Др Ана Човић, виша научна сарадница
Института за упоредно право у Београду

УДК: 341.645(4-672EU):316.77:004.738.5
DOI:

ПРЕНОС ЛИЧНИХ ПОДАТАКА НАКОН ОДЛУКЕ ЕВРОПСКОГ СУДА ПРАВДЕ *SCHREMS II*[*]

Резиме

У раду ће бити анализирана пресуда Европског суда правде из јула 2020. године, којом је пренос личних података Европљана у САД проглашен незаконитим. „Штит приватности" је правни оквир за регулисање трансатлантске размене личних података у комерцијалне сврхе између Европске уније и Сједињених Држава, који је америчким властима дозвољавао прикупљање личних података о субјектима у Европској унији, међутим без одговарајућих заштитних мера, наводи се у пресуди Суда. Из Фејсбука, незадовољни пресудом, значајном за мултинационалне компаније, истичу да ће заустављање преноса података имати негативне последице на резултате циљаног онлајн оглашавања, чији је обим последњих година значајно повећан. Утврђено је да принципи америчког "Штита приватности" нису усаглашени са европским законима, ни са Европском општом уредбом о заштити података (GDPR), те да су стога неважећи. Ова пресуда утиче на сваку америчку компанију, не само на Фејсбук и Инстаграм, па ће последице њеног доношења осетити и фирме попут Гугла и Амазона. У међувремену се поставило и питање утицаја ове пресуде на пренос података у друге државе, попут Кине и Русије, нарочито када се говори о преносу путем актуелне друштвене мреже ТикТок, путем технологије кинеске компаније Huawei и Yandex такси апликације.

***Кључне речи:** Европски суд правде, Фејсбук, Schrems II, заштита података.*

1. Увод

Наша приватност обухвата податке који се односе на наше брачно стање, верска и политичка убеђења, новчане трансакције, етничко порекло, здравствено стање, криминални досије, генетски материјал. Одлука Европске

[*] Рад је написан у оквиру Програма истраживања Института за упоредно право у Београду за 2022. годину који се финансира из средстава Министарства просвете, науке и технолошког развоја Републике Србије.

комисије број 2016/1250 која се односи на примереност заштите приватности, (*Privacy Shield*, споразум закључен између Европске комисије и америчког Министарства трговине о заштити личних података који се из Европске уније преносе у САД)[1], поништена је дана 16. јула 2020. године пресудом број *C - 311/18 (Data Protection Commissioner vs. Facebook Ireland Limited and Maximilian Schrems). Privacy Shield* датира из 2016. године када је пресудом *Schrems I* број *C - 362/14 (Maximilian Schrems vs. Data Protection Commissioner),* закључено да основна људска права нису довољно заштићена правним оквиром из 2000. године, када је Европска комисија у Одлуци број 2000/520 навела да САД гарантује примерен ниво заштите за пренос личних података грађана Европске уније. Повод за покретање судског поступка била је афера изазвана признањем *Edwarda Snowden*-а о деловању америчких тајних служби и њиховом прикупљању личних података, након чега је *Maximilian Schrems* затражио од надзорног тела у Ирској *(Data Protection Commissioner)* да забрани компанији Фејсбук пренос његових личних података у САД, због могућих злоупотреба и недовољног степена заштите. Аутори Дилигенски и Прља наводе да се "дигитална неписменост" огледа и у олаком приступању Фејсбуку и дељењу личних информација, и закључују да право у овој области касни за развојем технологије.[2]

Питање преноса личних података након одлуке *Schrems II*, интересантно је и из разлога што у нашој земљи велики број компанија преноси податке о личности у САД, у склопу послова које обављају. Компанија која контролише централизоване базе података на нивоу мултинационалне компаније, често се налази у САД. На територији САД налазе се и сервери многих компанија које корисницима пружају могућност коришћења друштвених мрежа и различитих популарних апликација.

Ова судска одлука својим домашајем утиче на велики број организација на територији Европске уније које су у пословном смислу повезане са САД, због чега је Европски одбор за заштиту података закључио да је неопходно прецизирати и објаснити све могуће недоумице у вези са њеном применом. У најновијем документу, дати су одговори на најчешћа питања у вези са овим случајем и кроз једанаест питања одговорено је на који начин и под којим условима се пренос личних података из Европске уније може вршити на територију САД. *Schrems II* је несумњиво важна одлука чији је циљ заштита субјеката података ЕУ од прекорачења овлашћења националне безбедности трећих земаља, међутим њене последице могу бити и многи потенцијални проблеми у области међународног преноса података. Хиљаде малих и средњих предузећа широм Сједињених Држава и Европе суочавају се са високим трошковима као последицом одлуке Европског суда правде да поништи

[1] Privacy Shield Framework. Доступно на https://www.privacyshield.gov/welcome

[2] Видети Дилигенски, А., Прља, Д., *Фејсбук: Заштита података и судска пракса*. Београд, 2018.

споразум ЕУ - САД *Privacy Shield*, због чега је неопходан нови правни оквир који би законски заштитио личне податке грађана ЕУ приликом њиховог преноса у САД. Наводи се да су заштита приватности и токови података одиграли кључну улогу у трансатлантском трговинском и иновацијском односу од 7,1 билион долара, што указује на хитност успостављања новог правног оквира од стране европских и америчких креатора политике.[3]

2. Правни оквир за заштиту личних података и права на приватност

Европски правни оквир за заштиту личних података и права на приватност се заснива на чл. 8 Европске конвенције о људским правима[4], чл. 15 Европске конвенције о људским правим[5] (слични њему су чл. 4 Међународног пакта о грађанским и политичким правима и чл. 27 Америчке конвенције о људским правима), као и чл. 17 Међународног пакта о грађанским и политичким правима, који произилази из чл. 12 Универзалне декларације о људским правима, којим се успоставља заштита од "произвољног или незаконитог уплитања" у „приватност, породицу, дом или преписку појединца.“

Конвенција о заштити лица у односу на аутоматску обраду личних података[6] у чл. 6 утврђује да се лични подаци у вези са расним пореклом, политичким опредељењем, верским убеђењем или неком другом врстом убеђења, као и лични подаци у вези са здравственим стањем или сексуалним животом могу аутоматски обрађивати само у случају да домаће законодавство

[3] Cory, N., Castro, D., Dick, E. V., *Schrems II': What Invalidating the EU-U.S. Privacy Shield Means for Transatlantic Trade and Innovation*, Information Technology & Innovation Foundation, 2020.

[4] Гарантује се право на поштовање приватног и породичног живота, дома и преписке, и прописује обавеза јавних власти да се не мешају у остваривање овог права, осим ако је то у складу са законом и неопходно у демократском друштву у интересу националне сигурности, јавне сигурности или економске добробити земље, ради спречавања нереда или криминала, заштите здравља или морала, права и слободе других. Закон о ратификацији Европске конвенције за заштиту људских права и основних слобода, Службени лист Србије и Црне Горе - међународни уговори, бр. 9/2003, 5/2005 и 7/2005 - кор. и Службени гласник РС - Међународни уговори, бр. 12/2010 и 10/2015.

[5] Прецизира се да у време рата или друге ванредне ситуације која прети животу нације, свака Висока уговорна страна може предузети мере одступања од својих обавеза из ове Конвенције у мери коју строго захтевају потребе ситуације, под условом да такве мере нису у супротности са њеним другим обавезама по међународном праву.

[6] Службени лист СРЈ - Међународни уговори, бр. 1/92, Службени лист СЦГ - Међународни уговори, бр. 11/2005 -др. закон и Сл. гласник РС -Међународни уговори, бр. 98/2008 - др. закон и 12/2010).

предвиђа одговарајуће гаранције за то, што важи и за личне податке из казнене евиденције.[7]

У Европској унији је од 2016. године на снази Општа уредбе о заштити података о личности (Уредба (ЕУ) 2016/679 *GDPR*)[8] и Директива о заштити физичких лица у вези са обрадом података о личности који су повезани са кривичним делима или извршењем кривичних санкција (ЕУ) 2016/680.[9] Обрада личних података мора да се заснива на сагласности субјекта података или на другим законским основама које су утврђене чланом 6 Уредбе, а став је да „ако се сагласност састави као део одредаба и услова који се не преговарају, претпоставља се да нису слободно дати" (чл. 29, Смернице за сагласност, 2018).

Када говоримо о националном правном оквиру за заштиту личних података и права на приватност, све одредбе о људским и мањинским правима тумаче се у корист унапређења вредности демократског друштва и у складу са важећим међународним стандардима и праксом међународних институција у овој области. Члан 18 Устава Републике Србије (Сл. гласник РС, бр. 98/2006) прописује да се људска и мањинска права зајемчена Уставом примењују непосредно, док се законом може прописати само начин њиховог остварења када је то Уставом изричито предвиђено или када је неопходно због природе појединог права, када се ни у ком случају не сме утицати на његову садржину.[10] Право је сваког грађанина да захтева судску заштиту и уклањање последица које су том приликом настале, уколико сматра да му је повређено или

[7] Свих 47 земаља Савета Европе су стране у овој Конвенцији (Конвенција 108), која је отворена и за државе које нису чланице Савета Европе. Она је ажурирана 2018. године (данас је позната као 108+) и њу су потписале све државе Савета Европе. Наша држава је 26. маја 2020. године ратификовала Протокол Савета Европе од 18. маја 2018. којим се ова Конвенција унапређује у погледу начела пропорционалности, законитости и транспарентности (Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No.223). Конвенцију је потписала Русија, али не и Кина. Више о томе: Човић, А., *Право на приватност и заштита личних података у доба пандемије COVID - 19*, *Социолошки преглед*, бр. 3/2020, стр. 672-673.

[8] 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.

[9] Directive EU 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

[10] Ограничења ових права су допуштена законом, у случајевима и у обиму који то Устав предвиђа, без задирања у њихову суштину, а достигнути ниво људских и мањинских права се не може смањивати (чл. 20. Устава РС). У истом члану се наводи да су сви државни органи, а посебно судови, дужни да у овим ситуацијама воде рачуна да ли постоји сразмера између ограничења права и сврхе, односно да ли се сврха могла остварити и мањим ограничењем.

ускраћено право зајемчено Уставом, а на располагању му стоји и могућност обраћања међународним институцијама. Неповредивост тајне писама и других средстава комуницарања је неповредива и заштићена чл. 41, а заштита података о личности се јемчи чл. 42 Устава.[11] Такође, утврђује се право сваке особе да буде обавештена о прикупљеним подацима о својој личности, као и право на судску заштиту у случају њихове злоупотребе.[12]

У Закону о заштити података о личности (Службени гласник РС, бр. 87/2018), чл. 18 прецизира се да је обрада коју врше надлежни органи у посебне сврхе, којом се открива расно или етничко порекло, политичко мишљење, верско или филозофско уверење или чланство у синдикату, као и обрада генетских података, биометријских података у циљу јединствене идентификације физичког лица, података о здравственом стању или података о сексуалном животу или сексуалној оријентацији физичког лица, допуштена само ако је то неопходно, уз примену одговарајућих мера заштите права лица на које се подаци односе. Ovaj закон је у складу са *GDPR* и дозвољава пренос података о личности у другу државу, у неким случајевима, уз сагласност Повереника за информације од јавног значаја и заштиту података о личности.

3. Тумачење пресуде *Schrems II* од стране Европског одбора за заштиту података - одговори на најчешћа питања

У складу са одредбама Закона о заштити података о личности, Одлуком Владе РС (Службени гласник Р", бр. 55/19) пренос података организацијама у САД у оквирима *Privacy Shiel*d утврђен је као пренос уз обезбеђивање примереног нивоа заштите с аспекта домаћег закона, на основу Одлуке Европске комисије о примерености заштите успостављене у оквиру ЕУ - САД. Међутим, након неважности ове одлуке, више се не обезбеђује примерени ниво заштите ни са аспекта Закона о заштити података о личности РС, због чега је неопходно пронаћи други основ преноса у складу са нашим законодавством. Повереник за информације од јавног значаја и заштиту података о личности Републике Србије, упутио је допис Влади РС у циљу усаглашавања Одлуке Владе РС (Службени гласник РС, бр. 55/19). На питање у које се све земље из Србије преносе подаци о личности, из канцеларије Повереника су одговорили да од почетка примене Закона о заштити података о личности у августу 2019. године, није издато ниједно одобрење за пренос података у друге државе, те да овај орган не може

[11] Прописује се да је забрањена 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 државе, на начин предвиђен законом.

[12] Одступања од зајемчених права су дозвољена за време ванредног стања или ратног стања у обиму у којем је то неопходно, а престају престанком ванредног или ратног стања (чл. 202. Устава РС).

имати сазнања у које се све земље тренутно преносе подаци о личности, будући да се пренос података може вршити и у другим случајевима прописаним Законом, без посебног одобрења.[13] Ово питање свакако захтева детаљнију анализу у оквиру ширих јавних расправа, имајући у виду да је у оквиру договора између *Huawei* и Србије увелико инсталирано више од хиљаду камера са техником препознавања лица, чини се, без довољне транспарентности целог поступка, уз фаворизовање сигурности у односу на приватност, што у одређеним кризним ситуацијама може бити изузетно опасан модел поступања. То нам је показало и деловање већег броја влада у свету и активности које су предузимане током двогодишње пандемије, нарочито када говоримо о апликацијама за праћење контаката заражених и увођењу ковид пропусница, будући да смо сведочили до сада невиђеном поништавању основних људских права и права на приватност, што је за последицу имало бројне протесте широм света и урушавање већ пољуљаног поверења у државне институције.

У документу Европског одбора за заштиту података[14] усвојеном 23. јула 2020. године наводи се да је у својој пресуди, Суд испитао валидност Одлуке Европске комисије 2010/87 о стандардним уговорним клаузулама[15] и навео да њена ваљаност, зависи од тога да ли Одлука 2010/87 укључује ефикасне механизме који омогућавају да се обезбеди усклађеност са нивоом заштите који је суштински једнак оном који у ЕУ гарантује *GDPR*. Стандардна уговорна клаузула која служи да обезбеди ниво заштите једнак оном који гарантује Општа уредба о заштити података, најчешће се користи као мера преноса података, односно механизам који компаније које подлежу *GDPR*-у могу да користе у циљу обављања законитих међународних трансфера података, уколико се прималац података налази у земљи која не пружа адекватан ниво заштите. С тим у вези, Суд посебно истиче да Одлука 2010/87 намеће обавезу извознику података и примаоцу података („увознику података“) да провере, пре сваког преноса и преузимања, узимајући у обзир околности преноса, да ли се тај ниво заштите поштује у трећој земљи. Увозник података је дужан да обавести извозника података о било каквој немогућности да се придржава стандардних клаузула о заштити података, и извозник података је тада обавезан да обустави пренос података и/или да раскине уговор са увозником података. Због свега наведеног, Суд је сматрао да захтеви домаћег закона САД, а посебно одређени

[13] Комарчевић, Д., Живановић, М., *Заштита података без 'Штита приватности' и у Србији*, Радио Слободна Европа, 24. август 2020, доступно на https://www.slobodnaevropa.org/a/zaštita-podataka-bez-štita-privatnosti-i-u-srbiji/30799807.html

[14] Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems. Доступно на https://edpb.europa.eu/our-work-tools/our-documents/other/frequently-asked-questions-judgment-court-justice-european-union_en

[15] Standard Contractual Clauses (SCC). Standard contractual clauses for data transfers between EU and non-EU countries. Доступно на https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

програми који омогућавају приступ јавним властима САД личним подацима који се преносе из ЕУ у САД у сврхе националне безбедности, резултирају ограничењима. Стандардне уговорне клаузуле *(SCC)* које су до сада коришћене, измењене су Проведбеном одлуком Комисије (ЕУ) 2021/914 од 4. јуна 2021. о стандардним уговорним клаузулама за пренос личних података у треће земље у складу са Уредбом (ЕУ) 2016/679 Европског парламента и Савета.[16] Нове стандардне уговорне клаузуле су у складу са Општом уредбом о заштити података и узимају у обзир ставове Европског суда правде у пресуди *Schrems II* и званично су у примени од 27. септембра 2021. године. Оне сада прецизно дефинишу одговорност увозника и извозника података, али и подобрађивача у зависности од тога која је страна оштећеном лицу нанела материјалну/нематеријалну штету.

Када се поставља питање утицаја ове пресуде на пренос података у друге државе, попут Кине и Русије, што је важно нарочито уколико имамо у виду да у Кини постоји обавеза компанија из сектора информационих технологија да податке дају властима на њихов захтев, може се закључити да иако се пресуда односи на размену података са Сједињеним Државама, део у коме се говори о стандардним уговорним клаузулама може се применити и на друге државе. Власти у Литванији су упозориле грађане да не инсталирају апликацију *Yandex*, због незаконитог прикупљања података о личности и њиховог чувања на серверима организације са седиштем у Русији, након чега би исти могли бити достављени јавним органима, регулаторним органима, судовима и другим трећим странама.[17]

Генерално, за треће земље, праг који је одредио Суд такође се примењује на све одговарајуће заштитне мере према чл. 46 *GDPR*-а које се користе за пренос података у било коју трећу земљу, а прелазни период током којег би било дозвољено да се настави са преносом података у САД, без процене правне основе за пренос, не постоји, будући да је Суд поништио Одлуку о заштити приватности без задржавања њених ефеката, јер амерички закон не пружа суштински једнак ниво заштите. Ова процена се мора узети у обзир за било какав трансфер у САД. Уколико су преношени подаци америчком увознику података који поштује *Privacy Shield*, трансфери на основу овог законског оквира били би свакако незаконити.

Суд је утврдио да амерички закон - Одељак 702 Закона о надзору страних обавештајних служби *(FISA - Foreign Intelligence Surveillance Act)* и Извршна наредба *"EO" 12333*, не обезбеђују суштински једнак ниво заштите. Суд наглашава да одређени програми надзора који омогућавају приступ јавних власти САД личним подацима пренетим из ЕУ у САД, у сврхе националне

[16] Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.
[17] Комарчевић, Д., Живановић, М., *нав. дело*.

безбедности, не предвиђају никаква ограничења овлашћења која су дата властима САД, нити постојање гаранција за потенцијално циљане особе које нису из САД. Надзор није неопходан нити сразмеран, мишљење је Суда. Одељак 702 *FISA* примењује се на све „провајдере електронских комуникационих услуга“, док *EO 12 333* организује електронски надзор, који се дефинише као „прибављање нејавне комуникације електронским путем без пристанка неког лица у електронској комуникацији или, у случају неелектронске комуникације, без пристанка лица које је видљиво присутно на месту комуникације, али не укључујући употребу радио-уређаја само за одређивање локације предајника” (3.4; б)). Може се рећи да је Суд идентификовао Одељак 702 Закона о надзору страних обавештајних служби (*FISA*) и Извршну наредбу 12333, као несагласне са правима загарантованим Повељом ЕУ, иако Влада САД оспорава основаност овог документа, наводећи да Суд за надзор страних обавештајних служби САД активно прати да ли америчке обавештајне агенције правилно циљају појединце како би добили обавештајне информације, а такође САД закони, укључујући *FISA* и Закон о административним поступцима, дозвољавају страним држављанима да траже обештећење у случају повреде права, пред америчким судовима кроз грађанске тужбе.[18] Поједини аутори истичу да је ЕУ - САД *Privacy Shield* успоставио вишу основу за трансатлантске токове података, због чега креатори политике ЕУ и САД треба да препознају да је то био напор учињен у ”доброј вери многих фирми укључених у *Privacy Shield*, и позитиван укупни резултат у смислу побољшане приватности комерцијалних података и дигиталне трговине.”[19] Извештај Организације за економску сарадњу и развој *(OECD)* под називом „Трговина и прекогранични токови података“, у коме је анкетирано 259 фирми (са седиштем у 48 земаља, углавном у ЕУ, Јапану и Сједињеним Државама), показао је да је за фирме из свих сектора скуп и компликован поступак раздвајања личних и неличних података, а без оквира *Privacy Shield*, организацијама постаје још скупље и компликованије да схвате које су мере заштите неопходне.[20]

Када се говори о другим алатима за пренос према чл. 46 *GDPR*, пресуда појашњава да је стандард за одговарајуће заштитне мере у чл. 46 *GDPR* стандард „суштинске еквиваленције“, а с обзиром на то да се чл. 46 појављује у петом поглављу *GDPR*-а, сходно томе, мора се читати у светлу чл. 44. *GDPR*-а, који прописује да се „све одредбе тог поглавља примењују како се не би нарушио ниво заштите физичких лица гарантован том уредбом”.

Када се поставља питање да ли је могуће ослонити се на једно од одступања приликом преноса података у САД, одговор је да је и даље могуће пренети податке из ЕУ у САД на основу одступања предвиђених у чл. 49 *GDPR*-а под

[18] Cory, N., Castro, D., Dick, E. V., *нав. дело*, https://itif.org/publications/2020/12/03/schrems-ii-what-invalidating-eu-us-privacy-shield-means-transatlantic
[19] *Исто*.
[20] *Исто*.

условом да се примењују услови наведени у овом члану. Посебно треба подсетити да када се пренос заснива на пристанку субјекта података, он треба да буде: експлицитан, специфичан за одређени пренос података или скуп трансфера и субјект података мора бити информисан, посебно о могућим ризицима преноса (што значи да субјект података такође треба да буде обавештен о посебним ризицима који произилазе из чињенице да ће његови подаци бити пренети у земљу која не пружа адекватну заштиту и не спроводи адекватне заштитне мере у циљу заштите података).

У вези са трансферима неопходним из важних разлога од јавног интереса (који морају бити признати у праву ЕУ или држава чланица), суштински услов за примену овог одступања јесте утврђивање важног јавног интереса, и иако ово одступање није ограничено на преносе података који су „повремени", то не значи да се пренос података на основу значајног одступања од јавног интереса може одвијати у великом обиму и на систематичан начин, већ је уместо тога, потребно поштовати општи принцип према којем дерогације наведене у чл. 49 *GDPR*-а не треба да постану „правило" у пракси, већ се морају ограничити на специфичне ситуације.

Треба имати у виду да је неопходно обезбедити овлашћење и за извршитеље обраде када поверавају подизвршитељима обраде пренос података у треће земље, а будући да велики избор рачунарских решења може да подразумева пренос личних података у трећу земљу (нпр. за потребе складиштења или одржавања), треба бити опрезан.

Ако се подаци могу пренети у САД, а не могу се предвидети никакве додатне мере како би се осигурало да амерички закон не утиче на суштински еквивалентан ниво заштите, нити се примењују одступања према чл. 49 *GDPR*-а, једино решење представља преговарање о измени или допунској клаузули уговора о забрани преноса у САД. Подаци не би требало само да се чувају, већ би њима требало и да се управља из неке друге државе, а уколико се могу пренети у неку другу земљу, треба проверити и њено законодавство, односно да ли је оно у складу са захтевима Суда и са очекиваним нивоом заштите личних података. Ако се не може пронаћи одговарајући основ за трансфер у трећу земљу, лични подаци не би требало да се преносе ван територије ЕЕП и све активности обраде треба да се одвијају у ЕЕП.

Може се претпоставити да ће већина корисника *Privacy Shield*, са обе стране Атлантика, бити значајно погођена због ограничених ресурса и стручности, неопходних за управљање поступцима усклађивања са међународним законима.

4. Закључак

Данас заштита приватних података и контролисање њихових токова, добијају сасвим нову димензију, будући да је неопходно да знамо не само са ким ми делимо наше податке, него и ко је овлашћен да их прикупља и у које сврхе. Законодавац је препознао ову област као једну од суштинског значаја у

последњој деценији, што је за последицу имало усвајање посебних закона којима се регулише заштита и остваривање овог права. Друштвене мреже, финансијске трансакције, плаћања путем интернета, и друге активности којима приступамо у виртуелном свету, повећали су могућност да појединац и његова приватност у сајбер простору буду угрожени на различите начине – путем прислушкивања, ширења вируса, изложености вербалном насиљу, до крађе идентитета.

Појединци заштиту од злоупотребе података о личности често траже пред Европским судом за људска права, као и пред Судом правде ЕУ.[21]

У образложењу пресуде *Schrems II*, широка и непрецизна овлашћења јавних власти у Сједињеним Државама у области обраде личних података кроз успостављене системе надзора и недостатак ефикасне правне заштите за лица ван Сједињених Држава и даље представљају ризик обраде личних података у САД. Наиме, акти које су надлежни органи САД донели у правцу ограничавања овлашћења обавештајних служби, по оцени суда, нису довели до увођења принципа пропорционалности и експедитивности као темељних европских принципа заштите права на приватност појединаца. Извоз података из Србије у САД сада се налази под посебним режимом, у складу са степеном усклађености српског законодавства са правним тековинама ЕУ и *GDPR* Уредбом.

Ако се одредбе *GDPR*-а примењују на компанију која има седиште у Србији, постоји обавеза коришћења нових *SCC* приликом извоза личних података у оне земље које не пружају довољан ниво заштите. Уколико је фирма регистрована у Србији и *GDPR* је не обавезује, али се подаци добијају из ЕУ, и обрађују у улози примаоца података, *SCC* би морале да се примене у пословном односу са партнерима из ЕЕП.

Поједини аутори истичу да су постојале алтернативне одлуке којима је Суд могао избећи "трансатлантски сукоб који је резултирао, те да без обзира на тачност пресуде Суд није био приморан да пресуди на тај начин, због чега је могао да усвоји помирљивији став."[22]

Такође, спекулише се да ли пресуда може довести до тога да се неке треће земље запитају "да ли је вредно настојати да се постигну стандарди заштите података ЕУ, упуштати се у дуготрајне преговоре само да би се споразум, или одлука о адекватности заснована на њему, касније поништили."[23]

---

[21] Видети Андоновић, С, Прља, Д., *Основи права заштите података о личности*, Београд, 2020, стр. 190-197.

[22] Atik, J., Groussot, X. A., *Weaponized Court of Justice in Schrems II*, Nordic Journal of European Law, no. 2/2021, p. 4.

[23] Murphy, H., M., *Assessing the Implications of Schrems II for EU - US Data Flow*, International & Comparative Law Quarterly, Volume 71, Issue 1, January 2022, p. 261. DOI: https://doi.org/10.1017/S0020589321000348

Без обзира на опречна мишљења, несумњиво се може закључити да је ЕУ у овом случају преузела иницијативу у циљу заштите људских права на приватност од државе. Међутим, да би се људи заштитили од масовног надзора, ”неопходни су усаглашенији глобални стандарди заштите података, проналажење равнотеже између приватности и безбедности, али и приватности и економске димензије међународног преноса података.”[24]

Тако, аутор *Rotenberg* сматра неопходним доношење свеобухватног закона о приватности од стране Конгреса САД, успостављање независне агенције за заштиту података и обавезу ратификације Конвенције Савета Европе 108, будући да је заједнички приступ у интересу и Европе и САД, као два кључна трговинска партнера.[25]

Судском одлуком *Schrems II* дугорочно ће највише бити погођена мала и средња предузећа, што ће довести до смањеног обима њиховог учешћа у трговини, као и до смањене конкурентности и могућности да опстану, нарочито ако имамо у виду да је током последње пандемије, али и у садашњем постпандемијском периоду, дигитална трговина робом и услугама доживела значајну експанзију и развој. Са друге стране, да ли ће заштита личних података грађана бити заиста унапређена овом пресудом Суда, у друштву ”великог брата” које нам се уводило стидљиво и на мала врата до почетка пандемије, а данас је наша реалност, питање је за неку ширу дискусију.

Ana Čovic, Ph.D., Senior Research Associate
Institute of Comparative Law in Belgrade

TRANSFER OF PERSONAL DATA AFTER THE DECISION OF THE EUROPEAN COURT OF JUSTICE *SCHREMS II*

Summary

The paper will analyze the judgment of the European Court of Justice from July 2020, which declared the transfer of personal data of Europeans to US illegal. The "Privacy Shield" is the legal framework for regulating the transatlantic exchange of personal data for commercial purposes between the European Union and the United

[24] Stehlik, V., Vardanyan, L., *Schrems II: Will it really increase the Level of Privacy Protection against Mass Surveillance? Bratislava Law Review* 4(2), p. 125. DOI: 10.46282/blr.2020.4.2.215

[25] Видети Rotenberg, M., *Schrems II, from Snowden to China: Toward a new alignment on transatlantic data protection*, European Law Journal, no. 26(1-2), DOI: 10.1111/eulj.12370

States, which allowed US authorities to collect personal data about entities in the European Union, but without adequate safeguards, the court said. From Facebook, dissatisfied with the verdict, which is important for multinational companies, they point out that stopping the transfer of data will have negative consequences on the results of targeted online advertising. It was determined that the principles of the American "Privacy Shield" are not in line with European laws, nor with the European General Data Protection Regulation (GDPR), and that they are therefore invalid. This verdict affects every American company, not only Facebook and Instagram, so the consequences of its adoption will be felt by companies such as Google and Amazon. In the meantime, the question of the impact of this verdict on the transfer of data to other countries, such as China and Russia, was raised, especially when it comes to transmission via the current social network TikTok or through the technology of the Chinese company Huawei, and Yandex taxi applications.

Keywords: *European Court of Justice, Facebook, Schrems II, data protection.*

Литература

Андоновић, С., Прља, Д., *Основи права заштите података о личности,* Београд, 2020.

Atik, J., Groussot, X., A *Weaponized Court of Justice in Schrems II*, Nordic Journal of European Law, no. 2/2021. DOI: 10.36969/njel.v4i2.23778

Дилигенски, А., Прља, Д., *Фејсбук: Заштита података и судска пракса*. Београд, 2018.

Murphy, H., M., *Assessing the Implications of Schrems II for EU - US Data Flow*, *International & Comparative Law Quarterly,* Volume 71, Issue 1, 2022. DOI: https://doi.org/10.1017/S0020589321000348

Rotenberg, M., *Schrems II, from Snowden to China: Toward a new alignment on transatlantic data protection*, European Law Journal, no. 26(1-2), DOI: 10.1111/eulj.12370

Stehlik, V., Vardanyan, L., *Schrems II: Will it really increase the Level of Privacy Protection against Mass Surveillance? Bratislava Law Review* 4(2). DOI: 10.46282/blr.2020.4.2.215

Cory, N., Castro, D., Dick, E. V., *'Schrems II': What Invalidating the EU-U.S. Privacy Shield Means for Transatlantic Trade and Innovation*, Information Technology & Innovation Foundation, 2020.

Човић, А., *Право на приватност и заштита личних података у доба пандемије COVID-19*, Социолошки преглед, бр. 3/2020, DOI: https://doi.org/10.5937/socpreg54-27284

Правни извори

Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

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

Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems. Доступно на https://edpb.europa.eu/our-work-tools/our-documents/other/frequently-asked-questions-judgment-court-justice-european-union_en

Закон о ратификацији Европске конвенције за заштиту људских права и основних слобода, Службени лист Србије и Црне Горе - међународни уговори, бр. 9/2003, 5/2005 и 7/2005 - кор. и Службени гласник РС - Међународни уговори, бр. 12/2010 и 10/2015.

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

Конвенција о заштити лица у односу на аутоматску обраду личних података, Службени лист СРЈ -Међународни уговори, бр. 1/92, Службени лист СЦГ - Међународни уговори, бр. 11/2005 -др. закон и Сл. гласник РС -Међународни уговори, бр. 98/2008 - др. закон и 12/2010).

Privacy Shield Framework. Доступно на https://www.privacyshield.gov/welcome

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.

Standard Contractual Clauses (SCC). Standard contractual clauses for data transfers between EU and non-EU countries. Доступно на https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

Устав Републике Србије, Сл. гласник РС, бр. 98/2006.

Интернет извори

Комарчевић, Д., Живановић, М., *Заштита података без 'Штита приватности' и у Србији*, Радио Слободна Европа, 24. август 2020, доступно на https://www.slobodnaevropa.org/a/zaštita-podataka-bez-štita-privatnosti-i-u-srbiji/30799807.html