UDK: 342.738(4-672EU)
Biblid: 1451-3188, 19 (2020)
God XIX, br. 73-74, str. 41–59
DOI: https://doi.org/10.18485/iipe_ez.2020.19.73_74.3

Originalan naučni rad
Primljen 23.09.2020.
Odobren 11.10.2020.

GRANICE VANTERITORIJALNOG DEJSTVA OPŠTE UREDBE O ZAŠTITI PODATAKA EVROPSKE UNIJE

*Mihajlo VUČIĆ**

Apstrakt: Opšta uredba o zaštiti podataka EU (GDPR) utiče na standarde zaštite podataka u drugim pravnim sistemima zbog svog vanteritorijalnog dejstva. Privlačnost poslovanja na unutrašnjem tržištu glavni je razlog što strane kompanije, koje u svojim poslovnim operacijama koriste lične podatke građana EU, ili lica sa prebivalištem u EU, pristaju da se podvrgavaju njenim odredbama. Na taj način dolazi do proširenja nadležnosti EU i izvan njene teritorije. Vanteritorijalno delovanje organa jedne suverene nadležnosti nije načelno zabranjeno međunarodnim pravom, ali stvara praktične probleme u primeni i izvršenju, kao i otpore drugih suverenih nadležnosti, koje mogu da polažu jače pravo na regulisanje datog pravnog odnosa. Zaključivanjem međunarodnih ugovora kojima se regulišu problemi vanteritorijalne nadležnosti između zainteresovanih strana, ovi problemi se otklanjaju. Međutim, pravo na zaštitu ličnih podataka koje štiti GDPR je koncipirano kao ljudsko pravo, koje mora biti apsolutno zaštićeno, što automatski poništava dejstvo zaključenih ugovora. Sud pravde EU pokazuje spremnost da brani apsolutnost ovog prava. U radu se postavlja pitanje da li privlačnost unutrašnjeg tržišta zajedno sa koncepcijom prava na zaštitu podataka kao ljudskog prava može da nametne model zaštite podataka u EU kao globalni model. Ističe se da države koje su ekonomski dovoljno moćne, čak i ako dele vrednosti zaštite ljudskih prava sa EU, mogu da odole vanteritorijalnom dejstvu GDPR-a, što pokazuje analizirani slučaj odnosa EU–SAD. Međutim, pravi problem nastaje kada dođe do sukoba nadležnosti sa ekonomskom silom koja ima potpuno drugačiji vrednosni pogled od EU na zaštitu podataka i ljudska prava uopšte (Kina). U tom smislu, u radu se zaključuje da vanteritorijalno dejstvo GDPR-a može da dovede do širenja modela zaštite podataka u EU najviše u okviru bloka srodnih pravnih sistema, pogotovo što zaštita podataka postaje u savremenim međunarodnim odnosima ne samo ekonomski nego sve više i bezbednosni problem.

Ključne reči: GDPR, vanteritorijalnost, zaštita podataka, pravo na privatnost, EU

---

* Naučni saradnik, Institut za međunarodnu politiku i privredu, Beograd. Rad je objavljen u okviru projekta „Srbija i izazovi u međunarodnim odnosima 2020. godine“.

1) UVOD

Živimo u eri sveopšte digitalizacije komunikacija i podataka koji se u komunikacijama razmenjuju. Internet i ostale komunikacijske tehnologije, poput društvenih mreža, postale su sveprisutne i njihovo pravno regulisanje dobija na značaju iz dana u dan. Istovremeno, društvene mreže i tokovi podataka na njima prevazilaze mogućnosti regulisanja unutar nacionalno omeđenih teritorija zbog svoje fluidne prirode koja im omogućava da neprestano prelaze državne granice. Naša komunikacija nije samo digitalizovana već i deteritorijalizovana, praktično globalna. Globalna pitanja zahtevaju globalni odgovor. Međutim, globalnog zakonodavca koji bi regulisao tokove komunikacija i sa njima povezana pitanja nema, niti će ga u skorije vreme biti. Takođe, do nekog opšteg međunarodnog ugovora, koji bi postavio pravila igre za sve u globalnom digitalnom prostoru, trenutno je teško doći zbog neslaganja velikih sila oko suštinskih načela na kojima bi se ta pravila zasnivala. Teren je prepušten unutrašnjim pravnim sistemima da pronađu rešenje. Države se, u skladu sa svojim interesima zaštite suvereniteta i teritorijalnog integriteta, opredeljuju na jednostrane poteze, primenjujući svoje zakone i na aktivnosti koje se odvijaju i izvan državne teritorije, ukoliko se posledice tih aktivnosti mogu odraziti na tu teritoriju ili stanovnike koji je naseljavaju. Teritorijalnost prerasta u vanteritorijalnost. Evropska unija nije izuzetak od ovih trendova. Naprotiv, vanteritorijalna primena propisa o zaštiti podataka EU – najpre Direktive o zaštiti podataka, a od 2018. godine i nove Opšte uredbe o zaštiti podataka (GDPR),[1] – postala je sinonim za vanteritorijalno delovanje zbog inherentne snage uticaja koju sa sobom nosi na druge pravne sisteme. Ta snaga se ogleda, pre svega, u privlačnosti unutrašnjeg tržišta EU, prepunog dobrostojećih potrošača sa kojim svaka kompanija u svetu želi da posluje.

Na koje podatke se odnosi GDPR? GDPR štiti lične podatke subjekata koji se nalaze u EU od zloupotrebe onih stranih entiteta koji te podatke obrađuju zbog prodaje roba i usluga subjektima u EU, ili radi posmatranja njihovog ponašanja (član 3.2). Takođe, GDPR dozvoljava prenos podataka izvan EU u neku treću državu (ili međunarodnu organizaciju), samo ukoliko ta država ima odgovarajuće standarde zaštite podataka, pri čemu o tim standardima odlučuje Komisija EU (čl. 45(1)). Na prvi pogled odredbe GDPR deluju savršeno legitimno i nesporno – jedan poseban pravni sistem kao što je EU želi da zaštiti svoje građane i teritoriju od postupaka koji nisu u skladu sa vrednostima na kojima se taj pravni poredak zasniva (u ovom slučaju prava na privatnost i zaštitu podataka o ličnosti kao ljudskog prava). Međutim, da bi GDPR efikasno štitio ljudska prava građana EU, on mora da počne

[1] 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), 2016 O.J. (L 199) 1.

da reguliše aktivnosti pravnih lica koja uopšte nisu deo pravnog sistema EU – stranih kompanija koje dolaze do tih ličnih podataka i koriste ih u svojim poslovnim aktivnostima. U tom trenutku, pravni sistem EU počinje da deluje vanteritorijalno i može da dođe u sukob sa nekim drugim pravnim sistemom, na primer onim u kome je data kompanija osnovana i koji ne mora da ima iste standarde o zaštiti podataka kao što ima GDPR.

U ovom procesu koji je dovoljno opisan u teoriji,[2] nameće se mnogo raznovrsnih pitanja. Da li je legitimno da u situacijama sukoba nadležnosti između sistema sa različitim standardima zaštite GDPR deluje vanteritorijalno, i kako je to uopšte moguće a da se ne naruši integritet tog drugog pravnog sistema? Da li u tom trenutku ljudska prava koja su zaštitni objekt GDPR-a odnose prevagu nad suverenitom države čiji je pravni sistem pogođen delovanjem ove uredbe? Da li u tom trenutku EU postaje, kroz vanteritorijalno dejstvo svoje uredbe o zaštiti podataka, taj globalni zakonodavac koji svetu naše digitalizovane i deteritorijalizovane komunikacije tako nedostaje? U okviru ovog rada najpre ćemo ukratko objasniti funkcionalno delovanje vanteritorijalnog dejstva GDPR-a, kroz analizu odredaba same Uredbe, odluka Suda pravde EU koje su te odredbe tumačile, koncepciju prava na privatnost podataka kao ljudskog prava i teorije o nadležnosti međunarodnog prava (odeljak 2). Zatim ćemo izložiti praktične prepreke vršenju ove nadležnosti, kao i otpore koji nastaju zbog sukoba vanteritorijalnog vršenja nadležnosti sa drugim suverenim nadležnostima kroz studiju slučaja aranžmana za prenos podataka između SAD i EU (odeljak 3). U poslednjem odeljku analiziramo koji su dometi ovakvog modela zaštite podataka, i dodajemo kako je, pored tradicionalno navođenih razloga privlačnosti unutrašnjeg tržišta, u poslednje vreme pogotovo opasnost od alternativnih modela, poput kineskog, doprinela zbijanju redova i potrebi za ujednačavanjem sistema zaštite podataka u zemljama koje dele vrednosti ljudskih prava (odeljak 4). Na kraju rada donosimo određene zaključke u pogledu navedenih pitanja.

[2] Da navedemo samo nekoliko novijih radova: Indriana Pramesti, Arie Afriansyah, „Extraterritoriality of Data Protection: GDPR and Its Possible Enforcement in Indonesia", *Advances in Economics, Business and Management Research*, Volume 130, 2020, pp. 83-94; Bindu Samuel Ronald, Abhijit Vasmatkar, Shashikala Gurpur, "GDPR: Legal Impact on Extra – Territorial Commercial Pressure on Indian Business, Trade and Investment", *The Next Seven of the European Union*, Sofia University "St. Kliment Ohridski" and "Hanns Seidel" Foundation, Sofia, 2020, pp. 45-56; Manuel Klar, "Binding Effects of the European General Data Protection Regulation (GDPR) on U.S. Companies", *Hastings Science and Technology Law Journal*, Vol. 11, No. 2, 2020, pp. 100-153; Christopher Kuner, "The GDPR and International Organizations", *American Journal of International Law Unbound*, Vol. 114, 2020, pp. 15-19; Cedric Ryngaert, "Mistale Taylor, Symposium on the GDPR and International Law: The GDPR as Global Data Protection Regulation?", *American Journal of International Law Unbound*, vol. 114, 2020, pp. 5-9.

2) PRAVCI VANTERITORIJALNOG DELOVANJA GDPR-a

2.1. PROŠIRENA TERITORIJALNOST ILI VANTERITORIJALNOST?

Sud pravde EU je 2014. godine primenio propise o zaštiti podataka EU na jednog stranog provajdera u predmetu *Gugl Španija*. Tada važeća Direktiva o zaštiti podataka je primenjena na Gugl, američku kompaniju osnovanu po zakonima Sjedinjenih Američkih Država, na osnovu određenih „vezivnih tačaka" u procesu poslovanja Gugla za teritoriju EU.[3] Vezivna tačka za zasnivanje nadležnosti EU prema jednoj stranoj kompaniji je nađena u izrazu „*establishment*" – „ustanova", koji podrazumeva da neka poslovna organizacija, inače strano pravno lice u odnosu na EU, obavlja stvarne i efektivne aktivnosti na trajnoj osnovi u nekoj državi članici, te je time „ustanovljena" na teritoriji EU. Pritom, nije potrebno da ista ustanova vrši obradu podataka. Ukoliko obradu podataka vrši provajder koji nije „ustanovljen", ali se „obrada obavlja u kontekstu aktivnosti" ustanove, opet će obrada podlegati pravnom sistemu EU. U slučaju *Gugl Španija* Sud je smatrao da je aktivnost Gugl pretraživača neodvojiva od aktivnosti njegove ustanove Gugl Španija, jer se profit od aktivnosti pretraživača stvara putem oglasnog prostora, a taj pretraživač upravo omogućava da se obavljaju oglasne aktivnosti.[4]

Predmet spora bilo je tzv. „pravo na zaborav",[5] koje zbog svog obima može da ima značajne posledice po korisnike interneta i van teritorije EU. Usvajanjem Uredbe o zaštiti podataka taj široki domet prava EU je samo ojačan. Ono što se postavilo kao problem već u sporu *Gugl Španija*, i na šta je tužena kompanija ukazivala u svom podnesku, jeste problematična nadležnost za primenu propisa EU – drugim rečima njena „vanteritorijalnost".

[3] C-131/12, Google Spain Sl V. AEPD (THE DPA) & Mario Costeja Gonzalez, 13 May 2014.

[4] Ibid., para 55-56.

[5] Kod nas je o pravu na zaborav dosta pisano pa je tako na stranicama ovog časopisa navedeno kako je nakon ove presude Suda pravde EU „kompanija Google primila preko 40 hiljada zahteva za brisanje … (ličnih podataka) za svega nekoliko dana od postavljanja obrasca na internet" (postavljanje obrasca je bio jedan od zahteva iz presude), videti: Siniša Domazet, Zdravko Skakavac, „Pravo na zaborav i opšta uredba Evropske unije 2016/679 o zaštiti podataka o ličnosti", *Evropsko zakonodavstvo*, God. XVII, br. 66, 2018, str. 77. Videti više o pravu na zaborav i kod Sanja Prlja, „Pravo na zaštitu ličnih podataka u EU", *Strani pravni život*, br. 1, 2018, str. 89-99; takođe Andrej Diligenski, Dragan Prlja, Dražen Cerović, *Pravo zaštite podataka – GDPR*, Institut za uporedno pravo, Beograd, 2018.

Osnovi zasnivanja vanteritorijalne nadležnosti u međunarodnom pravu nisu nepoznati,[6] pogotovo u oblasti ljudskih prava.[7] Vanteritorijalna nadležnost je, međutim, u svetu suverenih teritorijalizovanih entiteta sa posebnim pravnim sistemima, sama po sebi problematičnog značenja. Zato se ona često maskira koncepcijama proširene teritorijalnosti. Sud pravde EU je u ovom sporu praktično tvrdio da teritorijalno primenjuje Direktivu o zaštiti podataka, jer je pronašao vezivnu tačku sa teritorijom u vidu ustanove Gugl Španija i sa njom povezanih aktivnosti. Ako se još jednom vratimo na tekst Uredbe o zaštiti podataka koji smo gore citirali, vidi se opet nastojanje da se vanteritorijalna primena na neki način teritorijalizira, jer se primena odredbi Uredbe na pravna lica koja nisu osnovana u EU opravdava njihovim dejstvom prema subjektima koji se nalaze unutar EU. U teoriji je ovaj proces poznat kao „doktrina dejstva".[8]

Bilo da je zovemo „vanteritorijalna primena" ili „teritorijalna primena na osnovu dejstva", posledice ovakve prakse primene propisa su u oba slučaja iste – unutrašnji pravni propisi obavezuju strane subjekte, što ih može dovesti u sukob sa nacionalnim propisima tih stranih subjekata. Specifičnost vanteritorijalne primene EU prava je njen potencijalno izuzetno veliki domet, zbog toga što na tržištu EU posluje praktično svaka bitnija kompanija u svetu. Što može dovesti do sukoba sa praktično svakom suverenom državom u svetu čiji subjekti učestvuju u spoljnotrgovinskim odnosima.

2.2. LJUDSKO PRAVO NA PRIVATNOST KAO UZROČNIK VANTERITORIJALNOG DEJSTVA

Čemu onda uopšte ideja zakonodavaca u EU da pokušaju da na taj način „prostru" dejstvo EU prava i potencijalno se sukobe sa celim svetom koji ne sledi njihove načine razmišljanja o zaštiti podataka? Uredba o zaštiti podataka štiti ona lica koja imaju državljanstvo EU ili prebivalište na njenoj teritoriji, a čiji se podaci

[6] Menno T. Kamminga, *Extraterritoriality*, Max Planck Encyclopedia of Public International Law, https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1040, 20.9.2020. Vanteritorijalna primena prava jedne države može da ide od onog klasičnog pristupa „čizme na zemlji" – gde se radi o primeni nacionalnog prava na pripadnike oružanih snaga jedne države koji obavljaju operacije u inostranstvu, pa do sofisticiranih vanteritorijalnih primena nacionalnog privrednog prava u oblasti regulisanja globalnog tržišta.

[7] Marko Milanović, *Extraterritorial Application of Human Rights Treaties: Law, Principles, and Policy*, Oxford, Oxford University Press, 2011.

[8] Stalni sud međunarodne pravde je u slučaju *Lotus* postavio temelje doktrini dejstva. U slučaju da postoje neke štetne posledice po interese države od aktivnosti koja se inače obavlja izvan državne teritorije, ne postoji pravilo međunarodnog prava koje zabranjuje državi da zasnuje vanteritorijalnu nadležnost, bilo da je ta nadležnost zakonodavna, upravna ili izvršna, videti: *Case of the Lotus (France v. Turkey*), Judgment, 1927 P.I.C.J. (ser. A) No.10, at 19 (Sept. 7).

prenose u nadležnost sistema koji ne ispunjavaju EU standarde zaštite podataka. Čini se da je *ratio* u želji da se pojedinačnim ljudskim pravima koja važe u EU obezbedi apsolutna zaštita, u svakom pojedinačnom slučaju kada ta prava mogu da uživaju lica koja imaju državljanstvo ili prebivalište na teritoriji EU, a istovremeno su im prava ugrožena ili povređena. U tom smislu vanteritorijalna nadležnost se od „teritorijalne nadležnosti na osnovu dejstva" pretvara u pasivnu personalnu nadležnost, poznatu u teoriji međunarodnog prava kao vrsta nadležnosti kojom države štite svoje građane od protivpravnih dela koja se prema njima čine u inostranstvu. U praksi se nastojanja EU da primeni svoje propise o zaštiti podataka praktično svode na kombinaciju teritorijalnog i pasivnog personalnog načela.

Kao što smo naveli, međunarodno pravo posmatra nadležnost kao oblast u kojoj vlada načelo „sve što nije zabranjeno je dozvoljeno", ako se ispune i dodatni uslovi da neka država trpi štetu po svoje interese od strane aktivnosti koja po čisto teritorijalnom shvatanju nadležnosti ne bi mogla da potpadne pod udar njenih organa i propisa. U tom smislu, EU bi mogla da proširi dejstvo svojih propisa o zaštiti podataka sve dotle gde bi mogla da opravda postojanje štete po svoje interese, a da se tom proširenju istovremeno ne suprotstavlja teritorijalno dejstvo nekog drugog pravnog sistema. Kvaka je u tome što je zaštita podataka u EU postavljena kao zaštita osnovnog ljudskog prava, koja organima EU ne daje samo mogućnost već i obavezu da vrše svoju nadležnost vanteritorijalno. Za razliku od međunarodnih ugovora o ljudskim pravima, kao što je Međunarodni pakt o građanskim i političkim pravima ili Evropska konvencija o ljudskim pravima, Povelja EU o osnovnim pravima nema klauzulu o ograničenju nadležnosti.[9] Naprotiv, teritorijalni limiti važenja osnovnih prava iz Povelje, kao što je pravo na zaštitu podataka iz člana 8, prate opseg nadležnosti organa EU i domen primene prava EU.[10] Tako da, barem teorijski gledano, manje su prepreke vanteritorijalne primene Povelje nego drugih međunarodnih ugovora o ljudskim pravima. Podsetimo, da je Evropski sud za ljudska prava zbog ograničenja nadležnosti iz Konvencije po kojoj sudi morao da osmisli prilično komplikovani i u praksi često različito tumačeni test „kontrole" nad protivpravnim aktom, kako bi obezbedio pripisivost radnje državi iako se radnja odvijala van njene teritorije.[11]

---

[9] Videti tekst Povelje: Charter of Fundamental Rights of the European Union, 2000 O.J. (C 364) 1 (Dec. 18, 2000).

[10] Videti više kod Violeta Moreno-Lax, Cathryn Costello, "The Extraterritorial Application of the EU Charter of Fundamental Rights: From Territoriality to Facticity, the Effectiveness Model", Steve Peers et al. (eds.) *The EU Charter of Fundamental Rights: A Commentary*, Hart/Beck/Nomos, 2014, p. 1662.

[11] Ograničenje nadležnosti u Konvenciji Saveta Evrope o osnovnim ljudskim pravima i slobodama nalazi se u članu 1: „Visoke strane ugovornice jemče svakome u svojoj nadležnosti prava i slobode određene u Delu I ove Konvencije". Što se tiče testa efektivne kontrole, videti predmete: *M. v. Denmark* (application no. 17392/90), 14 October 1992 (decision of the European

S obzirom na virtuelnu prirodu pretnji po lične podatke, u teoriji se ističe kako jedan analogni „virtuelni test kontrole" može da se primeni na slučajeve koje pokriva član 8 Povelje.[12] Po tom shvatanju, EU bi imala obavezu da deluje vanteritorijalno ako ima virtuelnu kontrolu nad podacima državljanina EU, ili lica sa prebivalištem na teritoriji EU. U meri u kojoj EU ima mogućnost da utiče na način na koji se podaci obrađuju u inostranstvu, ona bi morala da iskoristi taj uticaj kako bi obezbedila da podaci zaštićenog subjekta ne budu zloupotrebljeni. Takođe, EU ne bi smela da pomaže trećim stranama u njihovim aktivnostima kojima se podaci zloupotrebljavaju (obaveza poštovanja), odnosno trebalo bi da spreči treće strane da podatke zloupotrebe (obaveza zaštite). Na taj način se EU propisi o zaštiti podataka tumače kao zaštita osnovnog ljudskog prava državljana EU i lica koja imaju prebivalište na teritoriji EU od povreda tih prava koja vrše treće države i entiteti u trećim državama koji upravljaju tim podacima. Samo je po sebi razumljivo da ovako shvaćena Uredba o zaštiti podataka daje mnogo više razloga za vanteritorijalni aktivizam organima EU, jer bi se eventualnim propuštanjem da deluju i vanteritorijalno ti organi mogli izložiti pozivanju na odgovornost za povredu osnovnog ljudskog prava na zaštitu ličnih podataka.

3) OTPORI I PREPREKE VANTERITORIJALNOM DEJSTVU EU PROPISA

3.1. PRAKTIČNE TEŠKOĆE APSOLUTNE ZAŠTITE PODATAKA

U praksi, aktivizam o kome smo govorili na kraju prethodnog odeljka je često nerealan, ali i nepotreban.[13] Organi EU praktično moraju da se uvere da sve odluke

Commission on Human Rights) – u odnosu na diplomatska predstavništva u inostranstvu; *Loizidou v. Turkey*, 23 March 1995 (judgment – preliminary objections); *Al-Skeini and Others v. the United Kingdom*, 7 July 2011 (Grand Chamber – judgment) – u odnosu na okupacione trupe; *Banković and Others v. Belgium and 16 Other Contracting States*, 19 December 2001 (Grand Chamber – decision on the admissibility) – u odnosu na vojne intervencije u inostranstvu koje nemaju efektivnu kontrolu nad teritorijom (u ovom slučaju vazdušna kampanja bombardovanja u okviru agresije na SRJ 1999. godine); *Hirsi Jamaa and Others v. Italy*, 23 February 2012 (Grand Chamber – judgment) – u odnosu na akte izvan teritorije bilo koje države (u ovom slučaju na otvorenom moru); i *Andreou v. Turkey*, 3 June 2008 (judgment) – u odnosu na akte koji se izvrše na teritoriji države ali posledice deluju vanteritorijalno.

[12] Peter Margulies, "The Non-state Actors in the Global Perspective: Surveillance, Human Rights and International Counterterrorism", *Fordham Law Review*, no. 82, 2014, p. 2137.

[13] Sa napretkom tehnologija poput veštačke inteligencije, blokčejna i interneta, stvari koje prodiru u domove građana širom sveta, pravo na zaštitu podataka je posebno ugroženo, s obzirom na to da je praktično nemoguće obezbediti njegovu zaštitu u svakom pojedinačnom slučaju, videti više kod Cameron F. Kerry, "Why Protecting Privacy Is a Losing Game Today –

ili sporazumi o prenosu podataka iz EU u treće države ne dovode te podatke pod udar nižih standarda zaštite, odnosno da strani entiteti, koji upravljaju podacima i obrađuju ih, podležu propisima u svojim zemljama koji dovoljno štite integritet tih podataka. Sud pravde EU je u nekoliko odluka koje se tiču prenosa podataka, pre svega preko Atlantika iz EU u SAD, pokušao da u praksi pomiri ovu apsolutnu obavezu zaštite ljudskog prava na lične podatke sa državnim interesima bezbednosne prirode, ali i tržišnim interesima slobodnog protoka.[14] U suštini, Sud je pokušao da natera EU da ponovo pokrene pregovore o sporazumima sa stranim državama ili stranim entitetima koji kontrolišu podatke a imaju uticaja na unutrašnje tržište, u cilju da se novim odredbama sporazuma ojača zaštita podataka državljana EU i lica sa prebivalištem u EU. U svim tim odlukama prirodno se postavilo pitanje njihovog vanteritorijalnog dejstva.

Na primer, u predmetu protiv kompanije Fejsbuk, postavilo se pitanje – koje EU telo nadležno za nadzor nad zaštitom podataka može da pokrene postupak izvršenja protiv ove američke kompanije?[15] Drugi primer je slučaj koji se vodio protiv još jedne američke kompanije – Gugl – oko ličnih podataka na Guglovim linkovima za pretragu interneta. Postavilo se pitanje da li se moraju uklanjati lični podaci samo sa linkova koji vode ka adresama dostupnim u EU ili na celom globalnom internetu, kao i da li samo oni subjekti koji se nalaze u EU treba da vide izmenjene linkove, ili izmenjeni linkovi moraju da budu vidljivi svim korisnicima Gugla, bez obzira gde se nalaze. Francusko telo za nadzor nad zaštitom podataka je najpre kaznilo Gugl jer nije obrisao lične podatke EU subjekata zaštite sa svih vrsta linkova, iako su oni to od Gugla zatražili.[16] Međutim, Sud pravde EU je na kraju ocenio da odredbe Direktive i Uredbe o zaštiti podataka ne obavezuju operatere internet pretraživača da brišu podatke sa svih verzija pretraživača,[17] a zatim pomirljivo dodao da tako sveobuhvatno brisanje podataka svakako nije zabranjeno.[18] Iz ovakvog jezika presude se vidi da je vršenje vanteritorijalne

---

and How to Change the Game," Brookings (blog), July 12, 2018, https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-gametoday-and-how-to-change-the-game/, 20.9.2020.

[14] Videti: Case C-362/14, *Schrems v. Data Protection Commissioner*, ECLI:EU:C:2015:650 (Eur. Ct. Justice, Oct. 6, 2015); *Opinion 1–15 on Draft EU-Canada PNR Agreement*, ECLI:EU:C:2017:592 (Eur. Ct. Justice, July 26, 2017); i već pominjani slučaj *Gugl Španija*, C-131/12, *Google Spain Sl V. AEPD (THE DPA) & Mario Costeja Gonzalez,* 13 May 2014.

[15] Brussels Court of Appeal, *Facebook Ireland Ltd., Facebook Inc. and Facebook Belgium B.V.B.A. v. Belgian Data Protection Authority (DPA)*, 2018/AR/410, May 8, 2019.

[16] Case C-507/17, *Google Inc. v. Commission nationale de l'informatique et des libertés* (CNIL), ECLI:EU:C:2019:772 (Eur. Ct. Justice, Sept. 24, 2019).

[17] Ibid., para. 73.

[18] Ibid., para. 72.

nadležnosti nad moćnim inostranim kompanijama problematično pitanje, pa su organi EU spremni da usko tumače svoju nadležnost kako ne bi ispalo da zaštita prava na privatnost ustupa pred bezbednosnim i tržišnim interesima.

Otpor prema obavezi vanteritorijalnog delovanja organa EU na zaštiti prava na lične podatke može da dolazi i iz strukture tih istih organa, pre svega iz razloga političkog oportuniteta. Iako su građani ili stanovnici EU voljni da njihovi lični podaci budu što je moguće šire i potpunije zaštićeni, mora se imati u vidu da su sporazumi EU sa trećim državama kojima se reguliše prenos podataka u te države, ili dozvoljava stranim operaterima podataka da obavljaju privredne aktivnosti u okviru unutrašnjeg tržišta, pod velikim uticajem politike kao umetnosti mogućeg. Nerealno je obavezivati se na preširoku vanteritorijalnu zaštitu međunarodnim sporazumima koji neće moći da budu sprovedeni u delo, te bi ta nerealnost očekivanja mogla i da uruši legitimitet i prestiž institucija EU.

3.2. SUKOB NADLEŽNOSTI

Sa druge strane, glavna prepreka širokom vanteritorijalnom dejstvu EU propisa je sukob do kojeg može da dođe između različitih nadležnosti koje polažu pravo da pravno regulišu iste situacije. Države u koje se podaci prenose, ili čije kompanije posluju sa podacima na unutrašnjem tržištu EU, imaju jednako jaku a u najvećem broju slučajeva i jaču vezu sa konkretnom situacijom nego EU. Da se vratimo na prethodne „transatlantske" primere – SAD je u svim tim predmetima mogla da tvrdi kako na osnovu teritorijalnog načela može da traži informacije o bilo kom državljaninu EU čiji se lični podaci čuvaju na njenoj teritoriji, jer bezbednosne potrebe države to opravdavaju. Recimo, neki državljanin EU želi da uđe na teritoriju SAD kao običan putnik avionom, svejedno, ali iz nekog razloga vlasti SAD žele da izvrše njegovu bezbednosnu proveru. Normalno je da će prvo posegnuti za njegovim ličnim podacima koji se nalaze uskladišteni na serverima na američkom tlu. EU bi u tom slučaju bilo vrlo teško da se poziva na potrebu zaštite privatnosti ličnih podataka kako bi pojačala osnovu svoje veze za zasnivanje nadležnosti. Namerno navodimo ovaj naizgled banalan primer avionskog putnika, jer je upravo u toj oblasti došlo do rešenja kome bi, po nama, trebalo stremiti kako bi se izbegle sve komplikacije vanteritorijalne primene EU prava – sklopljen je bilateralni sporazum između EU i SAD o spiskovima imena putnika koji dozvoljava agenciji za carine i bezbednost granica SAD da u određenim slučajevima zahteva lične podatke o putnicima.[19]

[19] Passenger Name Records Agreements, niz sporazuma od kojih je poslednji potpisan 2011. godine, videti tekst na: https://www.dhs.gov/sites/default/files/publications/dhsprivacy_PNR%20Agreement_12_14_2011.pdf, 20.9.2020. Naravno da je sporazum kompromis između apsolutne zaštite privatnosti podataka i bezbednosnih potreba države ulaska, u kome su prava izvukla deblji kraj u odnosu na interese bezbednosti, što opet otvara pitanje hijerahije normi između međunarodnih ugovora i Povelje o osnovnim pravima, koje prevazilazi okvire ove rasprave.

Kažemo treba težiti ovakvim aranžmanima jer se njima izbegava osnovna prepreka vanteritorijalnoj primeni prava EU – nedostatak legitimnosti u primeni na strane pravne subjekte. Međutim, dva su problema sa sklapanjem ugovornih aranžmana sa trećim državama. EU je autonomni pravni sistem u odnosu na međunarodno pravo, i odredbe međunarodnih ugovora ne bi smele da krše primarno zakonodavstvo EU, u koje spadaju osnivački ugovori i Povelja o osnovnim pravima. Od EU se očekuje da štiti prava svojih građana čak i ako mora da deluje vanteritorijalno. Ugovori ovog tipa su ustupak političkoj neophodnosti da se ublaže negativne spoljnopolitičke posledice koje bi po EU nastale ako ne bi uvažila legitimne bezbednosne interese trećih država, pogotovo države kao što je SAD sa kojom EU ima stratešku saradnju u svim oblastima, a naročito u bezbednosnoj.

Srećom, zaštita ličnih podataka nije oblast u kojoj se vanteritorijalno vršenje nadležnosti često susreće sa otporom druge suverene države u čiji bi pravni domen ta nadležnost zadirala. Tu dolazimo do druge strane problema. To što otpori vanteritorijalnoj nadležnosti nisu česti, ne znači da druge države takvu praksu smatraju zakonitom i legitimnom. Biće da je ipak u pitanju to što vanteritorijalna nadležnost u oblasti zaštite ličnih podataka pogađa privatna pravna lica – operatere koji upravljaju podacima i obrađuju ih. Ti operateri uopšte nisu neke nejake firmice, koje ne bi mogle da se izbore same sa ekonomskim troškovima ispunjavanja obaveza koje im se postavljaju od strane EU zakonodavstva. Naprotiv, radi se o ekonomskim gigantima koji imaju dovoljno sredstava da samostalno pokreću i vode postupke za zaštitu svojih prava, bez oslanjanja na diplomatsku zaštitu matične države. Ta situacija umnogome podseća na one koje nastaju u suprotnom smeru – kada dejstvo sekundarnih sankcija koje SAD nameću tržištima sa kojima EU intenzivno posluje pogađa evropske kompanije, a EU ih pušta da se bore kako znaju i umeju protiv takvih teškoća u poslovanju.[20]

Međutim, da bismo odredili da li je vršenje vanteritorijalne nadležnosti u skladu sa međunarodnim pravom, nije dovoljno da utvrdimo kako se privatni subjekti bune protiv takvog vršenja nadležnosti, potrebna nam je praksa država. Zato su od značaja reakcije pojedinih država, pre svega SAD, koje su izrazile rezerve u pogledu vanteritorijalnog važenja propisa EU o zaštiti podataka, mada nije uvek jasno da li se te rezerve mogu tumačiti kao na međunarodnom pravu zasnovani prigovori. Na

[20] Kako primećuju autori Evropskog saveta za međunarodne odnose u nedavnom izveštaju o sekundarnim sankcijama SAD, EU je pokazala da ne može da obezbedi autonomnost svog pravnog sistema i svojih vrednosti jer je ekonomska zavisnost od SAD, pogotovo u domenu spoljne trgovine čija se plaćanja odvijaju u dolarima u najvećem broju slučajeva, i dalje suviše velika. Ta zavisnost je primorala evropske kompanije da se povinuju pravilima koje nameću sekundarne sankcije u smislu prekida poslovanja sa inače unosnim tržištima poput Irana, Kine i Rusije, videti: Ellie Geranmayeh, Manuel Lafont Rapnouil, *Meeting the challenge of secondary sanctions*, Policy Brief, 25 June 2019, European Council on Foreign Relations, https://www.ecfr.eu/publications/summary/meeting_the_challenge_of_secondary_sanctions, 20.9.2020.

primer, u pogledu već pominjanih podataka o putnicima na letovima iz EU u SAD, SAD su se svakako opirale primeni propisa EU o zaštiti podataka putnika, ali se ne vidi iz tih prigovora da li SAD osporavaju zakonitost vanteritorijalnog vršenja nadležnosti od strane EU.

Druga dva primera u kojima je došlo do varničenja među transatlantskim partnerima i na kojima ćemo se sada duže zadržati, povezani su sa sporazumima „Sigurna luka" i „Štit privatnosti", prilikom čijeg sklapanja SAD jesu osporavale mogućnost da se stroga načela zaštite podataka EU zakonodavstva uvrste u ove sporazume, ali nisu izričito navele da je razlog tom osporavanju njihova protivnost međunarodnom pravu.[21]

3.3. STUDIJA SLUČAJA – SPORAZUMI „SIGURNA LUKA" I „ŠTIT PRIVATNOSTI"

Sporazumi „Sigurna luka" i „Štit privatnosti" doživeli su istovetnu sudbinu pred Sudom pravde EU. U predmetu *Šrems I*,[22] tužilac se najpre žalio agenciji za zaštitu podataka Republike Irske. Tvrdio je da lični podaci Evropljana koje oni dostavljaju američkim firmama kako bi mogli da koriste internet usluge tih firmi, mogu da završe u rukama Agencije za nacionalnu bezbednost SAD bez ikakve pravne zaštite. Smatrao je da Agencija za zaštitu podataka Republike Irske ima obavezu da prekine prenose ličnih podataka u SAD zbog ovog problema. SAD jednostavno nisu imale standarde zaštite podataka u svojim zakonima koji bi odgovarali standardima postavljenim EU propisima, niti nadležno telo koje bi obezbeđivalo zaštitu prava na privatnost, već je sve bilo prepušteno privatnoj inicijativi samih kompanija. Ugovor „Sigurna luka",[23] je praktično konvalidirao takvu praksu, jer je dozvolio kompanijama da se samostalno usklađuju sa vrlo široko definisanim načelima zaštite podataka. Zatim se dogodio i „zemljotres" u vidu otkrića Edvarda Snoudena da američke obaveštajne agencije sprovode program globalnog nadzora, ne diskriminišući između „neprijateljskih" i „prijateljskih država". Šrems je praktično nakon afere Snouden došao na ideju da tuži.[24] Sud pravde je prihvatio Šremsove

[21] U.S. Mission to the European Union, Statement from U.S. Secretary of Commerce Penny Pritzker on EU–U.S. Privacy Shield, (Feb. 2, 2016), navedeno prema Cedric Ryngaert, "Mistale Taylor, Symposium on the GDPR and International Law: The GDPR as Global Data Protection Regulation?", op. cit., p. 8.

[22] Case C-362/14, *Schrems v. Data Protection Commissioner*, ECLI:EU:C:2015:650 (Eur. Ct. Justice, Oct. 6, 2015).

[23] Poništen od Suda pravde EU nakon presude u predmetu Šrems I, izvorni tekst dostupan na https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32000D0520, 20.9.2020.

[24] Videti više o pozadini spora kod Marc Rotenberg, "On International Privacy: Path Forward for the United States and Europe", *Harvard International Review*, no. 35, 2014, pp. 24-28.

argumente. Ne samo što je zaključio da su odredbe „Sigurne luke" suprotne tada važećoj Direktivi o zaštiti podataka, već ih je poništio i na osnovu člana 8 Povelje o osnovnim pravima, koji garantuje pravo na zaštitu ličnih podataka.

Međutim, posledice odluke u predmetu *Šrems I* nisu bile izmene propisa u SAD, već zaključivanje novog međunarodnog ugovora između EU i SAD, ovoga puta nazvanog „Štit privatnosti", koji je u suštini samo prepisao odredbe poništene „Sigurne luke".[25] Neposredno nakon usvajanja „Štita privatnosti" došlo je do novog skandala oko zloupotrebe podataka od strane američkih kompanija – takozvana afera „Fejsbuk – Kembridž Analitika", koja je verovatno uticala na ishod glasanja o Bregzitu i uopšte uzdrmala temelje demokratskih društava sa obe strane Atlantika. Poslanici Evropskog Parlamenta su se oglasili rezolucijom povodom afere, u kojoj su naveli da su i Fejsbuk i Kembridž analitika bile firme koje su označene kao sigurne u smislu zaštite podataka na osnovu odredbi „Štita privatnosti". Istovremeno, poslanici su potvrdili da kršenja privatnosti podataka mogu da dovedu do poremećaja u demokratskim procesima, ako se podaci zloupotrebe kako bi se uticalo na političko opredeljenje ili glasačke izbore i pozvali vlasti SAD da bez odlaganja uklone kompanije odgovorne za zloupotrebe sa liste sigurnih kompanija.[26]

U okviru te pozadine se razvio i još jedan postupak protiv Irske agencije za zaštitu podataka (Fejsbuk ima regionalno sedište za Evropu u Dablinu), koji je na kraju završio pred Sudom pravde EU, pod imenom *Šrems II*.[27] Bez mnogo ulaženja u detalje oko nedostataka na osnovu kojih je od strane Suda poništen „Štit privatnosti", suština je opet bila u nedovoljnoj usklađenosti propisa SAD sa pravima na privatnost podataka zaštićenim Poveljom EU.[28] U oba predmeta, Sud je dao smernice kako budući ugovori o prenosu podataka mogu da izbegnu istu sudbinu – samo ukoliko pojedinačne agencije za zaštitu podataka u državama članicama dobiju ovlašćenje na osnovu ugovora da mogu da suspenduju ili zabrane prenos ličnih podataka u svim okolnostima u kojima nije zagarantovana primena standarda EU o zaštiti privatnosti.[29] Dakle, najviši sudski organ EU smatra da jedini legitimni način za prenos podataka može da bude prećutno prihvatanje vanteritorijalne nadležnosti evropskih organa prema inostranim kompanijama.

---

[25] Poništen od Suda pravde EU nakon presude u predmetu Šrems II, izvorni tekst dostupan na https://iapp.org/resources/article/eu-u-s-privacy-shield-full-text/, 20.9.2020.

[26] European Parliament, "Suspend EU–US Data Exchange Deal, unless US Complies by 1 September, say MEPs" (5 July 2018), https://www.europarl.europa.eu/news/en/press-room/20180628IPR06836/suspend-eu-us-data-exchange-deal-unless-us-complies-by-1-september-say-meps, 20.9.2020.

[27] Case 311/18, Data Protection Commissioner v. Facebook Ireland and Schrems, ECLI:EU:C:2020:559.

[28] Ibid., para. 185.

[29] Ibid., para. 187.

4) DOMETI GDPR-A KAO GLOBALNOG MODELA

Ma koliko Sud pravde EU bio strog i dosledan u svojim odlukama, problemi sa vanteritorijalnom primenom propisa EU neće moći da se reše nikakvim ambicioznim sudskim aktivizmom. Stav Suda pravde EU je isuviše neosetljiv za realnosti međunarodnih odnosa, iako je savršeno legitiman sa aspekta unutrašnjeg pravnog poretka EU. Sporazumi o prenosu podataka jednostavno moraju da budu kompromisni i da uvažavaju interese i standarde obe strane, ukoliko se ti standardi i interesi razlikuju. Nije čudo što je jedna od prvih reakcija nekog američkog zvaničnika na presudu u slučaju *Šrems II* bio ogorčeni tvit bivšeg ambasadora SAD u EU, Entonija Gardnera, koji se zapitao ko plaća Maksu Šremsu, običnom građaninu, sva ta silna tužakanja američkih firmi?[30]

Međutim, optimistična shvatanja vanteritorijalne nadležnosti EU govore o takozvanom „efektu Brisela" u oblasti zaštite podataka, s obzirom na to da jednostrano vršenje nadležnosti u određenim situacijama koje se tiču zaštite podataka ima uticaja na velike multinacionalne korporacije, strane države i korisnike interneta širom sveta.[31] Načela utkana u EU propise o zaštiti podataka počinju da prelaze granice EU i utiču na oblikovanje autonomnih normi zaštite podataka koje stvaraju međunarodne korporacije, odnosno firme koje nisu registrovane u EU. Izvršni direktor Fejsbuka, Mark Zakerberg, predvideo je da će Uredba o zaštiti podataka postati globalni model regulacije, makar po duhu, ako ne i slovu normi koje sadrži.[32] Pod uticaj padaju i države i međunarodne organizacije, pogotovo ukoliko imaju značajne poslovne interese u EU ili su ionako vrednosno bliske evropskim vrednostima. Model zaštite podataka koji nudi GDPR, sa pravom na privatnost podataka kao utuživim ljudskim pravom, prema ovom shvatanju postaje inspiracija izvorima prava širom sveta.

Čini nam se da „efekat Brisela" zaista ima potencijal da menja sliku sveta kada je zaštita podataka u pitanju, ali samo do određenih, čvrsto postavljenih granica. Najpre, šta se dešava u situacijama kada strane firme ili države ne žele da prilagode

[30] Videti: https://twitter.com/tonylgardner/status/1292910353966391296, 20.9.2020.

[31] Efekat Brisela je fenomen dobro poznat u literaturi i koristi se da opiše situacije u kojima EU projektuje svoj spoljnopolitički uticaj preko izvoza sopstvenih vrednosti, oličenih u pravnom sistemu i privlačnoj moći unutrašnjeg tržišta. Jedan od najnovijih sveobuhvatnih radova na tu temu je monografija Anu Bradford, *The Brussels Effect – How the European Union Rules the World*, Oxford, Oxford University Press, 2020, gde autorka objašnjava kako je kroz proces ekonomske globalizacije došlo do mogućnosti za projektovanje balansiranih evropskih pravila ka drugim akterima na globalnoj sceni, pre svega u oblasti zaštite podataka, životne sredine, potrošača i konkurencije. Na taj način se meka ekonomska i vrednosna moć koristi na mesto tradicionalnijih i tvrđih oblika projekcije spoljne politike.

[32] Alex Hern, "Facebook Refuses to Promise GDPR-Style Privacy Protection for US Users", *The Guardian*, 4th April 2018.

svoje sisteme regulacije GDPR-u? Šta je sankcija koja može da ih natera da to ipak urade? Čini se da je jedina realna sankcija još uvek strah od gubitka pristupa profitabilnom unutrašnjem tržištu, jer za one najveće kompanije, poput američkih softverskih giganata, štete koje proizađu iz eventualnih postupaka koji se protiv njihovih filijala i ćerki firmi mogu voditi pred organima EU zbog kršenja propisa o zaštiti podataka, gledano procentualno u odnosu na njihove ukupne globalne prihode, i dalje su zanemarljive, i biće sve manje sa rastom potrošačke moći masovnih tržišta u zemljama izvan EU, poput Indije.

Takođe, zemlje koje su dovoljno moćne da mogu da projektuju sopstvene vrednosti jednako uspešno ili čak uspešnije od EU, a istovremeno su snažno ekonomski prisutne u EU, mogu da predstavljaju najveću opasnost po integritet GDRP-a. Primer Kine se nameće sam od sebe. Kina nema sveobuhvatni propis o zaštiti podataka poput GDPR-a, već se nekoliko različitih pravnih akata bavi tim pitanjem, od kojih je Zakon o sajber bezbednosti iz 2017. najznačajniji. Ovaj Zakon se u velikoj meri razlikuje od GDPR-a jer je zasnovan na ideji sajber suvereniteta, što znači da je njegova primena, kako se to izričito navodi u članu 2, ograničena isključivo na teritoriju Narodne Republike Kine. U kontekstu bilateralnih ekonomskih odnosa Kine i EU, to znači da kompanije koje su registrovane u Kini, a posluju i u Kini i u EU treba da se povinuju propisima i ovog zakona i GDPR-a, dok nasuprot tome, kompanije registrovane u EU mogu da poštuju samo odredbe GDPR-a.[33]

Sledeći tu liniju razmišljanja, čini se da će upravo strah da Kina ne preuzme primat u globalnom oblikovanju pravila svetske trgovine i bezbednosti podataka, koji sve više obuzima transatlantske odnose, doprineti daljem prodoru GDPR-a u pravne sisteme koji dele vrednosti sa EU. Jednostavno rečeno, geopolitičke okolnosti su se promenile od vremena kada je donesena presuda u predmetu *Šrems I*. Tada je delovalo da je najveći problem bezbednosti podataka evropskih građana svemoćna Agencija za nacionalnu bezbednost SAD i slabašna zaštita koju je pružala autonomna regulacija velikih američkih kompanija. Na prvi pogled, kada čitamo odluku *Šrems II*, usvojenu pre samo nekoliko meseci, deluje da su američke obaveštajne agencije i dalje najveći neprijatelj privatnosti evropskih građana. Međutim, to je samo tako na površini, jer je već prethodna a pogotovo trenutna američka administracija počela da steže obruč oko svog obaveštajnog establišmenta nakon štete koju je izazvala afera „Snouden" po prestiž SAD i odnose sa partnerskim državama. Počelo je Obaminom predsedničkom direktivom iz 2014,[34] nastavilo se medijskim

[33] Lee Sang Wo, *A Study on the Extraterritorial Application of the General Data Protection Regulation with a Focus on Computing*, Doctoral Dissertation, China University of Political Science and Law, 2019. Autor u svojoj tezi raspravlja o sukobu između propisa o zaštiti podataka Kine i EU i uticaju tog sukoba na međusobne ekonomske odnose. U aneksu rada se daje i tekst Zakona o sajber bezbednosti na engleskom jeziku.

[34] Presidential Policy Directive – Signals Intelligence Activities, POLICY DIRECTIVE/PPD-28.

preispitivanjem efikasnosti određenih programa prikupljanja obaveštajnih podataka, a kulminiralo Trampovom prozivkom autoriteta Suda nadležnog za spoljne obaveštajne poslove, nakon što je generalni inspektor u svom izveštaju doveo u sumnju istinitost nalaza obaveštajnih podataka koji su bili pred Sudom.[35]

U međuvremenu, sve države „zapadnog sveta" postaju svesnije mogućnosti elektronskog nadgledanja podataka kojima raspolaže Vlada Narodne Republike Kine. I ne samo to, već i sve učestaliji sajber napadi koje izvode nedržavni akteri, čiji se akti mogu pripisati vladi ove zemlje, sve više gađaju podatke zapadnih korporacija i vladinih institucija. Intenzivna kampanja SAD kojom se putem sankcija i lobiranja ograničava uticaj moćne državne kineske firme Huavej, a istovremeno pozivaju zemlje koje dele vrednosti zaštite ljudskih prava da obustave ugovore o izgradnji 5G mreže sa ovom kompanijom, takođe je deo iste jednačine. Poslednja karika u nizu ovih događaja je afera sa aplikacijom „Tik-tok", u vlasništvu takođe kineske softverske firme. Aplikacija koja služi za deljenje zabavnih snimaka optužena je od strane američke administracije kao špijunska ispostava Kine, jer prikuplja lične podatke naivnih građana i prosleđuje kineskim obaveštajnim agencijama. Spor je kulminirao izvršnom naredbom američkog predsednika kojom se poslovanje Tik-toka na tržištu SAD uslovljava prodajom kompanije nekoj od američkih tehnoloških firmi.[36]

Pitanje zaštite podataka se tako od „ljudskopravaškog" pitanja pretvara najvećim delom u pitanje državne bezbednosti. Mogućnosti masovnog sajber nadgledanja i zloupotrebe velikog broja ličnih podataka jasnije naglašavaju tu činjenicu. Retorika lidera „slobodnog sveta" praktično preuzima ideale zaštite ljudskih prava za ideološku borbu protiv neprijatelja, što je vidljivo u rečima američkog ministra spoljnih poslova Pompea koji u inicijativi „Čista mreža" navodi: „Postoji dugoročna opasnost po privatnost, bezbednost i ljudsko pravo na zaštitu podataka. Nasuprot njoj stoji načelna saradnja slobodnog sveta. Nacionalne vrednosti poput privatnosti građana i preduzeća moraju da budu obezbeđene od agresivnih napada zločinačkih aktera, kao što je Komunistička partija Kine".[37]

U tom smislu, „efekat Brisela" ne može da dobaci do globalnog nivoa, jer trenutni tok međunarodnih odnosa ne ide u smeru potpunog usaglašavanja. Na polju digitalizacije, sajber bezbednosti i zaštite podataka, dolazi do fragmentacije u makar

[35] Office of the Inspector General, Department of Justice, "Review of Four FISA Applications and Other Aspects of the FBI's Crossfire Hurricane Investigation", dostupno na https://www.justice.gov/storage/120919-examination.pdf, 20.9.2020.

[36] The White House, "Executive Order on Addressing the Threat Posed by TikTok" (6 August 2020), https://www.whitehouse.gov/presidential-actions/executive-order-addressing-threat-posed-tiktok/, 20.9.2020.

[37] US Department of State, The Clean Network Safeguards America's Assets (11 August 2020), https://www.state.gov/the-clean-network-safeguards-americas-assets/, 20.9.2020.

dva, a potencijalno i više blokova. Kina sa svojim državocentričnim viđenjem sajber prostora nudi pojačanu bezbednost države na račun ljudskih prava građana. EU je fokusiranija na individualistički pristup, gde pravo na privatnost podataka mora da bude iznad svih drugih obzira. U najboljem slučaju, EU može da nastavi da utiče na politiku srodnih zemalja zapadnog sveta, gde se za primat bori sa SAD, i gde zajednička opasnost od Kine može da dovede do potrebe za zanemarivanjem sopstvenog rivalstva i bržim usklađivanjem politika zaštite podataka.

Nije neobično stoga, što je nakon sleganja prašine od negativnih reakcija na presudu u predmetu *Šrems II*, potreba za saradnjom ipak preuzela primat u transatlantskim komunikacijama. Zajednička izjava ministra trgovine SAD Vilbura Rosa (*Wilbur Ross*) i Komesara EU za pravosuđe Didijea Rejndersa (*Didier Reynders*) protekloga avgusta pohvalno je govorila o presudi Suda pravde EU i ocenila poništeni sporazum „Štit privatnosti" kao neodgovarajući mehanizam za prenos podataka iz EU u SAD. U izjavi je natuknuto kako bi neki „Štit privatnosti 2.0" uskoro mogao da bude potpisan, kao ugovor koji će obezbediti maksimalnu usaglašenost sa načelima zaštite privatnosti podataka koja su istaknuta u presudi.[38] Dakle, evropski i američki funkcioneri najavljuju nova ulaganja u jačanja transatlantskog partnerstva na polju zaštite podataka, sa jednom važnom novinom u odnosu na prethodne napore. Dok je „Štit privatnosti", kao i njegov prethodnik „Sigurna luka", bio ugovor koji nije imao volje da dira u interese američkih firmi ili da menja pravni sistem SAD, sada se govori o „zajedničkoj posvećenosti privatnosti i vladavini prava" koja je od „vitalnog značaja za blagostanje građana i privreda dve zemlje".[39]

5) ZAKLJUČAK

Zaštita podataka na nivou EU skopčana je sa potrebom zaštite ljudskog prava na privatnost koje je zagarantovano temeljnim pravnim izvorima EU. U tom smislu odredbe ranije postojeće Direktive, a sadašnje Opšte uredbe o zaštiti podataka (GDPR) oblikovane su tako da deluju i vanteritorijalno, čak i u situacijama kada podacima raspolažu entiteti koji inače nisu subjekti EU prava. Vanteritorijalna primena prava nije načelno zabranjena u međunarodnom pravu, ali se njenom doslednom vršenju suprotstavljaju ograničenja praktične prirode i sukoba nadležnosti sa onim državama koje sa datim pravnim odnosom imaju „jaču", pre svega, teritorijalnu vezu. Apsolutna zaštita prava se zato svodi na dogovorno

[38] US Department of Commerce, "Joint Press Statement from US Secretary of Commerce Wilbur Ross and European Commissioner for Justice Didier Reynders" (10 August 2020), https://www.commerce.gov/news/press-releases/2020/08/joint-press-statement-us-secretary-commerce-wilbur-ross-and-european, 20.9.2020.

[39] Ibid.

formulisanje standarda zaštite između različitih nadležnosti kako bi se izbegli nepotrebni sporovi.

S obzirom na to da je dosledna vanteritorijalna primena EU prava teško ostvariva, postavlja se pitanje da li koncept zaštite podataka koji je primenjen u EU može da se nametne kao regulatorni model i ostalim suverenim nadležnostima. *Prima facie* je jasno da privlačna snaga unutrašnjeg tržišta omogućava izvoz EU modela u države koje nisu ekonomski približno snažne, a dele srodne vrednosti pravnog sistema, u smislu apsolutnog poštovanja ljudskih prava. Međutim, kada je reč o najvećim ekonomskim silama, koje nemaju identične modele zaštite podataka, ali dele vrednosti zaštite ljudskih prava sa EU, videli smo na primeru odnosa sa SAD da prihvatanje evropskih vrednosti ne ide nimalo glatko, te da su evropski političari skloni da zanemare obaveze poštovanja ljudskih prava svojih građana i zaključuju sa tim silama sporazume o prenosu podataka koji kasnije moraju da budu poništeni pred Sudom pravde EU. Stvar je još komplikovanija kada su u pitanju ekonomske sile koje ne dele iste vrednosti zaštite ljudskih prava poput Kine. Kod tih država se „efekat Brisela" najslabije oseća jer su one zapravo konkurencija briselskom modelu vrednosti. U svetu kome predstoje dalja geopolitička grupisanja država na linijama shvatanja sajber bezbednosti, i zaštita podataka će neminovno slediti ta grupisanja, te „efekat Brisela" u najboljem slučaju može da dopre do država koje budu deo jednog od tih blokova.

6) LITERATURA

Bradford, Anu, *The Brussels Effect – How the European Union Rules the World*, Oxford, Oxford University Press, 2020.

Diligenski, Andrej, Prlja, Dragan, Cerović, Dražen, *Pravo zaštite podataka – GDPR*, Institut za uporedno pravo, Beograd, 2018.

Domazet, Siniša, Skakavac, Zdravko, „Pravo na zaborav i opšta uredba Evropske unije 2016/679 o zaštiti podataka o ličnosti", *Evropsko zakonodavstvo*, God. XVII, br. 66, 2018, str. 70-86.

Geranmayeh, Ellie, Lafont Rapnouil, Manuel, *Meeting the challenge of secondary sanctions*, Policy Brief, 25 June 2019, European Council on Foreign Relations, https://www.ecfr.eu/publications/summary/meeting_the_challenge_of_secondary_sanctions, 20.9.2020.

Hern, Alex, "Facebook Refuses to Promise GDPR-Style Privacy Protection for US Users", *The Guardian*, 4th April 2018.

Kamminga, Menno T., *Extraterritoriality*, Max Planck Encyclopedia of Public International Law, https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1040, 20.9.2020.

Kerry, Cameron F., "Why Protecting Privacy Is a Losing Game Today – and How to Change the Game," Brookings (blog), July 12, 2018, https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-gametoday-and-how-to-change-the-game/, 20.9.2020.

Klar, Manuel, "Binding Effects of the European General Data Protection Regulation (GDPR) on U.S. Companies", *Hastings Science and Technology Law Journal*, Vol. 11, No. 2, 2020, pp. 100-153.

Kuner, Christopher, "The GDPR and International Organizations", American Journal of International Law Unbound, Vol. 114, 2020 , pp. 15-19.

Margulies, Peter, "The Non-state Actors in the Global Perspective: Surveillance, Human Rights and International Counterterrorism", *Fordham Law Review*, no. 82, 2014.

Milanović, Marko, *Extraterritorial Application of Human Rights Treaties: Law, Principles, and Policy*, Oxford, Oxford University Press, 2011.

Moreno-Lax, Violeta, Costello, Cathryn, "The Extraterritorial Application of the EU Charter of Fundamental Rights: From Territoriality to Facticity, the Effectiveness Model", Steve Peers et al. (eds.) *The EU Charter of Fundamental Rights: A Commentary*, Hart/Beck/Nomos, 2014.

Pramesti, Indriana, Afriansyah, Arie, Extraterritoriality of Data Protection: GDPR and Its Possible Enforcement in Indonesia, *Advances in Economics, Business and Management Research*, Volume 130, 2020, pp. 83-94.

Prlja, Sanja, „Pravo na zaštitu ličnih podataka u EU", *Strani pravni život*, br. 1, 2018, str. 89-99.

Ronald Bindu, Samuel, Vasmatkar, Abhijit, Gurpur, Shashikala, "GDPR: Legal Impact on Extra – Territorial Commercial Pressure on Indian Business, Trade and Investment", *The Next Seven of the European Union*, Sofia University "St. Kliment Ohridski" and "Hanns Seidel" Foundation, Sofia, 2020, pp. 45-56.

Rotenberg, Marc, "On International Privacy: Path Forward for the United States and Europe", *Harvard International Review*, no. 35, 2014, pp. 24-28.

Ryngaert, Cedric, Mistale, Taylor, "Symposium on the GDPR and International Law: The GDPR as Global Data Protection Regulation?", *American Journal of International Law Unbound*, vol. 114, 2020, pp 5-9.

Sang Wo, Lee, *A Study on the Extraterritorial Application of the General Data Protection Regulation with a Focus on Computing*, Doctoral Dissertation, China University of Political Science and Law, 2019.

THE LIMITS OF THE EXTRATERRITORIAL EFFECT OF THE EU GENERAL DATA PROTECTION REGULATION

Summary: The EU General Data Protection Regulation (GDPR) has an impact on standards of data protection in other legal systems due to its extraterritorial effect. The attractive internal market is the main reason for foreign companies that use personal data of the EU citizens or residents in their business operations to comply with its provisions. Therefore the EU jurisdiction stretches extraterritorially. The extraterritorial activity of one sovereign jurisdiction, in principle, is not contrary to international law but creates problems in practical application and enforcement, as well as objections of other sovereign jurisdictions that can claim a stronger link with the legal issue at hand. Through international treaties that regulate the extraterritorial jurisdictional issues, these problems can be solved. However, the right of personal data protection of the GDPR is constructed as a human right, absolutely protected, which automatically negates the effect of such a treaty. The Court of Justice of the EU has shown the willingness to defend the integrity of this right. This article raises the question of whether the attraction of the internal market together with the conception of the right to data protection as a human right can impose the EU's data protection model as a global model. It is argued that economically powerful states, even if they share human rights values with the EU, can stand the extraterritorial impact of the GDPR shown through the lens of the EU-US relationship. However, the real problem exists in the conflict of jurisdiction with an economic power with a totally different system of values concerning human rights, and especially data protection rights, such as China. In this context, the article's conclusion states that, in the best scenario, the extraterritorial effect of the GDPR can lead to the EU's data protection model becoming a role model for a bloc of like-minded legal systems, especially since data protection in current international relations is rather a security than an economic issue.

Keywords: GDPR, extraterritoriality, data protection, right to privacy, EU