УДК 342.721:004.738.6
DOI: https://doi.org/10.22182/spm.6022018.7
Прегледни рад

Српска политичка мисао
број 2/2018.
год. 25. vol. 60
стр. 115-133

Синиша Домазет*
Факултет за студије безбедности,
Универзитет Едуконс, Сремска Каменица

Здравко Скакавац
Факултет за правне и пословне студије др Лазар Вркатић,
Нови Сад, Универзитет Унион, Београд

СКАНДАЛ „КЕМБРИЏ АНАЛИТИКА“ – НОВИ ИЗАЗОВ У ЗАШТИТИ ПОДАТАКА О ЛИЧНОСТИ?**

Сажетак

У овом раду је анализирана афера у вези са компанијама Фејсбук и Кембриџ аналитика, у светлу нове Уредбе ЕУ у области заштите података (GDPR). Анализа је показала да постоји велика потреба за ефикаснијом заштитом личних података корисника на интернету. Такође, анализа је показала на који начин су вршене злоупотребе личних података. С обзиром да се нова Уредба може примењивати и ван граница Европске уније, у вези са њеном екстериторијалном применом указано је на неколико кључних проблема. Прво, утврђено је да у пракси постоје тешкоће у вези са спровођењем Уредбе. Друго, анализа је показала да се у случају екстериторијалне примене Уредбе јавља проблем сукоба јурисдикција. Треће, нису довољно развијени механизми за решавање сукоба закона између различитих држава. Решење представља закључивање билатералних међународних уговора између Европске уније и трећих земаља. На овај начин би се омогућила примена Уредбе и у државама које нису чланице Уније. У истраживању су коришћени нормативни метод и правно-логички методи индукције и дедукције.

Кључне речи: право, политика, безбедност, ЕУ, заштита података

* sdomazetns@gmail.com

** Овај рад је део истраживачког пројекта под шифром 47009 (Европске интеграције и друштвено-економске промене привреде Србије на путу ка ЕУ), финансираног од стране Министарства просвете, науке и технолошког развоја Републике Србије.

1. ДРУШТВЕНЕ МРЕЖЕ КАО ИЗВОР ЛИЧНИХ ПОДАТАКА

Социјалне интеракције милиона људи широм света, заједно са стварањем виртуелних идентитета, друштвених односа и заједнице, доводе до сценарија у којем рачунарска технологија и виртуелна комуникација формирају паралелно друштво и нови виртуелни културни простор.[1] Предности интернета су велике, али само када се интернет схвати као средство, а не као тренутна замена стварном животу.[2] Док су класични *broadcast* медији организовани по моделу један-свима, интернет је заснован на принципу сви-свима.[3] Да би повећали своју атрактивност и привукли што већи број нових познаника, корисници мрежа остављају различите врсте информација и фотографија. У тој намери често заборављају на опасност коју за собом носи доступност њихових личних података великом броју корисника. Мреже су примамљиве посебно због тога што корисници могу сами да управљају врстом садржаја које остављају, уз могућност да уклањају информације које би могле да умање њихово пројектовано друштвено представљање.[4] Годинама су крајњи корисници безбедност у сајбер окружењу схватали здраво за готово. Користили су готове апликације и услуге познатих компанија сматрајући их заштићеним и безбедним. Верујући компанијама, заправо су веровали њиховом IT-сектору рачунајући да свакодневно раде на унапређивању безбедности. То јесте било тачно и ефикасно дуги низ година, али последњих година то више није довољно. Број претњи је већи него икада раније и у порасту је њихова учесталост и озбиљност.[5]

1) Vesna Baltezarevic *et al.*, "Human need for communication in the system of virtual organizations", *Egyptian Computer Science Journal*, Vol. 40, No.1/2016, стр. 54.

2) Vesna Baltezarević *et al.*, "Who controls the controllers of the internet?", *Journal of Systems Applications, Engineering & Development*, North Atlantic University Union, Vol. 10, 2016, стр. 324. Преузето из: Весна Балтезаревић, Радослав Балтезаревић, „Заштита приватности на интернету – европски модел", *Мегатренд ревија*, Универзитет Џон Незбит, Београд, Вол. 14, бр. 1/2017, стр. 242.

3) Милорад Ђурић, „Глобалне комуникације и светско друштво: проблем легитимацијског дефицита", *Српска политичка мисао*, Институт за политичке студије, Београд, бр. 02/2016, стр. 43-59.

4) Cliff Lampe, Nicole Ellison, Charles Steinfield, *Changes in use and perception of Facebook*, Internet, http://www-personal.umich.edu/~enicole/LampeEllisonSteinfield2008.pdf, 25/04/2018.

5) Тања Каурин, Драган Ануцојић, Здравко Скакавац, „Дифузија моћи у сајберпростору: изазов или претња безбедности", у монографији: *Савремени изазови међународне безбедности*, (приредио: Слободан Марковић), Факултет за правне и пословне студије др Лазар Вркатић, Универзитет Унион, Београд и Центар за међународне студије, Загреб, 2017, стр. 208.

Велики проблем у вези са личним подацима корисника друштвених мрежа лежи у чињеници да су и они сами, неретко, неопрезни приликом коришћења ових мрежа, те њихови подаци често завршавају у погрешним рукама, укључујући и њихове личне фотографије. У пракси се показало да су лични подаци корисника друштвених мрежа често предмет објављивања, коришћења, али и трговине, без њиховог знања. Истина, корисници покушавају да се заштите тако што би просто обрисали свој налог и тако уклонили депоноване податке, али испоставило се да то није довољно, јер су мреже и даље наставиле да чувају њихове податке. Корисници су настојали да се заштите и креирањем лажних профила, као и остављањем лажних података на друштвеним мрежама, или увођењем ограниченог приступа својим профилима.[6] Ипак, помало зачуђујуће делује чињеница да корисници друштвених мрежа, иако су свесни да њихови лични подаци могу бити злоупотребљени, често уопште не предузимају одговарајуће мере заштите, што по неким ауторима представља такозвани „приватни парадокс".[7]

Дакле, интернет и друштвене мреже су унели праву пометњу у погледу заштите права на приватност појединца, штавише, у великој мери су угрозили ово право. Један од највећих проблема представља чињеница да се ови подаци могу лако искористити у различите сврхе, као што су наношење финансијске и друге штете корисницима, уцене, крађу идентитета, израду профила корисника, или нарушити принцип „добросуседских односа" између држава, који добија све већи значај у политици проширења Уније.[8] Ипак, пракса је показала да се лични подаци могу злоупотребити и у политичке сврхе, што је показао случај компанија Фејсбук и Кембриџ аналитике, о којима ће у наставку бити више речи.

2. СЛУЧАЈ „КЕМБРИЏ АНАЛИТИКА"

Заштита приватних података нарочито је добила на значају када је у светску јавност „испливала" сензационална прича у вези са оптужбама за злоупотребу података од стране компаније Кем-

6) Danah Boyd, Eszter Hargittai, *Facebook privacy settings: Who cares?*, Internet, http://firstmonday.org/ojs/index.php/fm/article/view/3086/2589, 25/04/2018; Alison Young, Anabel Quan-Haase, "Privacy protection strategies on Facebook: the Internet privacy paradox revisited", *Information, Communication & Society*, UK, No. 16(4)/2013, стр. 479-500.

7) Patricia Norberg, Daniel Horne, David Horne, "The privacy paradox: Personal information disclosure intentions versus behaviors", *Journal of Consumer Affairs*, George Washington University School of Business, Vol. 41, No. 1/2007, стр. 100-126.

8) Синиша Домазет, Здравко Скакавац, „Добросуседски односи на Балкану као услов за приступање Европској унији: препрека или добра пракса?", *Српска политичка мисао*, Институт за политичке студије, Београд, бр. 3/2016, стр. 139-155.

бриџ аналитике и компаније Фејсбук. Технолошки гигант Фејсбук и компанија за анализу података Кембриџ аналитика нашли су се у сред расправе о прибављању и коришћењу личних података, а постављено је питање да ли је тиме извршен утицај на резултате избора у Сједињеним Државама 2016. године и референдум о Брегзиту.[9]

Треба истаћи да се поменута афера, суштински, не односи на украдене податке корисника, већ на једну сасвим нову, моћну технику манипулације тамном страном људског карактера, која има своју технолошку позадину. Реч је о моделу за одређивање карактеристика личности, који су развили Михаил Косински и Дејвид Стилвел.[10] Резултати њиховог рада, који су објавили 2013. године, су били веома запажени у научној јавности и довели су до тога да компанија Фејсбук изврши значајне промене у својој политици приватности, које су подразумевале забрану приступа апликација подацима корисникових пријатеља. Као да су знали шта ће уследити пар година потом, аутори су на крају свог рада навели да постоји ризик да ће растућа свест о дигиталној изложености негативно утицати на искуства људи у вези са дигиталним технологијама, умањити њихово поверење у онлајн услуге, или их чак у потпуности одвратити од коришћења дигиталних технологија.[11]

Након пет година, дошло је до поменуте афере са компанијама Кембриџ аналитика и Фејсбук, када се показало да су компромитовани подаци око 87 милиона корисника Фејсбука. Разумљиво, компанија Кембриџ аналитика је оштро негирала ове наводе, нагласивши да „Кембриџ аналитика не одобрава подстрекивање на незаконито деловање, подмићивање или такозване 'намештаљке', нити се упушта у ове радње, као и да не користи нетачне податке у било које сврхе".[12]

Из дана у дан, афера је постајала све већа, па су Њујорк тајмс и лондонски Обзервер објавили наводе да је компанија Фејсбук извршила одабир личних података преко 50 милиона корисника Фејсбука у циљу помоћи кампањи Доналда Трампа. Након тога су најављене и истраге од стране званичних власти, а компанија Фејсбук је саопштила да је суспендовала компанију Кембриџ аналитика. Аме-

9) BBC news, „Afera Fejsbuk-Kembridž analitika: Šta sve znamo do sada", Internet, https://www.danas.rs/bbc-news-serbian/afera-fejsbuk-kembridz-analitika-sta-sve-znamo-do-sada/ 08/04/2018.

10) Nauka kroz priče, „Pet dimenzija Kembridž analitike", Internet, https://naukakrozprice.rs/pet-dimenzija-kembridz-analitike/ 06/04/2018.

11) Michal Kosinski, David Stillwell, Thore Graepel, "Private traits and attributes are predictable from digital records of human behavior", *Proceedings of the National Academy of Sciences,* Vol. 110, No. 15/2013, ***стр.*** 5802-5805.

12) BBC news, „Afera Fejsbuk-Kembridž analitika: Šta sve znamo do sada", нав. дело.

рички и британски листови су, позивајући се на бивше запослене Кембриџ Аналитике, са седиштем у Лондону, навели да је ово једна од највећих злоупотреба података у историји Фејсбука.[13]

Нови скандалозни детаљи откривени су од стране Кристофера Вајлија, директора Кембриџ аналитике, када се показало да је „Кембриџ аналитика" (иначе у власништву је хеџ фонда Роберта Мерсера) од 2014. године неовлашћено прикупљала приватне податке корисника „Фејсбука" које је користила да би потенцијалним гласачима циљано биле достављане одређене политичке рекламе и поруке. У том погледу, Компанија је разврставала људе по категоријама у зависности од интересовања: 1) милитаризам (пиштољи, пуцање, борилачке вештине, стреле и ножеви); 2) насилни окултизам (дроге, црна магија, паганизам); 3) интелектуалне активности (певање и прављење музике, путовања у иностранство, околина): 4) они који слепо верују (паранормално, летећи тањири); 5) здрава интересовања – камповање, баштованство, пешачење.[14]

Поред тога, истрагу у вези са овом компанијом спровео је и британски „Канал 4". Тада је утврђено да се „Кембриџ аналитика", како би утицала на изборе широм света, служила и методама као што су шпијунирање, уцене, мито, лажни искази и слање проститутки клијентима, што је углавном снимано, а потом пласирано (или пређено да ће бити пласирано) на друштвене мреже. Доказ за ове незаконите радње забележен је и камером. Наиме, репортер британског телевизијског канала тајно је снимио разговоре са шефовима компаније „Кембриџ аналитика" у којима се чује како одговорни у тој фирми отворено говоре како политичаре широм света доводе у клопку и потом уцењују.[15] Методе уцене су биле различите, а снимци и новински извештаји су показали да се „Кембриџ аналитика" служила мрежом других компанија.

Разуме се, корисници Фејсбука и јавност широм света су били згрожени оваквим понашањем поменутих компанија, запитавши се како је могуће да су лични подаци корисника тако лако доступни, практично без било каквих ограничења. То је резултирало веома организованом кампањом на интернету под називом „Обришите Фејсбук" (#deletefacebook). Чак су се појавила и упутства о томе како обрисати налог са Фејсбука, али и других познатих

13) Танјуг, „Трампов тим је украо податке 50 милиона људи на Фејсбуку да би победио на изборима", *Блиц*, 19.03.2018, Internet, https://www.blic.rs/vesti/svet/trampov-tim-je-ukrao-podatke-50-miliona-ljudi-na-fejsbuku-da-bi-pobedio-na-izborima/yt5y2y0, 08/04/2018.

14) Миленко Бајић, „Како је 50 милиона корисника Фејсбука несвесно увучено у тајни програм шпијунаже", *Блиц*, 20.03.2018, Internet, https://www.blic.rs/vesti/svet/kako-je-50-miliona-korisnika-fejsbuka-nesvesno-uvuceno-u-tajni-program-spijunaze/cwkf67n, 09/04/2018.

15) Исто.

сервиса као што су *Instagram* или *What's Up*. Према наводима Гардијана, Фејсбук је објавио да ће независни тим дигиталних форензичара спровести истрагу и покушати да установи да ли компанија „Кембриџ аналитика" и даље располаже спорним подацима. У саопштењу компаније наводи се да „уколико подаци и даље постоје, то би било тешко кршење правила коришћења" и да је реч о „неприхватљивом кршењу поверења и обавеза".[16]

Афера је проузроковала оштру реакцију у САД, тако да је група америчких сенатора позвала Марка Закерберга да сведочи пред Конгресом на који начин компанија Фејсбук прикупља личне податке од корисника, односно о методама заштите личних података. До тога је дошло у априлу ове године, када је Закерберг више часова одговарао на питања о скандалу који је погодио ову компанију.

Разуме се, афера није мимоишла ни Европски парламент који је најавио спровођење истраге у овом случају. У том погледу, председник Европског парламента Антонио Тајани потврдио је да Европски парламент намерава да спроведе пуну истрагу у вези са злоупотребом личних података, истакавши да „наводи о злоупотреби података корисника Фејсбука представља неприхватљиво кршење права наших грађана на приватност".[17]

Имајући у виду скандал у вези са компанијама Фејсбук и Кембриџ аналитика, примена нове Опште уредбе о заштити података у ЕУ долази до пуног изражаја.

3. ОСНОВНА РЕШЕЊА ОПШТЕ УРЕДБЕ О ЗАШТИТИ ПОДАТАКА

Општа уредба о заштити појединаца у вези са обрадом личних података и о слободном кретању таквих података, те о стављању ван снаге Директиве 95/46/ЕЗ (Општа уредба о заштити података)[18] (у даљем тексту: Уредба) се примењује на обраду личних података која се у целини обавља аутоматизовано, као и на неаутоматизовану обраду личних података који чине део система похране или су намењени да буду део тог система.

16) Исто.

17) Танјуг, „Тајани: Европски парламент ће спровести истрагу о злоупотреби података са Фејсбука", *Блиц*, 20.03.2018, Internet, https://www.blic.rs/vesti/svet/tajani-evropski-parlament-ce-sprovesti-istragu-o-zloupotrebi-podataka-sa-fejsbuka/cfs6hb1, 08/04/2018.

18) 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), OJ L 119, 4.5.2016, p. 1–88. Уредба ступа на снагу 25. маја 2018. године.

Поменута Уредба се не примењује у одређеним случајевима. Пре свега, Уредба се не примењује на обраду личних података током делатности која није обухваћена опсегом права Уније. Друго, Уредба се неће применити ни у случају обраде личних података када државе чланице обављају активности које су обухваћене подручјем примене главе V поглавља 2. УЕУ. Треће, Уредба се не примењује ни у погледу обраде личних података коју спроводи физичко лице током искључиво личних или кућних активности. Најзад, Уредба се не односи ни на обраду личних података коју обављају надлежна тела у сврху спречавања, истраге, откривања или прогона кривичних дела или извршавања кривичних санкција, укључујући заштиту од претњи јавној безбедности и њиховог спречавања.[19]

Ratio legis Опште уредбе је да се подигне ниво поверења корисника из Европске уније у сервисе информационог друштва, уз заштиту њихових фундаменталних права.[20] С обзиром да је реч о Уредби, она ће се непосредно примењивати у државама чланицама ЕУ, без обавезе да се примени кроз доношење појединачних прописа у државама чланицама.

Посебно важан део Уредбе се односи на њено *територијално важење*. Наиме, ова Уредба се односи на обраду личних података у оквиру активности пословног седишта водитеља обраде или извршиоца обраде у Унији, независно од тога обавља ли се обрада у Унији или не. Такође, Уредба се примењује на обраду личних података испитаника у Унији коју обавља водитељ обраде или извршилац обраде без пословног седишта у Унији, ако су активности обраде повезане са нуђењем робе или услуга таквим испитаницима у Унији (независно од тога треба ли испитаник извршити плаћање), или праћењем њиховог понашања док год се њихово понашање одвија унутар Уније. Ова се Уредба примењује на обраду личних података коју обавља водитељ обраде који нема пословно седиште у Унији, већ на месту где се право државе чланице примењује на основу међународног јавног права.[21] Из овога следи да се Уредба може применити и у случају када извршилац обраде поседује у својој збирци податке које се односе на лице које има држављанство неке од чланица Уније.

19) Уредба, чл. 2.

20) Gregory Voss, "Looking at European Union Data Protection Law Reform Through a Different Prism: the Proposed EU General Data Protection Regulation Two Years Later", *Journal of Internet Law*, Vol. 17, No. 9/2014, стр. 13, преузето из: Дејан Ђукић, „Заштита података о личности са освртом на ново законодавство Европске уније у овој области", *Правни записи*, Универзитет Унион, Београд, Год. VIII, бр. 1/2017, стр. 55.

21) Уредба, чл. 3.

У Уредби су дефинисана и *начела обраде личних података*. У том смислу, лични подаци морају бити: а) законито, поштено и транспарентно обрађивани с обзиром на испитаника; б) прикупљени у посебне изричите и законите сврхе те се даље не смеју обрађивати на начин који није у складу са тим сврхама; даља обрада у сврхе архивирања у јавном интересу, у сврхе научног или историјског истраживања или у статистичке сврхе не сматра се неусклађеном са првобитним сврхама („ограничавање сврхе“); в) примерени, релевантни и ограничени на оно што је нужно у односу на сврхе у које се обрађују („смањење количине података“); г) тачни и према потреби ажурни; мора се предузети свака разумна мера ради обезбеђења да се лични подаци који нису тачни, узимајући у обзир сврхе у које се обрађују, без одлагања избришу или исправе („тачност“); д) чувани у облику који омогућава идентификацију испитаника само онолико дуго колико је потребно у сврхе ради којих се лични подаци обрађују; лични подаци могу се похранити на дужа раздобља ако ће се лични подаци обрађивати искључиво у сврхе архивирања у јавном интересу, у сврхе научног или историјског истраживања или у статистичке сврхе, што подлеже спровођењу примерених техничких или организационих мера прописаних овом Уредбом ради заштите права и слобода испитаника („ограничење похрањивања“); ђ) обрађивани на начин којим се обезбеђује одговарајућа сигурност личних података, укључујући заштиту од неовлашћене или незаконите обраде или од случајног губитка, уништења или оштећења применом одговарајућих техничких или организационих мера („целовитост и поверљивост“). Водитељ обраде је одговоран за усклађеност са овим начелима и мора бити у стању да то докаже („поузданост“).[22]

У члану 6. Уредбе се говори о условима који се морају испунити да би обрада података била законита. У том смислу, обрада је *законита* само ако и у оној мери у којој је испуњен најмање један од следећих услова: а) испитаник је дао сагласност за обраду својих личних података у једну или више посебних сврха; б) обрада је нужна за извршавање уговора у којем је испитаник странка или како би се предузеле радње на захтев испитаника пре склапања уговора; в) обрада је нужна ради поштовања правних обавеза водитеља обраде; г) обрада је нужна како би се заштитили кључни интереси испитаника или друга физичка лица, д) обрада је нужна за извршавање задатака од јавног интереса или при извршавању службених овлашћења водитеља обраде; ђ) обрада је нужна за потребе легитимних интереса водитеља обраде или треће стране,

22) Уредба, чл. 5.

осим када су од тих интереса јачи интереси или темељна права и слободе испитаника који захтевају заштиту личних података, посебно ако је испитаник дете.[23]

Кад је реч о деци, у члану 8. Уредбе се наводи да је обрада личних података детета законита ако дете има најмање 16 година, а ако је дете испод 16 година старости таква је обрада законита само ако и у мери у којој је пристанак дао или одобрио носилац родитељске одговорности над дететом. Државе чланице могу у те сврхе предвидети нижу старосну границу, под условом да таква нижа старосна граница није нижа од 13 година.[24] Ова одредба је јако значајна, с обзиром да велики број деце користи Фејсбук и игра видео-игре, па се поставља питање на који начин ће руковаоци података прикупити сагласности од њихових родитеља, односно старалаца.

Такође, Уредбом је забрањена *обрада личних података* који откривају расно или етничко порекло, политичка мишљења, верска или филозофска уверења или чланство у синдикату те обрада генетских података, биометријских података у сврху јединствене идентификације појединца, података који се односе на здравље или података о полном животу или сексуалној оријентацији појединца. Ипак, под одређеним условима поменута забрана се неће примењивати.[25]

Посебна новина у Уредби у односу на ранију Директиву је везана за *право на брисање („право на заборав")*. Поменуто право је проистекло из европске праксе у случају Гугл Шпанија[26] и подразумева да испитаник има право од водитеља обраде затражити брисање личних података који се на њега односе без непотребног одлагања, а водитељ обраде има обавезу да обрише личне податке без непотребног одлагања уколико је испуњен један од следећих услова: а) лични подаци више нису нужни у односу на сврхе за које су прикупљени или на други начин обрађени; б) испитаник повуче сагласност на којој се обрада заснива у складу са чланом 6. ставом 1. тачком а) или чланом 9. ставом 2. тачком а) и ако не постоји друга правна основа за обраду; в) испитаник уложи приговор на обраду у складу са чланом 21. ставом 1 те не постоје јачи легитимни разлози за обраду, или испитаник уложи приговор на обраду у складу са

23) Уредба, чл. 6.

24) Уредба, чл. 8.

25) Уредба, чл. 9.

26) Daphne Keller, *The Right Tools: Europe's Intermediary Liability Laws and the 2016 General Data Protection Regulation*., 2017. стр. 22-26. Internet, https://law.stanford.edu/publications/the-right-tools-europes-intermediary-liability-laws-and-the-2016-general-data-protection-regulation/, 25/04/2018.

чланом 21. ставом 2; г) лични подаци су незаконито обрађени; д) лични подаци морају се брисати ради поштовања правне обавезе из права Уније или права државе чланице којем подлеже водитељ обраде; ђ) лични подаци прикупљени су у вези с понудом услуга информационог друштва из члана 8. става 1.[27]

Дакле, право на брисање би се могло раздвојити на три категорије: 1) право да се изврши брисање након одређеног периода, 2) право да одређено лице може да има чисту прошлост и 3) право да подаци о одређеном лицу буду повезани са актуелним информацијама, те да се уклони повезаност са подацима који су застарели.[28]

Посебно интересантан део Уредбе односи се на *пренос личних података трећим земљама или међународним организацијама*. У том погледу, сваки пренос личних података који се обрађују или су намењени за обраду након преноса у трећу земљу или међународну организацију одвија се једино ако, у складу са другим одредбама ове Уредбе, водитељ обраде и извршилац обраде делују у складу са условима из овог поглавља који важе и за даље преносе личних података из треће земље или међународне организације у још једну трећу земљу или међународну организацију. Пренос личних података трећој земљи или међународној организацији може се, према Уредби, догодити када Комисија одлучи да трећа земља, подручје, или један или више одређених сектора унутар те треће земље, или међународна организација о којој је реч обезбеђује примерен ниво заштите. Такав пренос не захтева посебно одобрење.[29]

Комисија након процене примерености степена заштите може одлучити да трећа земља, подручје, или један или више одређених сектора унутар треће земље, или међународна организација обезбеђује примерен ниво заштите. Предвиђено је постојање механизма за периодично преиспитивање. Најмање сваке четири године, којим ће се узети у обзир сви релевантни догађаји у тој трећој земљи или међународној организацији. Уколико доступне информације откривају да трећа земља, подручје или један или више одређених сектора унутар треће земље, или међународна организација више не обезбеђује примерен ниво заштите у мери у којој је то потребно, Комисија ће одговарајућим актом ставити ван снаге, изменити или суспендовати одлуку без ретроактивног ефекта. У службеном листу Европске уније Комисија објављује попис трећих земаља, подручја и одређених сектора унутар треће земље

27) Уредба, чл. 17.

28) Michael Rustad, Sanna Kulevska, "Reconceptualizing the Right to Be Forgotten to Enable Transatlantic Data Flow", *Harvard Journal of Law & Technology*, Harvard Law school, Cambridge, Vol. 28, No. 2/2015, стр. 349.

29) Уредба, чл. 45, ст. 1.

и међународних организација у погледу којих је донела одлуку да не обезбеђују одговарајући ниво заштите или да је више не обезбеђују.[30]

Ако није донета одлука на основу члана 45. става 3. Уредбе, водитељ обраде или извршилац обраде трећој земљи или међународној организацији личне податке могу пренети само ако је водитељ обраде предвидео одговарајуће заштите мере и под условом да су испитаницима на располагању спроводљива права и ефикасна судска заштита. Све пресуде суда или све одлуке управног тела треће земље којима се од водитеља обраде или извршитеља обраде захтева пренос или откривање личних података могу бити признате или извршиве на било који начин само ако се заснивају на неком међународном споразуму, попут уговора о узајамној правној помоћи, који је на снази између треће земље која је поднела захтев и Уније или државе чланице, не доводећи у питање друге разлоге за пренос.[31]

Ако не постоји одлука о примерености у складу са чланом 45. ставом 3. Уредбе, или одговарајуће заштитне мере у складу са чланом 46. Уредбе, што укључује обавезујућа корпоративна правила, пренос или скуп преноса личних података у трећу земљу или међународну организацију остварује се само под једним од следећих услова: а) испитаник је изричито пристао на предложени пренос након што је био обавештен о могућим ризицима таквих преноса за испитаника због непостојања одлуке о примерености и одговарајућих заштитних мера; б) пренос је нужан за извршавање уговора између испитаника и водитеља обраде или спровођење предуговорних мера на захтев испитаника; в) пренос је нужан ради склапања или извршавања уговора склопљеног у интересу испитаника између водитеља обраде и другог физичког или правног лица; г) пренос је нужан из важних разлога јавног интереса; д) пренос је нужан за постављање, остваривање или одбрану правних захтева; ђ) пренос је нужан за заштиту животно важних интереса испитаника или других лица ако испитаник физички или правно не може дати пристанак; е) пренос се обавља из регистра који према праву Уније или праву државе чланице служи пружању информација јавности и који је отворен на увид јавности или било ком лицу које може доказати неки оправдани интерес, али само у мери у којој су испуњени сви услови прописани у праву Уније или праву државе чланице за увид у том посебном случају.[32]

30) Уредба, чл. 45, ст. 3, 5 и 8.

31) Уредба, чл. 46. и 48.

32) Уредба, чл. 49.

4. ПРОБЛЕМ ЕКСТЕРИТОРИЈАЛНОСТИ ОПШТЕ УРЕДБЕ О ЗАШТИТИ ПОДАТАКА

Дакле, може се закључити да Уредба има за циљ усаглашавање заштите личних података у ЕУ. Осим тога, примећује се да је Унија, доношењем нове регулативе, настојала да постигне интернационализацију заштите података о личности, имајући у виду да је интернет постао доступан корисницима широм света. На тај начин, обезбеђење адекватне обраде и чувања података постало је један од примарних задатака националних тела држава чланица ЕУ.

С обзиром да је претходно важећа Директива 95/46/ЕС садржала недостатке у погледу територијалне примене, за њу се не може рећи да представља правни оквир којим би се на ефикасан начин обезбедила заштита личних података корисника, имајући у виду члан 16. Уговора о функционисању Европске уније. То посебно важи код мултинационалних компанија као што су Гугл или Фејсбук, имајући у виду да се седишта њихових управа налазе ван ЕУ, у САД. С обзиром да су поменуте компаније у прошлости одбијале да поштују прописе ЕУ у области заштите података, нова Уредба има проширену територијалну примену. У том смислу, примена Уредбе и ван граница Уније проузроковала је многобројне дилеме у њеној примени.

Као што је већ поменуто, члан 3. став 2. Уредбе поставља својеврстан темељ за екстериторијалну примену Уредбе, јер се у њему наводи да ће Уредба да се примењује на обраду личних података испитаника у Унији коју обавља водитељ обраде или извршилац обраде *без пословног седишта у Унији*, ако су активности обраде повезане са *нуђењем робе или услуга* таквим испитаницима у Унији (независно од тога треба ли испитаник извршити плаћање), или *праћењем њиховог понашања* док год се њихово понашање одвија унутар Уније. Дакле, применом правила *lex loci solutionis* долази се до решења да за примену ове Уредбе уопште није неопходно да извршилац обраде има седиште на територији Уније.

Уколико се пажња усмери на део члана 3. става 2. Уредбе у коме се говори о *нуђењу роба или услуга*, а у вези са тачком 23. Уредбе, да би се утврдило нуди ли водитељ обраде или извршилац обраде робу или услуге испитаницима који се налазе у Унији, потребно је утврдити да ли је очигледно да водитељ обраде или извршилац обраде намерава понудити услуге испитаницима који се налазе у једној или више држава чланица Уније. Притом, у обзир се узимају фактори као што су коришћење језика или валуте који су генерално у употреби у једној или више држава чланица са мо-

гућношћу наручивања робе и услуга на том другом језику, или помињање купаца или корисника који се налазе у Унији. С друге стране, за утврђивање намере нису довољни (пасивни) чиниоци, као што су доступност интернет страна водитеља обраде, извршиоца обраде или посредника у Унији, као ни адресе електронске поште и других контактних података, или коришћење језика који је генерално у употреби у трећој држави у којој водитељ обраде има седиште.

На овај начин, Уредба би се могла применити на ситуације када се нуде бесплатне услуге од стране интернет претраживача или друштвених мрежа, као што су компаније Фејсбук или Гугл, али би се Уредба несумњиво могла применити и на компаније из трећих земаља које не нуде своје услуге корисницима у Унији. Примера ради, уколико би носилац података у ЕУ „букирао" путовање у Калифорнији у САД, користећи се веб-сајтом путничке агенције из САД који је вишејезичан (на енглеском, француском, шпанском или немачком језику) и омогућава плаћање аранжмана и у еврима, тада би се Уредба применила и на овај случај, премда су релевантна услуга и плаћање извршени на територији САД.[33]

Проблем око екстериторијалности Уредбе се додатно усложњава ако су активности обраде повезане са праћењем понашања испитаника док год се њихово понашање одвија унутар Уније. У складу са тачком 23. Уредбе, како би се одредило може ли се активност обраде сматрати праћењем понашања испитаника, треба се утврдити прати ли се појединац на интернету међу осталим могућом накнадном употребом техника обраде личних података које се састоје од израде профила појединца, нарочито ради доношења одлука које се на њега односе, или ради анализе или предвиђања његових личних склоности, понашања и ставова.

Из овога следи да би на удару Уредбе могле да се нађу и компаније из трећих земаља које пружају услуге друштвених мрежа, или *e-mail* услуга, користећи се притом такозваним „колачићима" (*cookies*) који служе за праћење понашања корисника, праћење посета одређених веб-сајтова, и слично. Ово је посебно карактеристично за компаније попут Гугла или Фејсбука, које се обилато користе овим текстуалним датотекама које се чувају у веб-прегледачу, чиме обезбеђују средства за финансирање својих бесплатних услуга корисницима. Случај Фејсбука и Кембриџ аналитике и коришћење података у политичке сврхе је додатно указао на опасност овакве праксе.

33) О овоме видети шире: Paul de Hert, Michal Czerniawski, "Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context", *International Data Privacy Law*, Oxford University Press, Oxford, Vol. 6, No. 3/2016, стр. 230–243.

Међутим, не може се из овога закључити да би се Уредба применила само на велике компаније, попут Фејсбука. Уредба би се, свакако, могла применити и на било коју интернет компанију на свету, односно провајдера интернет услуга (који користи „колачиће"), чији би испитаник који је лоциран у Унији посетио веб-сајт компаније која је лоцирана у трећој земљи. Из овога следи да би се Уредба могла применити на *интернет у целини*, чим би носилац података био стациониран на територији Уније.

Још један проблем који се јавља у вези са применом Уредбе односи се на *потенцијалну немогућност њене потпуне примене у пракси*. Иако је према правилима међународног јавног права државама дозвољено да доносе прописе који би се могли односити и на случајеве који су се догодили ван њихових територија, то не значи да се ти прописи могу ефективно примењивати ван државне територије. С обзиром на екстериторијалност Уредбе, односно проширење домашаја правила о заштити личних података Уније и ван њених граница, извлачи се закључак да ће примена Уредбе бити врло тешка.

То се посебно односи на ситуацију када је реч о мултинационалним компанијама, као што су Гугл или Фејсбук. У том погледу, поставља се питање како решити питање *сукоба закона*, до кога може доћи услед екстериторијалности Уредбе? Наиме, за компанију која има седиште у САД у овом случају би се примењивала два правна режима – америчко законодавство у области заштите личних података и Уредба ЕУ. Којем од ова два прописа дати предност, уколико се узме у обзир да прописи могу садржати различита, неретко супротстављена решења, као и чињеницу да су европски прописи у области заштите података строжи од америчких. На овај начин, екстериторијално важење Уредбе доводи до повећаног нивоа правне несигурности, јер би субјекти на које се примењују ови прописи дошли у дилему који пропис их обавезује. То се посебно односи на санкције које предвиђају прописи. Уколико се компанија определи за један пропис, постоји реална опасност да ће јој бити изречена санкција која је у складу са другим прописом, и обрнуто. Због тога је неопходно разрешити овај, вештачки изазван, сукоб закона. Заиста, уколико европски туриста обавља куповину на петој авенији у Њујорку, не могу се пронаћи ваљани разлози зашто би обрада његових података у овом контексту требала *ex lege* да потпада под територијални домашај Уредбе. У таквој ситуацији, постоји врло јака веза између носиоца података и права САД (територијални принцип), а недовољна повезаност са правним режимом ЕУ.[34]

34) Paul de Hert, Michal Czerniawski, "Expanding the European data protection scope beyond

Имајући наведено у виду, на законодавцу је да направи својеврсни „баланс" између потребе да се Уредба ефективно примењује у територијалном смислу, узимајући у обзир дигитално доба и свеприсутност интернета и потребе да се обезбеди правна сигурност за ентитете и лица ван ЕУ који обрађују личне податке појединаца у ЕУ.[35] У противном, прети опасност да ће се нова Уредба моћи применити ван ЕУ у „црном или белом облику" („*black or white fashion*", превод аутора), без сигурносних вентила који би могли да спрече преклапање јурисдикција.[36] Проблем лежи и у нивоу *стандарда за заштиту личних података* у САД и у ЕУ. За разлику од Европске уније, где је Уредба поставила „златни стандард" права заштите података који представља рационално оправдање легитимности екстериторијалне примене Уредбе и фундаментално људско право загарантовано Уговором о функционисању ЕУ, дотле је стандард заштите података у САД нижи, и не представља фундаментално право, већ је заштита података ствар грађанског права. Стога, оно што је са европске (ЕУ) тачке гледишта низак ниво заштите података, то је са америчког становишта адекватан ниво заштите.

Један од начина на који би се могао решити овај комплексан проблем екстериторијалне примене Уредбе би било индивидуално, добровољно, спровођење одредаба о заштити података садржаних у Уредби од стране мултинационалних компанија као што су Фејсбук или Гугл, с обзиром на њихову жељу да и даље буду присутни на унутрашњем тржишту Европске уније.

Друга солуција би се могла пронаћи у закључењу посебних, *билатералних споразума* између Европске уније и трећих земаља (на пример са САД), чиме би се отклониле недоумице у погледу сукоба јурисдикција и повећао степен правне сигурности. На овај начин би се Уредба могла примењивати и у трећим земљама, које нису чланице ЕУ.

Проблем је у томе што се закључење оваквих споразума уопште не назире у ближој будућности, а ЕУ, чини се, не намерава да одустане од ефективне примене Уредбе и ван њене јурисдикције. Случај Фејсбука и Кембриџ аналитике је додатно подигао потребу за детаљним регулисањем ових питања. Најновији скандал у вези са злоупотребом личних података милиона корисника (поред оста-

territory: Article 3 of the General Data Protection Regulation in its wider context", нав. дело, стр. 230–243.

35) Исто.

36) Christopher Kuner, "Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law", *International Data Privacy Law*, Oxford University Press, Oxford, No. 5/2015, стр. 242.

лог, и у политичке сврхе) Фејсбука показао је да мултинационалне компаније нису претерано заинтересоване да се на њих примењују одредбе Опште Уредбе о заштити података. О томе сведочи недавна изјава Марка Закерберга да ће применити Уредбу на глобалном нивоу, према корисницима широм света. Тада је Закерберг, између осталог, изјавио да се још преговара о детаљима, али да би у том смеру, требало да иде цела ствар. Током испитивања пред америчким Конгресом, Закербергу је поново постављено питање да ли ће се Уредба примењивати на све кориснике Фејсбука. Његов одговор је био потврдан, али само што се тиче регулатива, не и мера заштите. Фејсбук је за Ројтерс рекао да свуда примењује исте мере заштите приватности, без обзира на то је ли реч о споразумима са *Facebook Incom* или са *Facebook* Ирском. Компанија је додала да је нова промена извршена само јер закон ЕУ захтева специфичан језик у правилима о приватности, који амерички закон нема. Међутим, компанија Фејсбук је пренела одговорност за све кориснике ван САД, Канаде и ЕУ са свог међународног седишта у Ирској на главну канцеларију у Калифорнији. То значи да ће ти корисници сада бити на страницама које се уређују америчким, а не ирским прописима. Слично је најавила и компанија *Linkedln*, која треба да премести своје кориснике који нису у земљама чланицама ЕУ у своју америчку подружницу. Након афере Кембриџ аналитика, Фејсбук је представио пакет мера које корисницима омогућавају остваривање права у складу са Уредбом, као што је преузимање и брисање података те нове контроле сакупљања података.[37]

Овакав поступак компаније Фејсбук сведочи о томе да екстериторијална примена Уредбе, дакле, ван ЕУ, уопште није примамљива мултинационалним компанијама (и не само њима), поготово имајући у виду високе казне за кршење њених одредаба, при чему су предвиђене казне до 4 одсто глобалног саобраћаја, што би у случају Фејсбука износило око 1,6 милијарди америчких долара. Друго, очигледно је да ће глобалне компаније, као што је Фејсбук „бежати" у државе где се примењује блажи правни режим у погледу заштите личних података. Треће, афера око Кембриџ аналитике је свакако дубоко пољуљала поверење обичних корисника друштвених мрежа у безбедност њихових података на интернету, али и указала на много озбиљнију појаву обраде личних података корисника у политичке сврхе. На крају, један од основних недостатака нове Уредбе о заштити података лежи и у чињеници

37) Tportal.hr, „ФБ пребацио 1,5 милијарду корисника ван досега нових прописа", *Б92*, 19.04.2018, Internet, https://www.b92.net/tehnopolis/vesti.php?yyyy=2018&mm=04&nav_id=1383424, 01/05/2018.

да њоме нису обухваћени различити интернет претраживачи, *Big Data*, *Cloud Computing*, *Ubiquitous Computing*, што ће представљати озбиљан проблем и добру подлогу за неку нову аферу попут Кембриџ аналитике. Све у свему, чини се да ће у будућности бити много изазова у вези са заштитом личних података, не само у Европској унији, већ и шире.

ЛИТЕРАТУРА

Миленко Бајић, „Како је 50 милиона корисника Фејсбука несвесно увучено у тајни програм шпијунаже", *Блиц*, 20.03.2018, Internet, https://www.blic.rs/vesti/svet/kako-je-50-miliona-korisnika-fejsbuka-nesvesno-uvuceno-u-tajni-program-spijunaze/cwkf67n, 09/04/2018.

Балтезаревић Весна, Балтезаревић Радослав, „Заштита приватности на интернету – европски модел", *Мегатренд ревија*, Универзитет Џон Незбит, Београд, Вол. 14, бр. 1/2017, стр. 241-252.

Домазет Синиша, Скакавац Здравко, „Добросуседски односи на Балкану као услов за приступање Европској унији: препрека или добра пракса?", *Српска политичка мисао*, Институт за политичке студије, Београд, бр. 3/2016, стр. 139-155.

Ђукић Дејан, „Заштита података о личности са освртом на ново законодавство Европске уније у овој области", *Правни записи*, Универзитет Унион, Београд, Год. VIII, бр. 1/2017, стр. 49-60.

Ђурић Милорад, Глобалне комуникације и светско друштво: проблем легитимацијског дефицита, *Српска политичка мисао*, Институт за политичке студије, Београд, бр. 02/2016, 43-59.

Каурин Тања, Ануцојић Драган, Скакавац Здравко, „Дифузија моћи у сајберпростору: изазов или претња безбедности", у монографији: *Савремени изазови међународне безбедности*, (приредио: Слободан Марковић), Факултет за правне и пословне студије др Лазар Вркатић, Универзитет Унион, Београд и Центар за међународне студије, Загреб, 2017, стр. 141-168.

Тањуг, „Тајани: Европски парламент ће спровести истрагу о злоупотреби података са Фејсбука", *Блиц*, 20.03.2018, Internet, https://www.blic.rs/vesti/svet/tajani-evropski-parlament-ce-sprovesti-istragu-o-zloupotrebi-podataka-sa-fejsbuka/cfs6hb1, 08/04/2018.

Танјуг, „Трампов тим је украо податке 50 милиона људи на Фејсбуку да би победио на изборима, *Блиц*, 19.03.2018. Internet, https://www.blic.rs/vesti/svet/trampov-tim-je-ukrao-podatke-50-miliona-ljudi-na-fejsbuku-da-bi-pobedio-na-izborima/yt5y2y0, 08/04/2018.

Baltezarević Vesna *et al.*, "Human need for communication in the system of virtual organizations", *Egyptian Computer Science Journal*, Vol. 40, No. 1/2016, стр. 53-60.

BBC news, „Afera Fejsbuk-Kembridž analitika: Šta sve znamo do sada",

Internet, https://www.danas.rs/bbc-news-serbian/afera-fejsbuk-kembridz-analitika-sta-sve-znamo-do-sada/, 08/04/2018.

Boyd Danah, Hargittai Eszter, *Facebook privacy settings: Who cares?*, Internet, http://firstmonday.org/ojs/index.php/fm/article/view/3086/2589, 25/04/2018.

De Hert Paul, Czerniawski Michal, "Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context", *International Data Privacy Law*, Oxford University Press, Oxford, Vol. 6, No. 3/2016, стр. 230–243.

Keller Daphne, *The Right Tools: Europe's Intermediary Liability Laws and the 2016 General Data Protection Regulation*., 2017. стр. 22-26. Internet, https://law.stanford.edu/publications/the-right-tools-europes-intermediary-liability-laws-and-the-2016-general-data-protection-regulation/, 25/04/2018.

Kosinski Michal, Stillwell David, Graepel Thore, "Private traits and attributes are predictable from digital records of human behavior", *Proceedings of the National Academy of Sciences,* Vol. 110, No. 15/2013, стр. 5802-5805.

Kuner Christopher, "Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law", *International Data Privacy Law*, Oxford University Press, Oxford, No. 5/2015, стр. 235-245.

Lampe Cliff, Ellison Nicole, Steinfield Charles, *Changes in use and perception of Facebook*, Internet, http://www-personal.umich.edu/~enicole/LampeEllisonSteinfield2008.pdf, 25/04/2018.

Nauka kroz priče, „Pet dimenzija Kembridž analitike", Internet, https://naukakrozprice.rs/pet-dimenzija-kembridz-analitike/, 06/04/2018.

Norberg Patricia, Horne Daniel, Horne David, "The privacy paradox: Personal information disclosure intentions versus behaviors", *Journal of Consumer Affairs*, George Washington University School of Business, Vol. 41, No. 1/2007, стр. 100-126.

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), OJ L 119, 4.5.2016, p. 1–88.

Rustad Michael, Kulevska Sanna, "Reconceptualizing the Right to Be Forgotten to Enable Transatlantic Data Flow", *Harvard Journal of Law & Technology*, Harvard Law school, Cambridge, Vol. 28, No. 2/2015, стр. 349-417.

Tportal.hr, „ФБ пребацио 1,5 милијарду корисника ван досега нових прописа", *Б92*, 19.04.2018, Internet, https://www.b92.net/tehnopolis/vesti.php?yyyy=2018&mm=04&nav_id=1383424, 01/05/2018.

Young Alison, Quan-Haase Anabel, "Privacy protection strategies on Facebook: the Internet privacy paradox revisited", *Information, Communication & Society*, UK, No.. 16(4)/2013, стр. 479-500.

Sinisa Domazet, Zdravko Skakavac

“CAMBRIDGE ANALYTICA” SCANDAL – NEW CHALLENGE IN PERSONAL DATA PROTECTION?

Resume

In this paper we analyzed the affair in relation to the companies Facebook and Cambridge Analytica, in the light of new EU regulations in the field of data protection (GBER). The analysis showed that there is a great need for more effective protection of personal data of users on the Internet. Also, the analysis showed how abuses of personal data are carried out. Bearing in mind that the new Regulation can be applied beyond the borders of the European Union, it has been pointed out several key issues regarding its extraterritorial application. First, it was found that in practice there are difficulties regarding the implementation of the Regulation. Second, the analysis showed that in the case of extraterritorial application of the Regulation the problem of the conflict of jurisdictions occurs. Third, mechanisms for resolving conflicts between the laws of different countries are not sufficiently developed. Solution is the conclusion of bilateral international agreements between the EU and third countries. This would enable the implementation of the Regulation in countries which are not members of the Union. The research used normative methods and legal and logical methods of induction and deduction.

Keywords: law, politics, security, EU, data protection

* Овај рад је примљен 01. маја 2018. године, а прихваћен на састанку Редакције 26. јуна 2018. године.