтеву у прописаном року (15 дана код захтева за обавештењем са могућим продужењем на укупно 45 дана у случају оправданог продужења рока; 15 дана код захтева за исправку, допуну, ажурирање и брисање података, као и код захтева за опозив и привремену обуставу обраде података; односно 30 дана код захтева за увид или копију, са могућим продужењем на укупно 60 дана у случају оправданог продужења рока);

[73] Водич кроз Закон о заштити података о личности, *op.cit*, страна 52.

3. ако руковалац не стави на увид податак, односно не изда копију податка или то не учини у року и на начин прописан овим законом;

4. ако руковалац услови издавање копије података уплатом накнаде која превазилази износ нужних трошкова израде копије;

5. ако руковалац, супротно закону, отежава или онемогућава остваривање права подносиоца.

Уз жалбу се прилаже захтев са доказом о предаји и одлука која се оспорава.

Повереник доноси одлуку по жалби најкасније у року од 30 дана од дана подношења жалбе. Жалба се пре тога доставља руковаоцу, који има могућност одговора на жалбу. О наводима из одговора на жалбу, потом има право да се изјасни подносилац који је поднео првобитни захтев. Повереник одбацује решењем неблаговремену или непотпуну жалбу, односно жалбу која је изјављена од неовлашћеног лица. Ако Повереник не одбаци жалбу већ је узме у суштинско одлучивање, предузима све потребне мере за утврђивање чињеничног стања које су потребне за одлучивање по жалби. Поверенику, односно лицу кога он посебно овласти, у складу са чланом 40. Закона који дефинише утврђивање чињеничног стања у поступку по жалби, ради утврђивања чињеничног стања, омогућиће се увид у податак. Према првобитној верзији Закона, Поверенику је било омогућено да изврши увид и у комплетну документацију која се односи на прикупљање података и друге радње обраде, као и на остваривање права лица из овог закона, опште акте руковаоца, просторије и опрему коју користи руковалац. Међутим, доношењем Закона о тајности података[74], одредбе чл. 45. од 2. до 4. престају да важе.

Повереник у одређеним случајевима (ако би се тиме могао истински угрозити интерес националне или јавне безбедности, одбрана државе или активности спречавања, откривања, истраге и гоњења кажњивих радњи) нема увид, односно приступ до свих потребних података. У пракси би та ограничења могла истински угрозити или сасвим онемогућити рад Повереника, нарочито у случајевима који су из угла заштите права лица на приватност пред захтевима државе, највише осетљиви.[75]

Снага Повереника у надзирању законитости обраде података о личности је најзначајнија управо у односу на руковаоце који имају таква овлашћења за приступ

[74] Закон о тајности података, *Службени гласник РС, бр.* 104/2009.

[75] Водич кроз Закон о заштити података о личности, *op.cit*, страна 53

основном људском праву на заштиту података о личности и највише задиру у приватност лица. Заправо ови органи имају таква овлашћења да могу задирати у приватност лица тако да оно за то уопште не зна (прислушкивање телефонских разговора, тајно праћење...), те довести до дугорочних последица. Ограничити надзорни орган управо у том делу је такође нелогично. Сваки руковалац збирком података мора поштовати начело сразмерности, које је основни принцип, такође и при заштити основног људског права на приватност, коју обезбеђује члан 8. Конвенције о основним људским правима Савета Европе. Такође, Повереник мора у свом раду поштовати начело сразмерности (посматрати и надзирати тачно толико података о личности колико је то неопходно за успешно извођење надзора). С тога је начело сразмерности управо то које Повереника ограничава, а не a priori одредба у закону. [76]

Када Повереник, на основу жалбе поднете из разлога ћутања руковаоца (јер руковалац није одговорио на захтев појединца), утврди да је жалба основана, решењем ће наложити руковаоцу да у одређеном року поступи по захтеву. Решење Повереника по жалби је обавезујуће, коначно и извршно. У случају потребе, Влада обезбеђује извршење решења Повереника и може ближе да одреди начин извршења решења. У случају неизвршења решења Повереника могуће је руковаоца, обрађивача или корисника (правно или физичко лице, као и одговорно лице у правном лицу, државом органу, органу територијалне аутономије или органу локалне самоуправе) у прекршајном поступку, такође казнити новчаном казном.

Од почетка рада Повереника до 30.09.2016. године, укупно је примљено 1315 жалби, од тога:

1) у 2009. години – 3 жалбе
2) у 2010. години – 43 жалбе
3) у 2011. години – 70 жалби
4) у 2012. години – 153 жалбе
5) у 2014. години – 241 жалба
6) у 2015. години – 307 жалба
7) закључно са 30.09.2016. године – 310 жалби[77]

[76] Водич кроз Закон о заштити података о личности, о*p.cit,* strana 54.

[77] Информатор о раду Повереника за приступ информацијама од јавног значаја и заштиту података о личности, преузето 29.09.2016. године са :
http://www.poverenik.rs/images/stories/informator-o-radu/2016/septembar/cirinformatorseptembar2016.pdf, стр. 179.

Након пријема жалбе, повереник обуставља жалбени поступак:

– ако руковалац након изјављене жалбе због непоступања по захтеву, а пре доношења одлуке по жалби, омогући остваривање права на увид, односно копију, или одлучи у складу са захтевом;

– ако подносилац одустане од жалбе.

Табела 1. Поступање Повереника по жалби због повреде прва на заштиту података о личности[78]

Број/година	2009.	2010.	2011.	2012.	2013.	2014.	2015.	Закључно са 30.09.2016. године
Укупно примљено жалби	3	43	70	153	188	241	307	310
Основане жалбе		17	29	59	78	105	111	70
Налог руковаоцу за поступање		7	15	35	54	63	90	60
Поништено решење и враћено руковаоцу на поновни поступак		5	10	15	15	27	15	7
Поништено решење руковаоца и наложено да се поступи по захтеву странке		5	2	7	9	13	5	2
Поништава се		0	2	2	0	2	1	1

[78] Информатор о раду Повереника, *op.cit*, str. 179-180

Жалба одбијена као неоснована		0	10	11	17	49	45	76

Дата статистика указује на ширење свести код грађана у вези са важношћу чувања личних података на прави начин, обрадом која се над њиховим подацима врши, као и о облицима заштите који су им на располагању уколико дође до повреде. Грађани из године у годину упућују све већи број жалби Поверенику и тиме предузимају проактивне кораке у вези са заштитом својих права. Ипак, велики број основаних жалби указује и да руковаоци подацима не поступају у складу са законом, те је велики број ситуација у којима је повереник морао да реагује.

Поред конкретног управног поступка у ком Повереник врши заштиту права, он то чини и кроз вршење надзора над спровођењем Закона о заштити података о личности, и указивањем на уочене злоупотребе приликом прикупљања података, даје предлоге и препоруке за унапређење заштите података у складу са чл. 44 Закона, као и давањем мишљења о руковању подацима о личности.

Тако је повереник до данас вршио надзор над спровођењем Закона, па је у том смислу упозоравао различите државне органе и приватне организације уколико њихов рад није у складу са Законом о заштити података о личности. Битна улога повереника се огледа и у томе што он стално прати нове тенденције у руковању подацима, па правовремено реагује уколико је неки од нових начина противан Закону.

Тако је Повереник реаговао у ситуацијама злоупотребе података о личности, те је издао упозорење Републичком геодетском заводу - да снимањем камерама у пријемним канцеларијама служби за катастар у Београду, Земуну, Нишу и Новом Саду и даљом обрадом личних података путем преноса истих (live streaming), чинећи податке доступним неограниченом броју корисника Интернета врши недозвољену обраду података о личности, Министарству здравља - у коме му је указао на неправилности у обради података о личности коју врши у оквиру Интегрисаног здравственог информационог система, јер псриступ истом има преко 60 хиљада људи неограничено, Министару просвете - указао је на то да су подаци о синдикалном чланству посебно осетљиви подаци, те да је противно Закону правити базе и сачињавати такве спискове, сем уколико иста лица не дају свој изричит пристанак.

VI ЗАКЉУЧАК

Док се право и даље бори да потпуно дефинише и регулише зашититу података о личности, нове технологије све више постају централни део наше свакодневнице, породице и целокупног друштва. Оне чине да изнова испитујемо шта сматрамо приватним, и да померамо границе у оквиру којих желимо да се одрекнемо својих права, само да бисмо ускористили услугу коју нам технологија омогућава.

Разлог пружања овако јефтиних, а за кориснике погодних услуга, је што се заузврат одричемо својих података о личности и дозвољавамо компанијама да их даље обрађују и користе у сопствене комерцијалне сврхе. Значај заштите података о личности државе разумеју, те раде на детаљној регулацији ове области, предвођене Европском унијом која поставља пример добре праксе, а који се понекад сматра и превише строгим за компаније.

Државе то чине због велике вредности које подаци о личности имају, поготово у ери потрошачког друштва где за остваривање маркетиншких и трговинских циљева такви подаци представљају значајну информацију. Препознавањем велике важности заштите података о личности, ово право је временом постало и самостално основно људско право.

Због тога је потребно стално праћење и регулисање ове области, а поред заштите права грађана, држава мора водити рачуна и о остваривању економских циљева компанија, па је велика борба између приватних руковаоца подацима и држава које им намећу нова правила и обавезе.

Због тога јавно право има велику улогу у овој области, које руковаоцима намеће низ принципа за фер обраду података о личности и чува баланс између права грађана иосталих интереса. Управни орган - повереник за заштиту података о личности, јавља као најзначајнији орган који надзире примену закона. Ипак, потребно је много урадити на едукацији становништва, а и пооштрити казне за руковаоце, јер се велики број налога повереника не извршава и поред новчаног кажњавања које он врши.

Како се обрада података о личности, у условима савременог света, не може просто заобићи, потребно је са великом пажњом пратити и правовремено регулисати ову област, јер нас могућности нових технологија у супротном чине отвореном књигом, а да тога ни сами нисмо свесни.

ЛИТЕРАТУРА

1. A. Rouvroy and Y. Poullet, *The Right to Informational Self-Determination and the Value of Self- Development: Reassessing the Importance of Privacy for Democracy*, Reinventing Data Protection, 2009
2. A. Moore, Privacy rights: Moral and legal foundations, *The Pennsylvania State University Press, University Park, Pennsylvania*, 2010.
3. B. Van Alsenoy and M. Koekkoek, *The extra-territorial reach of the EU's "right to be forgotten",* Working Paper No. 152 – March 2015.
4. F. Hondius, Emerging Data Protection in Europe, Амстердам, 1975
5. G. Domien, *Short guide to the European Convention on Human Rights (3rd edition),* Counsil of Europe, 2005.
6. G. Gonza´lez Fuster and R. Gellert, The fundamental right of data protection in the European Union: in search of an uncharted right, *International Review of Law, Computers & Technology,* Vol. 26, No. 1, 2012.
7. M. Cunningham, Complying with International Data Protection Law, 84 *University of Cincinnaty Law Review*, 2016.
8. M. Friedwald, D. Wright, S. Guzwirght and E. Mordini, Privacy, data protection and emerging sciences and technologies: Towards a common framework; in: *Innovation – The European Journal of Social Science Research, Vol. 23, No. 1,* 2010.
9. M. Tzanou, Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right, in: *International Data Privacy Law 3 (2*), 2013.
10. M. Tzanou, Is data protection the same as privacy? An analysis of telecommunications' Metadata Retention Measures, *Journal of Internet Law*, 2013, Вол. 17, Издање 3.
11. L. Bygrave, *Data Protection Law: Approaching Its Rationale, Logic, and Limits*, The Hague, 2002.
12. Н. Пирц Мусар, *Водич кроз Закон о заштити података о личности*, Повереник за информације од јавног значаја и заштиту података о личности, Београд, 2009.
13. P. Carey, Data Protection, *A practical guide to UK and EU law,* Oxford, 2014.
14. S. Gutwirth, Y. Poullet, P. De Hert, C. de Terwangne and S. Nouwt (eds.), *Reinventing data protection?*, Springer**,** Dordrecht, 2009.
15. S. Warren and L. Brandeis, The Right to privacy, *Harvard Law Review*, Vol. 4, No. 5.

16. Westin, Privacy and freedoms, *in: Washigton and Lee Law review*, Bodley Head, 1970.
17. У. Мишљеновић, Б. Недић, А. Тоскић, *Заштита приватности у Србији – Анализа примене Закона о заштити података о личности*, Београд, 2013.
18. N. Ni Loidean, The End of Safe Harbor: Implications for EU Digital Privacy and Data Protection Law, *Journal of Internet Law*, vol. 19, no. 8.
19. R. Gellert and S. Gutwirth, "The legal construction of privacy and data protection", *Computer Law & Security Review (CLSR)*, 2013, Vol. 29.
20. J. Kokott and C. Sobotta, The distinction between privacy and data protection in the jurisprudence of the CJEU and the EctHR, *International Data Privacy Law*, 2013, Vol. 3, No. 4.

Судске одлуке

1. Application no. 30562/04 and 30566/04, S. and Marper v. the United Kingdom.
2. Application no. 25576/04, Flinkkilä and Others v. Finland.
3. Application no. 184/06, Saaristo and Others v. Finland.
4. Application no. 42811/06, Alkaya v. Turkey.
5. Application no. 1593/06, Kurier Zeitungsverlag und Druckerei GmbH v. Austria(no. 2).
6. Application no. no. 53495/09, Bohlen v. Germany.
7. Application no. 62617/00, Copland v. the United Kingdom.
8. Application no. 40660/08 and 60641/08, Von Hannover v. Germany (no. 2).
9. Application no. 59631/09, The Verlagsgruppe News GmbH and Bobi v. Austria.
10. Application no. 44647/98, Peck v. the United Kingdom.
11. Application Series A no. 91, X and Y v. the Netherlands.
12. Application no. 36505/02, August v. the United Kingdom;
13. Application no. 39272/98, M.C. v. Bulgaria.
14. Application no. 2872/02, K.U. v. Finland.
15. Application no. 35623/05, Uzun v. Germany.
16. Case C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González.
17. Case C-362/14 Maximillian Schrems v Data Protection Commissioner joined party: Digital Rights Ireland Ltd.

18. Одлука Уставног суда, I Уз број 421/2013 од 5. јуна 2014. године, објављена у "Сл. гласнику РС", бр. 73/2014 од 16. јула 2014. године.
19. Одлука Уставног суда, I Уз број 252/2002 од 26. децембра 2013. године, објављена у "Сл. гласнику РС", бр. 65/2014 од 27. јуна 2014. године.
20. Одлука Уставног суда, I Уз број 41/2010 од 30. маја 2012. године, објављена у "Сл. гласнику РС", бр. 68/2012 од 18. јула 2012. године.

Остала истраживачка грађа

1. Европска конвенција за заштиту људских права и основних слобода, Рим, 4. новембар1950, CETS бр:005.
2. Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, *Official Journal L 215.*
3. Commission implementing decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, *Official Journal of the European Union* L 207/1
4. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ETS No.108, *European Treaty Series - No. 108*.
5. Директива 95/46/ЕС Европског парламента и Савета од 24. октобра 1995. године о заштити појединаца у вези са обрадом података о личности и слободном кретању тих података, *Службени гласник Европске уније* Л 281 , 23/11/1995 П. 0031 – 0050.
6. 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), *Official Journal of the European Communities* L 201 , 31/07/2002 P. 0037 – 0047
7. Информатор повереника за приступ подацима од јавног значаја и заштиту података о личности, 2016.

8. European Union Agency for Fundamental Rights, Council of Europe, Handbook on European Data protection Laws, Publications Office of the European Union, Luxembourg, 2014.
9. Лисабонски уговор којим се мења Уговор о Европској унији и Уговор о оснивању Европских заједница, потписан у Лисабону, 13. децембра 2007. Године, Службени гласник Европске уније, Ц 306, 17 December 2007.
10. Повеља Европске уније о основним слободама, 2007 (2007/Ц 303/01).
11. Појашњења Европске комисије у вези са реформом заштите података о личности – питања и одговори, 2015.
12. 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, *Official Journal of the European Communities*, no L 8/1
13. 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), *Official Journal of the European Union* L 119/1
14. Смернице за регулисање компјутеризованих података о личности, усвојене на 68. Седници Уједињених нација дана 14. Децембра 1990. Године, A/RES/45/95
15. The European Data Protection Supervisor, *Leading by example - The European data protection supervisor strategy 2015-2019*, Luxembourg, Publications Office of the European Union, 2015
16. The right to privacy in the digital age, no. A/HRC/28/L.27, 26 March 2015
17. Универзална декларација о људским правима, усвојена и проглашена резолуцијом Генералне скупштине Уједињених нација 217 (III) од 10. децембра 1948. године.
18. UN Human Rights Committee (HRC), CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988.
19. Устав Републике Србије, *Службени гласник РС* бр. 98/2006.
20. Закон о заштити података о личности, Службени гласник РС бр. 97/2008, 104/2009 - др. закон, 68/2012 - одлука УС и 107/2012.
21. Закон о заштити података о личности, *Службени лист СРЈ бр.* 24/98.

22. Закона о потврђивању Конвенције у односу на аутоматску обраду личних података, *Службени лист СРЈ* бр. 1/92
23. Закон о тајности података, *Службени гласник РС, бр.* 104/2009.

Сажетак

Јавноправна заштита података о личности

Заштита података о личности је грана права која се бави начином на који организације могу и треба да рукују личним подацима. Настала је услед повећане централизације података о личности и стварања огромних база података и потребе омогућавања слободног протока тих информација. Код заштите података о личности, потреба да се обрада података врши се претпоставља, због чега нас право на заштиту података о личности не штити од обраде, већ од нелегалне и непропорционалне обраде података. Услед брзог развоја технологије и стварања нових начина за манипулацију подацима о личности, законодавци врше детаљну правну регулацију, у међувремену покушавајући да тумачењем попуне празнине које услед константног напредовања у технологији настају. Европска унија се тренутно највише бави овим питањем, а ове године је усвојила и Генералну регулативу за заштиту података о личности која ће 2018. године заменити до тада примењивану Директиву из '95, а у циљу боље заштите грађана Европске уније. Како земља у којој се подаци прикупљају врло често разликује од земље у којој се подаци о личности обрађују, у том смислу ЕУ утиче и на остатак света, наметајући обавезе у погледу руковања подацима грађана ЕУ. Зато су 2016. године усвојена нова правила „ЕУ-САД штит приватности“ који је 2016. године заменио до тада важеће принципе „Сигурне луке“ у погледу прекоокенске обраде података грађана ЕУ. У циљу контроле над спровођењем закона о заштити података о личности, државе успостављају независтан државни орган – повереника за заштиту података о личности, који пружа заштиту грађанима чијим се подацима рукује, прати примену закона и упозорава на новонастале претње по заштиту података о личности указујући јавном и приватном сектору на неадекватно руковање подацима. Подаци о личности трпе посебну опасност од злоупотребе приликом коришћења информационих технологија и интернет услуга, где пружаоци услуга постају руковаоци огромне

количине података који конкретно одређују лице, или великог броја података преко којих је лице одредиво, те стварно или потенцијално управљају приватношћу корисника. Јављају се у форми свеобухватних пружаоца услуга путем претраживача интернета, мобилних телефона и мобилних апликација, као и интернет сајтова који користе податке о личности, стваран свет селе „online“ и стварају велику заједницу у којој обавезе њених чланова нису истоветно регулисане као у стварном свету. Како корисници пре употребе ових услуга увек дају сагласност за коришћење података о личности, на државама је да ову област што боље уреде и наметну правила пословања компанијама, јер је обрада података неминовност, а држава мора да нађе начин да у свему томе своје грађане заштити.

Кључне речи: приватност, заштита података о личности, штит приватности, сигурна лука, повереник за заштиту податак о личности, Гугл политика приватности

Abstract

Personal data protection in public law

Personal data protection a branch of law that deals with the way in which organizations can and should handle personal data. It emerged due to increased centralization of personal data and the growth of huge databases, and the need to facilitate the free flow of such information. The need for processing of personal data is assumed, which is why personal data protection laws do not protect us against processing, rather from illegal and disproportionate processing. Due to the rapid technology development and making new ways for handling personal data, legislators are conducting detailed legal regulation, in the meantime interpreting the law to fill in the legal gaps which occur due to the constant advancement in technology. The European Union is currently most concerned with this issue, and this year it has adopted the General regulations for the protection of personal data that will replace in 2018 the Directive from '95, in order to protect better the citizens of the European Union. Since country where the data is collected is often different from the country in which the data are processed in this context, the EU also affects the rest of the world by imposing obligations in terms of handling the data of EU citizens. Therefore, the 2016 adopted new rules,, EU-USA privacy shield” which will in 2016 replace previously applicable,,Safe harbor" principles regarding overseas processing of EU citizens data. In order to control over the implementation of the Law on Personal Data Protection, states are establishing an independent state body - the Commissioner for Personal Data Protection,

which provides protection to citizens whose data are used, monitors the implementation of laws and alerts to new threats to the protection of personal data by indicating inadequate data handling by the public and the private sector. Personal data are in a distinct risk of abuse in the use of information technology and internet services, where service providers are becoming operators of the huge amount of data which identify the particular person or a large number of data over which the person identifiable, and actually or potentially manage user privacy. They appear in the form of comprehensive service provider via the Web browser, mobile phones and mobile applications as well as internet sites that use personal data, moving the real world 'online' and creatinh a great community in which the obligations of its members are not identically regulated like in the real world. As users before using these services always give consent for use of personal data, states are to regulate this area as good as possivle and enforce the rules of business to companies, because data processing is inevitable, and the state must find a way to protect its citizens.

Keywords: privacy, data protection, privacy shield, safe harbour, data protection commissioner, Google privacy policy

Биографија студента

Ивана Станковић је рођена 1990. године у Нишу. Правни факултет Универзитета у Нишу уписала је школске 2009/2010. године, а дипломирала је 27. јуна 2014. године, са просечном оценом 9,09. Школске 2014/2015. године уписала је мастер академске студије на истом факултету, на општем смеру, ужа јавноправна научна област. У току основних студија, испред Факултета је учествовала на регионалним и међународним симулацијама суђења, и то Регионалној симулацији суђења у Сарајеву 2012. године у организацији Civil right defenders, Европској симулацији суђења у Стразбуру 2013. године у организацији Савета Европе и Европског удружења студената права (ELSA) , Светској симулацији суђења у Оксфорду 2013. године у организацији Универзитета у Окфорду и Програма за компаративно медијско право и политику, на ком је освојила Награду за најбољи поднесак. У регионалној фази истог такмичења наредне године је учесвовала као судија.

Добитник је „Константинове стипендије“ која се додељује у оквиру Програма „Покрени се за будућност“, као најбољи студент Правног факултета Универзитета у Нишу за школску 2012/2013. годину. Била је стипендиста Министарство просвете, науке и технолошког развоја Републике Србије, као и Града Ниша. У оквиру Програма „Покрени се за будућност“, Ивана је водила тим студената који је спроводио пројекат пружања бесплатне правне помоћи „Мобилна правна клиника“. Учествовала је у бројним семинарима и конференцијама, од чега издваја: „Young Faces Conference: “Use and Abuse of Electronic Surveillance” у организацији The Geneva Centre for the Democratic Control of Armed Forces (DCAF), with the support of the Swiss Ministry of Defence, „Youth Capstone Coalition“, организован од стране International Republican Institute у Београду, „Protection of Safety and Integrity of Journalists in the OSCE region“ организован од стране Organisation for Safety and Cooperation in Europe, „Правна клиника за заштиту права жена“.

Ивана Станковић тренутно завршава приправнички стаж у адвокатској канцеларији у Нишу. Говори енглески и италијански језик.