Društvene mreže i međunarodni prijenos podataka

Horak, Tamara

REPUBLIKA HRVATSKA
SVEUČILIŠTE U ZAGREBU
PRAVNI FAKULTET

Studentica:
Tamara Horak

DIPLOMSKI RAD

DRUŠTVENE MREŽE I MEĐUNARODNI PRIJENOS PODATAKA

Kolegij:
Pravo informacijskih tehnologija

Mentor:
Izv.prof.dr.sc. Hrvoje Lisičar

Zagreb, 2025.

SADRŽAJ

1. UVOD

Razvoj tehnologije i rast popularnosti društvenih mreža omogućili su nevjerojatnu povezanost ljudi diljem svijeta, ali su istovremeno donijeli i nove izazove, osobito u pogledu zaštite privatnosti i osobnih podataka. Tema ovog rada – društvene mreže i međunarodni prijenos podataka – od iznimne je važnosti u današnjem digitalnom dobu gdje osobni podaci predstavljaju ne samo privatnu, već i ekonomsku vrijednost.

Rad se osvrće na povijesni razvoj zaštite podataka, od ranih zakonodavnih inicijativa u Njemačkoj i Švedskoj do ključnih trenutaka poput usvajanja Konvencije br. 108 Vijeća Europe i Opće uredbe o zaštiti podataka (GDPR). Posebna pažnja posvećena je međunarodnoj dimenziji prijenosa podataka, uključujući složene odnose između Europske unije i Sjedinjenih Američkih Država, koji su obilježeni nizom pravnih izazova i reforma poput sustava Sigurne luke, Sustava zaštite privatnosti i najnovijeg okvira za zaštitu podataka (engl. Data Privacy Framework).

Kroz rad razmatraju se ključni koncepti privatnosti, prava na zaštitu podataka i njihove implikacije u kontekstu društvenih mreža s posebnim naglaskom na globalne igrače poput Facebooka, TikToka i Googlea. Osim pravnih izazova, istaknuta je važnost transparentnosti, informirane privole i regulacije prijenosa podataka kako bi se osigurala ravnoteža između tehnološkog napretka i zaštite temeljnih prava korisnika.

2. POJMOVNA RAZRADA

Budući da je tema ovog rada društvene mreže i međunarodni prijenos podataka, bitno je definirati središnji pojam teme, što su osobni podaci. "Osobni podaci znači svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi („ispitanik"); pojedinac čiji se identitet može utvrditi jest osoba koja se može identificirati izravno ili neizravno, osobito uz pomoć identifikatora kao što su ime, identifikacijski broj, podaci o lokaciji, mrežni identifikator ili uz pomoć jednog ili više čimbenika svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca."[1] Tako glasi definicija osobnih podataka iz Opće uredbe o zaštiti podataka Europskog parlamenta i Vijeća za koju se može reći da je kruna zaštite osobnih podataka u svijetu.

Ključnu ulogu u razvoju, održavanju društvenih mreža i u upravljanju međunarodnim prijenosom podataka ima informacijski sustav. Zakon o informacijskoj sigurnosti (NN 79/07) informacijski sustav definira kao: komunikacijski, računalni ili drugi elektronički sustav u kojem se podaci obrađuju, pohranjuju ili prenose tako da budu dostupni i upotrebljivi za ovlaštene korisnike.[2] Informacijski sustav razvijao se eksponencijalnom brzinom zadnjih četrdesetak godina. Od osamdesetih godina 20. stoljeća, od prvih računala, do interneta. Takvi sustavi uz primjenu načela ekonomičnosti, učinkovitosti i sigurnosti omogućuju personalizaciju sadržaja, zaštitu osobnih podataka i optimizaciju resursa.[3] Svakako je bitna pravovremenost, dostupnost i valjanost informacija koje predstavlja načelo učinkovitosti. Načelo ekonomičnosti pada danas u drugi plan zbog široke dostupnosti znanja i resursa, kao i visoke razine razvoja. Najvažnijim načelom danas moglo bi se smatrati načelo sigurnosti. Podaci su lako dostupni, u trenutku se može saznati jako puno informacija, a jednom objavljen podatak na internetu, skoro je nemoguće izbrisati. Podatak se može učiniti nedostupnim korisnicima interneta, ali često jako puno korisnika vidi određen

[1] UREDBA (EU) 2016/679 EUROPSKOG PARLAMENTA I VIJEĆA od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) (dalje u tekstu: Opća uredba), L 119/1, Službeni list Europske unije, 4. svibnja 2016.

[2] čl.2. Zakona o informacijskoj sigurnosti (NN 79/07).

[3] Dragičević, D., *Pravna informatika i pravo informacijskih tehnologija*, Narodne novine, Zagreb, listopad 2015., str. 80-85.

podatak u istom trenutku kad je objavljen, a iz glava ljudi izbrisati se ne može. Razvojem društvenih mreža, u vremenu kad više od 62% populacije u svijetu koristi društvene mreže što predstavlja broj od 5 milijarda ljudi, načelo sigurnosti sve je važnije.[4] Stoga je ključna stroga regulacija obrade osobnih podataka.

Informacijski sustav čini osnovu informacijskog društva, a prema Hrvatskoj enciklopediji: "Informacijsko društvo, naziv koji se od početka 1990-ih upotrebljava u dokumentima Europske unije za označivanje suvremenoga društva, koje svoj gospodarski, znanstveni i kulturni razvoj zasniva na uvođenju i širenju računalne i telekomunikacijske tehnologije te stvaranju, obradi i prijenosu informacija kao temelju za rast produktivnosti društva."[5]

Društvene mreže smatraju se uslugama informacijskog društva prema definiciji iz Zakona o elektroničkoj trgovini. Prema članku 2. stavku 1. točki 2. tog zakona, usluga informacijskog društva je "svaka usluga koja se uz naknadu pruža elektroničkim putem na individualni zahtjev primatelja usluge".[6] Takve usluge uključuju internetsku prodaju robe i usluga, ponudu podataka na internetu, reklamiranje putem interneta, elektroničke pretraživače, mogućnost traženja i posredovanja u pristupu podacima i uslugama putem elektroničke mreže. Iako društvene mreže često ne naplaćuju izravno svoje usluge korisnicima, njihov poslovni model temelji se na prihodima od oglašavanja što zadovoljava kriterij pružanja usluge uz naknadu. Nadalje, prema Direktivi (EU) 2015/1535, usluga informacijskog društva definira se kao "svaka usluga koja se obično pruža uz naknadu, na daljinu, elektroničkim sredstvima te na osobni zahtjev primatelja usluga".[7] Društvene mreže ispunjavaju ove uvjete jer omogućuju korisnicima pristup sadržaju i komunikaciju putem interneta, često financirane putem oglašavanja. Iako zakonodavstvo ne navodi izričito društvene mreže kao primjer usluga informacijskog društva, one se uklapaju u opće definicije i kriterije navedene u relevantnim zakonima i direktivama.

---

[4] Petrosyan, A., *Worldwide digital population 2024,* Statista, 4. listopada 2024., dostupno na: https://www.statista.com/statistics/617136/digital-population-worldwide/ (10. listopada 2024.).
[5] Informacijsko društvo, *Hrvatska enciklopedija, mrežno izdanje.* Leksikografski zavod Miroslav Krleža, 2013. – 2025 dostupno na:https://www.enciklopedija.hr/clanak/informacijsko-drustvo, 5.1.2025.
[6] Zakon o elektroničkoj trgovini, Narodne novine 173/03, 67/08, 36/09, 130/11, 30/14, 32/19.
[7] Čl.1. Direktive (EU) 2015/1535 Europskog parlamenta i Vijeća od 9. rujna 2015. o utvrđivanju postupka pružanja informacija u području tehničkih propisa i pravila o uslugama informacijskog društva, L241/1, Službeni list Europske unije.

3. PRAVO NA PRIVATNOST – KRONOLOŠKI ZAKONODAVNI RAZVOJ

Zaštita osobnih podataka problem je modernog društva koji nastaje u novije doba. Postaje značajna razvojem tehnologije i informacijsko komunikacijske tehnologije. Zaštita osobnih podataka bit je informacijske sigurnosti. U doba tehnologije, osobni podaci postaju ključni element privatnosti. Bez pravilne zaštite osobnih podataka, privatnost je ugrožena. Ideja o pravu na privatnost počinje se širiti razvojem tiska i fotografije u 19. stoljeću.

Pravo na privatnost na svjetskoj razini prvi put navedeno je Općoj deklaraciji o ljudskim pravima 1948. godine u čl.12.[8]:"Nitko ne smije biti podvrgnut samovoljnom miješanju u njegov privatni život, obitelj, dom ili dopisivanje, niti napadima na njegovu čast i ugled. Svatko ima pravo na zakonsku zaštitu protiv takvog miješanja ili napada."[9][10] Na europskoj razini, to se dogodilo u Europskoj konvenciji za zaštitu ljudskih prava i temeljnih sloboda iz 1950. godine u čl.8.:"1. Svatko ima pravo na poštovanje svoga privatnog i obiteljskog života, doma i dopisivanja. 2. Javna vlast se neće miješati u ostvarivanje tog prava, osim u skladu sa zakonom i ako je u demokratskom društvu nužno radi interesa državne sigurnosti, javnog reda i mira, ili gospodarske dobrobiti zemlje, te radi sprječavanja nereda ili zločina, radi zaštite zdravlja ili morala ili radi zaštite prava i sloboda drugih.".[11] Pravo na privatnost propisano je i Hrvatskim Ustavom u čl.36.:"Sloboda i tajnost dopisivanja i svih drugih oblika općenja zajamčena je i nepovrediva. Samo se zakonom mogu propisati ograničenja nužna za zaštitu sigurnosti države ili provedbu kaznenog postupka."[12] i čl.37.:"Svakom se jamči sigurnost i tajnost osobnih podataka. Bez privole ispitanika, osobni se podaci mogu prikupljati, obrađivati i koristiti samo uz uvjete određene zakonom. Zakonom se uređuje zaštita podataka te nadzor nad djelovanjem informatičkih sustava u državi. Zabranjena je uporaba osobnih podataka suprotna utvrđenoj svrsi njihovoga prikupljanja.".[13]

---

[8] Resolution 217A (III), Universal Declaration of Human Rights, A/RES/217(III).
[9] Odluka o objavi Opće deklaracije o ljudskim pravima, Narodne novine 12/2009.
[10] Konvencija za zaštitu ljudskih prava i temeljnih sloboda te Protokola br. 1, Protokola br. 4, Protokola br. 6 i Protokola br. 7 uz tu Konvenciju, Narodne novine 6/1999.
[11] (Europska) Konvencija za zaštitu ljudskih prava i temeljnih sloboda, MU 18/97, 6/99, 14/02, 13/03, 9/05, 1/06, 2/10, 13/17.
[12] Čl.36. Ustav Republike Hrvatske (dalje u tekstu: Ustav RH) Narodne novine 56/90, 135/97, 08/98, 113/00, 124/00, 28/01, 41/01, 55/01, 76/10, 85/10, 05/14.
[13] Čl.37. Ustava RH.

Ne postoji potpuna suglasnost oko točnog opsega zaštite privatnosti pojedinca niti o tome što sve pravo na privatnost obuhvaća. Različite zemlje, pravni sustavi i kulture imaju različite definicije privatnosti, a njezina zaštita često ovisi o društvenim normama, zakonodavnim okvirima i tehnološkim izazovima. Unatoč tome, postoji široko prihvaćeno načelo da privatnost pojedinca treba štititi jer je to u interesu svakoga. Osim toga, zaštita prava privatnosti nije samo u interesu pojedinca, već je i u širem društvenom interesu. Osiguranje privatnosti doprinosi izgradnji povjerenja u društvu i u institucije, kao i razvoju ekonomije. Kada ljudi vjeruju da su njihovi podaci sigurni i da se poštuje njihova privatnost, vjerojatnije je da će biti spremni koristiti digitalne usluge, podijeliti svoje podatke s javnim i privatnim sektorom, i aktivno sudjelovati u društvu. Stoga je zaštita privatnosti univerzalni interes koji nadilazi individualne potrebe i ima ključnu ulogu u očuvanju slobodnog, sigurnog i otvorenog društva.

Velik utjecaj na širenje ideje o pravu na privatnost imao je članak *The Right to Privacy* autora Samuela Warrena i Louisa Brandeisa iz 1980. godine izdan u Harvard Law Review.[14] Pojedini američki pravni znanstvenici nazivaju taj članak najznačajnijim pravnim člankom ikad napisanim.[15] I pravo na privatnost i pravo na zaštitu podataka služe očuvanju sličnih vrijednosti, poput autonomije i ljudskog dostojanstva, stvaranje prostora u kojem pojedinci mogu slobodno razvijati svoju osobnost, donositi odluke i oblikovati vlastita mišljenja. Ova prava čine temelj za ostvarivanje ključnih ljudskih sloboda, kao što su sloboda izražavanja, pravo na mirno okupljanje i udruživanje, i sloboda vjeroispovijedi. Ljudi moraju osjećati sigurnost da slobodno izražavaju svoje misli i ideje, znajući da njihovi podaci neće biti zloupotrijebljeni, a da bi se ljudi slobodno okupljali i organizirali, moraju biti zaštićeni od nadzora ili praćenja koji bi mogli ugroziti njihovu privatnost. Privatnost također osigurava da pojedinci mogu prakticirati svoju vjeru ili uvjerenja bez straha od progona ili diskriminacije.

Pravo na privatnost razlikuje se od zaštite osobnih podataka po svojoj formulaciji i primjeni. Pravo na privatnost obuhvaća opću zabranu miješanja osim kada javni interes opravdava

---

[14] Bratman, B. E., *BRANDEIS AND WARREN'S THE RIGHT TO PRIVACY AND THE BIRTH OF THE RIGHT TO PRIVACY,* Tennessee Law Review, Vol.69:623, 2002., str. 623, dostupno na: https://scholarship.law.pitt.edu/cgi/viewcontent.cgi?article=1062&context=fac_articles (10. listopada 2024.).

[15] Joshi, D., *Privacy Theory 101: Warren and Brandeeis's 'The Right to Privacy' - Law Affect and the 'Right to be Let Alone',* Centre for Law & Policy Research, 25. rujna 2020., dostupno na: https://clpr.org.in/blog/privacy-theory-101-warren-and-brandeiss-law-affect-and-the-right-to-be-let-alone/ (10. listopada 2024.).

takvo miješanje. S druge strane, zaštita osobnih podataka smatra se modernim, aktivnim pravom koje postavlja sustav nadzora i kontrole kako bi se pojedinci zaštitili prilikom obrade svojih osobnih podataka.[16]

[16] Agencija Europske unije za temeljna prava i Vijeće Europe, *Priručnik o europskom zakonodavstvu i zaštiti podataka. Izdanje iz 2018.*, travanj 2018., dostupno na: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_hr.pdf.

4. RAZVOJ ZAKONODAVNOG OKVIRA ZA ZAŠTITU OSOBNIH PODATAKA

Prvi zakonodavni akt na području zaštite podataka donosi se u Njemačkoj saveznoj državi Hessen 1970. godine, a prvi nacionalni zakon donesen je u Švedskoj 1973. godine.[17] Idućih petnaestak godina nekoliko je država u Europi donijelo zakone o zaštiti podataka, kao što su Francuska, Njemačka, Nizozemska i Ujedinjeno Kraljevstvo i tako je zaštita podataka postala posebna pravna vrijednost odvojena od tradicionalnog prava na poštivanje privatnog života. [18]

Jedan od ključnih trenutaka za međunarodnu zaštitu osobnih podataka bilo je usvajanje Konvencije br. 108 1981. godine[19], koju je donio Odbor ministara Vijeća Europe na temelju članka 8. Europske konvencije za zaštitu ljudskih prava i temeljnih sloboda.[20] Ova konvencija, službenog naziva Konvencija o zaštiti osoba glede automatizirane obrade osobnih podataka i njezin dodatni protokol[21], predstavljali su prekretnicu u međunarodnom pravnom okviru za zaštitu privatnosti i osobnih podataka. Bila je prvi pravno obvezujući međunarodni dokument koji se izravno bavio ovom temom, a i do danas ostaje jedini takav instrument na globalnoj razini. Konvencija je imala ogroman utjecaj na nacionalna zakonodavstva unutar Europe jer su mnoge države koje su je potpisale morale prilagoditi svoje zakonodavne okvire kako bi osigurale da njihovi zakoni budu u skladu s načelima Konvencije 108. To je bio prvi korak prema stvaranju koherentnog sustava zaštite osobnih podataka unutar Europe koji je kasnije postao temelj za razvoj Opće uredbe. Njezin značaj prepoznat je i u novijim revizijama, poput Protokola 223 iz 2018. godine, koji je ažurirao

---

[17] Korff, D.; Georges, M., *Priručnik za DPO-ove, Smjernice za službenike za zaštitu osobnih podataka u javnom i gotovo isključivo-javnom sektoru o tome kako osigurati usklađenost s Općom Uredbom o zaštiti podataka Europske unije*, rujan 2018., str.17, dostupno na: https://azop.hr/wp-content/uploads/2020/12/prirucnik-_za_dpo-t4data-hrv.pdf.
[18] Korff, D.; Georges, M., *Priručnik za DPO-ove, Smjernice za službenike za zaštitu osobnih podataka u javnom i gotovo isključivo-javnom sektoru o tome kako osigurati usklađenost s Općom Uredbom o zaštiti podataka Europske unije*, rujan 2018., str.19, dostupno na: https://azop.hr/wp-content/uploads/2020/12/prirucnik-_za_dpo-t4data-hrv.pdf.
[19] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, European Treaty Series - No. 108.
[20] (Europska) Konvencija za zaštitu ljudskih prava i temeljnih sloboda.
[21] Zakon o potvrđivanju Konvencije za zaštitu osoba glede automatizirane obrade osobnih podataka i Dodatnog protokola uz Konvenciju za zaštitu osoba glede automatizirane obrade osobnih podataka u vezi nadzornih tijela i međunarodne razmjene podataka, NN 4/2005-38.

Konvenciju kako bi bila u skladu s novim izazovima digitalne ere uključujući umjetnu inteligenciju i globalni prijenos podataka.[22]

Još jedan važan trenutak u razvoju europskog pravnog okvira bila je Direktiva 95/46/EZ, usvojena 1995. godine.[23] Cilj ove direktive bio je uskladiti zakonodavstvo država članica EU o zaštiti podataka, kako bi se osigurao slobodan protok osobnih podataka unutar EU uz poštivanje osnovnih prava na privatnost.[24] Direktiva je uvela ključne pojmove poput osobnih podataka, voditelja obrade i privole, kao i obvezu osnivanja nacionalnih tijela za zaštitu podataka u svim državama članicama.[25] Ona je bila temelj za nacionalne zakone o zaštiti podataka u državama članicama EU sve do stupanja na snagu Opće uredbe 2018. godine.

Uz to, važan korak bio je donošenje Direktive o privatnosti i elektroničkim komunikacijama 2002. godine.[26] Ova direktiva, poznata i kao Direktiva o e-privatnosti, bavila se specifičnim pitanjima zaštite privatnosti u kontekstu elektroničkih komunikacija, poput korištenja kolačića[27], e-mail marketinga[28], kao i sigurnosti komunikacija.[29] Direktiva je nadopunila opći okvir zaštite podataka i naglasila važnost zaštite privatnosti u digitalnom okruženju.

[22] Protokol kojim se mijenja i dopunjuje Konvencija za zaštitu osoba glede automatizirane obrade osobnih podataka, Strasbourg, 10. listopada 2018., Niz ugovora Vijeća Europe - Br. 223.
[23] Direktiva 95/46/EZ Europskog parlamenta i vijeća od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom osobnih podataka i slobodnom protoku takvih podataka, Službeni list Europske unije, L 281/31.
[24] čl.1. Direktive 95/46/EZ.
[25] čl.2. Direktive 95/46/EZ.
[26] UREDBA (EU) 2018/1725 EUROPSKOG PARLAMENTA I VIJEĆA od 23. listopada 2018. o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama, tijelima, uredima i agencijama Unije i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Uredbe (EZ) br. 45/2001 i Odluke br. 1247/2002/EZ, Službeni list Europske unije L 295/39.
[27] Čl.5,st.3. UREDBE (EU) 2018/1725.
[28] Čl.13 UREDBE (EU) 2018/1725.
[29] Čl.4. i 5. UREDBE (EU) 2018/1725.

5. BITNE ODREDBE ZAKONODAVNOG OKVIRA ZA PRIJENOS PODATAKA

Jedan od ključnih problema bio je nedostatak jedinstvenog zakonodavstva u Europskoj uniji. Svaka država članica imala je svoje nacionalne zakone temeljene na Direktivi 95/46/EZ što je rezultiralo neujednačenom zaštitom osobnih podataka i složenim pravnim okruženjem za trgovačka društva koja posluju unutar više država EU. To je stvorilo potrebu za donošenjem jedinstvenog i sveobuhvatnog pravnog instrumenta koji bi osigurao dosljednu zaštitu podataka u cijeloj EU.

Osim toga, globalne tehnološke kompanije uključujući društvene mreže, počele su igrati ključnu ulogu u svakodnevnom životu pojedinaca. Međutim, nedovoljna transparentnost u načinu prikupljanja i korištenja podataka, kao i nedostatak učinkovitih pravnih mehanizama za zaštitu privatnosti, izazvali su zabrinutost među građanima i zakonodavcima. Veliki skandali, poput zloupotrebe osobnih podataka od strane korporacija, dodatno su naglasili potrebu za jačom regulacijom.

Opća uredba odgovorila je na ove izazove uvođenjem sveobuhvatnih pravila o zaštiti podataka koja su prilagođena digitalnom dobu. Opća uredba značajno proširuje prava pojedinaca u pogledu njihovih osobnih podataka. Pojedinci sada imaju pravo na pristup svojim podacima, ispravak netočnih podataka, brisanje podataka („pravo na zaborav“), prijenos podataka drugom voditelju obrade, ograničenje obrade, kao i pravo na prigovor uključujući prigovor na profiliranje.[30] Ove odredbe omogućuju korisnicima veću kontrolu nad vlastitim podacima što je posebno važno u kontekstu društvenih mreža gdje se veliki obujam osobnih podataka obrađuje svakodnevno.

Uz proširena prava pojedinaca, Opća uredba uvodi obveze za voditelje i izvršitelje obrade. Društvene mreže dužne su prijaviti povrede osobnih podataka u roku od 72 sata nadležnom tijelu za zaštitu podataka i, kada je potrebno, korisnicima.[31] Ove obveze naglašavaju važnost

[30] Čl.15.-21. Opće uredbe.
[31] Čl.33 Opće uredbe.

pravovremenog i odgovornog djelovanja u slučajevima povreda podataka čime se štiti integritet korisnika i njihovi osobni podaci.

Kazne predviđene Općom uredbom za povredu zaštite osobnih podataka koje mogu doseći 20 milijuna eura ili 4% godišnjeg globalnog prometa organizacije[32], dodatno motiviraju društvene mreže na strogo pridržavanje odredaba. Opća uredba također zahtijeva od društvenih mreža da pružaju jasne i detaljne informacije o načinima prikupljanja, obrade i prijenosa podataka.[33]

Osim toga, Opća uredba ograničava profiliranje i personalizirano oglašavanje što je od velike važnosti za poslovne modele društvenih mreža. Društvene mreže ne smiju automatizirano obrađivati osobne podatke za donošenje odluka koje značajno utječu na korisnike, uključujući profiliranje, bez njihove privole.[34] Korisnici sada imaju pravo zatražiti brisanje svojih podataka što uključuje i podatke pohranjene na poslužiteljima društvenih mreža nakon deaktivacije računa.[35] Ove promjene povećavaju odgovornost društvenih mreža prema korisnicima i osiguravaju veću razinu zaštite privatnosti.

[32] Čl.83 Opće uredbe.
[33] Čl.12.-14. Opće uredbe.
[34] Čl.22. Opće uredbe.
[35] Čl.17. Opće uredbe.

6. NACIONALNI PRAVNI OKVIR

Zaštita osobnih podataka u Hrvatskoj razvijala se u skladu s međunarodnim i europskim standardima uz značajan utjecaj zakonodavnog okvira Europske unije i međunarodnih konvencija. Proces prilagodbe počeo je još prije ulaska Hrvatske u EU, a nastavio se nakon toga usklađivanjem s novim direktivama i uredbama.

Prvi zakon kojim se u Hrvatskoj regulirala zaštita osobnih podataka bio je Zakon o zaštiti osobnih podataka iz 2003. godine.[36] Ovaj zakon postavio je temelje za zaštitu osobnih podataka, definirajući ključne pojmove poput osobnih podataka, voditelja obrade i prava ispitanika.[37] Njime su osnovane obveze za voditelje obrade i izvršitelj obrade osobnih podataka. Uveden je i nadzor nad obradom podataka putem tadašnje Agencije za zaštitu osobnih podataka (AZOP), koja je osnovana kao neovisno tijelo zaduženo za praćenje provedbe zakona.[38]

Hrvatska se 2013. godine pridružila Europskoj uniji, što je zahtijevalo daljnje usklađivanje zakonodavstva s pravnom stečevinom EU. Zakon o zaštiti osobnih podataka iz 2003. godine u nekoliko je navrata mijenjan i dopunjavan kako bi bio u skladu s europskim standardima, uključujući Direktivu 95/46/EZ. [39]

Donošenjem i stupanjem na snagu Opće uredbe, kojom se ujednačila zaštita osobnih podataka na razini cijele EU, Zakon o zaštiti osobnih podataka više nije bio u skladu s novim europskim standardima. Zamijenio ga je Zakon o provedbi Opće uredbe o zaštiti podataka (NN 42/18) koji regulira i određena specifična pitanja za koja je sama Opća uredba ostavila prostor državama članicama da ih urede nacionalnim propisima.[40]

---

[36] Zakon o zaštiti osobnih podataka, Narodne novine 103/2003, 18. lipnja 2023.
[37] Čl.2. Zakona o zaštiti osobnih podataka.
[38] Čl.27.-35. Zakona o zaštiti osobnih podataka.
[39] Zakon o zaštiti osobnih podataka, Narodne novine 106/2012, 26. rujna 2012.
[40] Zakon o provedbi Opće uredbe o zaštiti podataka (dalje u tekstu: Zakon o provedbi Opće uredbe), Narodne novine 42/18, 9. svibnja 2018.

Opća uredba propisuje da države članice moraju uspostaviti nadzorno tijelo.[41] U Hrvatskoj je to Agencija za zaštitu osobnih podataka (dalje u tekstu: AZOP) koja je pravni sljednik bivše Hrvatske Agencije za zaštitu osobnih podataka osnovane prema ranijem Zakonu o zaštiti osobnih podataka. [42] Stupanjem na snagu novog zakona, AZOP je izgubio status pravne osobe s javnim ovlastima i postao državno tijelo. Zakonom o provedbi Opće uredbe određeno je da se upravne novčane kazne za povrede odredaba Zakona o provedbi Opće uredbe i Opće uredbe ne mogu izreći tijelima javne vlasti, uključujući državna tijela, tijela državne uprave, tijela lokalne i područne (regionalne) samouprave.[43] Ta se odredba temelji na Općoj uredbi koja državama članicama omogućuje da same odluče o izricanju takvih kazni javnim tijelima.[44] U obrazloženju Zakona o provedbi Opće uredbe navodi se da bi kažnjavanje javnih tijela bilo neučinkovito jer bi se sredstva za plaćanje kazni preusmjeravala unutar državnog proračuna bez stvarnog učinka sankcioniranja.[45]

Zakonom o provedbi Opće uredbe uređena je obrada osobnih podataka u posebnim slučajevima uključujući privolu djece za usluge informacijskog društva, obradu genetskih i biometrijskih podataka, i obradu putem video nadzora. U vezi s ponudom usluga informacijskog društva izravno djeci, propisano je da je obrada osobnih podataka zakonita ako dijete ima najmanje 16 godina, dok je za mlađu djecu potrebna privola nositelja roditeljske odgovornosti.[46] Nadalje, s obzirom na posebnu rizičnost obrade genetskih podataka, Zakon o provedbi Opće uredbe zabranjuje njihovu obradu radi izračuna zdravstvenih rizika u kontekstu sklapanja ili izvršavanja ugovora o životnom osiguranju, a ta zabrana ostaje na snazi i u slučaju kada ispitanik da svoju privolu.[47] Obrada biometrijskih podataka podložna je strožim ograničenjima, no dopuštena je u svrhu evidencije radnog vremena i kontrole ulaska i izlaska iz službenih prostorija zaposlenika.[48] Također, Zakon o provedbi Opće uredbe uređuje i područje video nadzora, dopuštajući ga samo

[41] Čl.51. Opće uredbe.
[42] Čl.4. Zakona o provedbi Opće uredbe.
[43] Čl.47. Zakona o provedbi Opće uredbe.
[44] Čl.83.st.7 Opće uredbe.
[45] RH, Ministarstvo uprave, PRIJEDLOG ZAKONA O PROVEDBI OPĆE UREDBE O ZAŠTITI PODATAKA, S KONAČNIM PRIJEDLOGOM ZAKONA, Zagreb, ožujak 2018., dostupno na: https://vlada.gov.hr/UserDocsImages/2016/Sjednice/2018/04%20travnja/90%20sjednica%20VRH/90%20-%201.pdf.
[46] Čl.19. Zakona o provedbi Opće uredbe.
[47] Čl.20. Zakona o provedbi Opće uredbe.
[48] Čl.23. Zakona o provedbi Opće uredbe.

kada je nužan i opravdan za zaštitu osoba i imovine uz obvezu poštivanja prava ispitanika, osobito u kontekstu video nadzora radnih prostorija, stambenih i poslovno-stambenih zgrada, i javnih površina.[49] U skladu s odredbama Opće uredbe, Zakon o provedbi Opće uredbe propisuje i mogućnost odstupanja od pojedinih prava ispitanika, kao što su pravo pristupa osobnim podacima, pravo na ispravak, pravo na ograničenje obrade i pravo na prigovor, kada se osobni podaci obrađuju u svrhe službene statistike koju izrađuju službena statistička tijela u Republici Hrvatskoj.[50]

[49] Čl.26. Zakona o provedbi Opće uredbe.
[50] Čl.33. Zakona o provedbi Opće uredbe.

7. MEĐUNARODNI PRIJENOS PODATAKA

Opća uredba predviđa različite mehanizme koji osiguravaju da se osobni podaci, prilikom prijenosa tih osobnih podataka izvan Europske ekonomske zajednice (EEA), primjereno štite i ostaju u skladu s europskim standardima zaštite privatnosti. Ove mjere sprječavaju neovlašteno korištenje ili zloupotrebu osobnih podataka i omogućuju transparentan način prijenosa podataka. To su odluke o primjerenosti (engl. *adequacy decisions*), standardne ugovorne klauzule (engl. *standard contractual clauses*), obvezujuća korporativna pravila (engl. *binding corporate rules*), mehanizmi certificiranja (engl. *certification mechanisms*) i kodeksi ponašanja (engl. *codes of conduct*).[51]

7.1. Odluke o primjerenosti

Odluke o primjerenosti odluke su Europske komisije kojima utvrđuje ima li treća zemlja država, koja nije država članica EGP-a niti Švicarska Konfederacija[52], primjerenu razinu zaštite osobnih podataka s onom unutar EU prilikom njihova prijenosa. Ako Europska komisija zaključi da određena treća zemlja pruža primjerenu zaštitu, prijenos podataka može se odvijati bez potrebe za dodatnim mjerama zaštite što olakšava međunarodne poslovne aktivnosti i suradnju.[53]

Pri analizi razine zaštite osobnih podataka u trećim zemljama, Europska komisija razmatra različite aspekte uključujući nacionalne propise o zaštiti podataka, pravne i administrativne mjere, kao i praksu u tim zemljama. Osim toga, Komisija uzima u obzir međunarodne obveze koje ta država ima, poput članstva u međunarodnim konvencijama o ljudskim pravima, kao i mehanizme zaštite privatnosti koji su uspostavljeni unutar tih okvira.[54]

---

[51] European Commission, *Digital Single Market - Communication on Exchanging and Protecting Personal Data in a Globalised Worls Questions and Answers,* dostupno na: https://ec.europa.eu/commission/presscorner/detail/en/memo_17_15 (15. rujna 2024.).
[52] Čl.3. Zakona o strancima, Narodne novine br. 133/2020, 2. prosinca 2020.
[53] Čl.45.,st.1. Opće uredbe.
[54] Čl.45.,st.2. Opće uredbe.

Do sada odluke o primjerenosti postojale su samo u komercijalne svrhe, ali Komisija je po novome ovlaštena donositi i odluke i u području provedbe prava.

Države za koje je trenutno utvrđeno da imaju podjednaku razinu zaštite kao EU su – Andora, Argentina, Kanada, Farski Otoci, Guernsey, Izrael, Isle of Man, Jersey, Novi Zeland, Švicarska, Urugvaj i Sjedinjene Američke Države.

Dakako, odluke o primjerenosti ne mogu biti trajne i nepromjenjive, stoga ih Komisija provjerava barem svake četiri godine.[55] Ova redovita provjera ključna je zbog stalnih promjena u zakonodavnom okviru, kako na nacionalnoj, tako i na međunarodnoj razini, nove zakonske regulative ili izmjene postojećih zakona mogu utjecati na razinu zaštite podataka u određenim zemljama.

7.2. Standardne ugovorne klauzule

U nedostatku odluke o primjerenosti, prijenos podataka može se vršiti između različitih trgovačkih društava na temelju standardnih ugovornih klauzula. Ove klauzule pružaju standardizirane ugovorne odredbe koje se koriste kako bi se osigurala usklađenost s visokim standardima zaštite podataka EU prilikom prijenosa podataka u treće zemlje ili međunarodnim organizacijama. Unaprijed su definirane, a donose ih Komisija ili Nadzorno tijelo[56] koje je neovisno tijelo javne vlasti koje osigurava svaka država članica i ono je odgovorno za praćenje primjene Opće uredbe.[57] Standardne ugovorne klauzule postojale su i prije Opće uredbe, ali Opća uredba pojednostavljuje i proširuje njihovu upotrebu. U Općoj uredbi standardne ugovorne klauzule navode se kao primjer odgovarajućih zaštitnih mjera za prijenose podataka u nedostatku odluke o primjerenosti.[58] Moguće je koristiti standardne ugovorne klauzule za prijenose različitih voditelja obrade podataka što je važno za obradu podataka od strane pružatelja usluga u oblaku koji često prenose osobne podatke izvan EU iz operativnih razloga kako bi se osigurali od specifičnih rizika. Općom uredbom se i dodatno olakšava korištenje standardnih ugovornih

[55] Čl.45.,st.3. Opće uredbe.
[56] Čl.28. Opće uredbe.
[57] Čl.51. Opće uredbe.
[58] Čl.46. Opće uredbe.

klauzula jer ukida postojeći zahtjev za obavještavanje i odobravanje nacionalnih tijela za međunarodne prijenose.

7.3. Obvezujuća korporativna pravila

Obvezujuća korporativna pravila mogla su se primjenjivati samo unutar korporacije, a primjenom Opće uredbe, mogu se koristiti i za prijenose između različitih korporacija koje sudjeluju u zajedničkoj ekonomskoj aktivnost kao što su različiti prijevoznici koji pripadaju istoj zrakoplovnoj alijansi.[59] Na taj način omogućavaju veću fleksibilnost u suradnji poslovnih subjekata koji dijele podatke radi ostvarenja zajedničkog cilja poboljšanja usluga ili optimizacija procesa. Obvezujuća korporativna pravila odobrava nadzorno tijelo. [60]

Za društvene mreže, koje često djeluju na globalnoj razini i obrađuju ogromne količine osobnih podataka korisnika, obvezujuća korporativna pravila su ključna za zakonit prijenos podataka između njihovih podružnica i povezanih subjekata u različitim zemljama, uključujući i one izvan Europskog gospodarskog prostora. Velike društvene mreže, poput Facebooka ili Instagrama, imaju podružnice diljem svijeta. Obvezujuća korporativna pravila omogućuju im da prenose podatke korisnika (primjerice objave, slike, podatke o profilima) između svojih ureda u različitim zemljama, osiguravajući usklađenost s Općom uredbom. Korištenjem obvezujućih korporativnih pravila, društvene mreže osiguravaju zaštitu podataka korisnika čak i kada se ti podaci obrađuju u zemljama koje nemaju jednako stroge zakone o zaštiti podataka kao Europska unija.

[59] Čl.47. Opće uredbe.
[60] Čl.47. Opće uredbe.

7.4. Odobreni kodeksi ponašanja i certifikati akreditirani od treće strane

Odobreni kodeksi ponašanja prema Općoj uredbi pomažu organizacijama i industrijama uskladiti svoje prakse zaštite podataka s propisima.[61] Olakšavaju primjenu Opće uredbe voditeljima obrade podataka, posebice malim i srednjim poduzećima što je u pravilu 99,8% pravnih subjekata u Europskoj uniji.[62] Ti voditelji obrade podataka teško bi se sami mogli nositi s novim pravnim zahtjevima samostalno, a skupina voditelja obrade može imati slične ili jednake postupke obrade podataka. Stoga poduzetnici unutar istog gospodarskog sektora, industrije ili vrste organizacije mogu primijeniti jedinstven kodeks ponašanja. Primjenjuju se dobrovoljno, a odobrava ih nadzorno tijelo za zaštitu podataka kao što je Agencija za zaštitu osobnih podataka u Hrvatskoj ili Europski odbor za zaštitu podataka na razini Europe.[63]

Društvene mreže obrađuju velike količine osobnih podataka korisnika. Odobreni kodeksi ponašanja pružaju detaljne smjernice specifične za sektor kako bi društvene mreže mogle pravilno primijeniti Opću uredbu u svom poslovanju. Odobreni kodeksi ponašanja također pomažu standardizirati načine na koje različite društvene mreže primjenjuju pravila zaštite osobnih podataka, čime se osigurava konzistentniji pristup unutar industrije. To korisnicima olakšava razumijevanje svojih prava na različitim platformama. Budući da društvene mreže djeluju globalno, odobreni kodeksi ponašanja mogu im pomoći u usklađivanju s Općom uredbom dok istovremeno zadovoljavaju specifične zahtjeve različitih tržišta.

Certifikati akreditirani od treće strane slični su kodeksima ponašanja jer su također vanjski mehanizmi koje donose treće strane. Olakšavaju dokazivanje da je obrada podataka u skladu s Općom uredbom.[64] Certifikati sami po sebi ne dokazuju da određeni voditelj obrade podataka vodi

[61] Čl.40.,st.2. Opće uredbe.
[62] Europski parlament, Informativni članci o EU, *Mala i srednja poduzeća*, dostupno na: https://www.europarl.europa.eu/factsheets/hr/sheet/63/mala-i-srednja-poduzeca (11. siječnja 2025.).
[63] European Commission, *Codes of conduct and certification mechanisms,* dostupno na: https://ec.europa.eu/programmes/erasmus-plus/project-result-content/2cf83d56-345f-4f36-989b-8bfd8461f023/Module%206%20Codes%20of%20conduct%20and%20certification%20mechanisms.pdf.
[64] Čl.42. Opće uredbe.

obradu u skladu s Općom uredbom, ali služi kao jedan od elemenata koji se mogu koristiti za dokazivanje usklađenosti.[65]

Certifikacija je proces u kojem organizacija podliježe procjeni od strane neovisnog tijela za certifikaciju koje je akreditirano od strane nacionalnog nadzornog tijela za zaštitu podataka ili nacionalnog tijela za akreditaciju.[66] Tijekom postupka certifikacije organizacija mora dokazati da njeni procesi obrade podataka, sigurnosne prakse i politike ispunjavaju kriterije utvrđene Općom uredbom. Kriteriji za certifikaciju prethodno su odobreni od strane nadzornih tijela i prilagođeni specifičnostima sektora ili vrsti obrade podataka.[67] Certifikat koji se izdaje vrijedi najviše tri godine, nakon čega se mora obnoviti.[68]

Certifikati omogućuju društvenim mrežama da pokažu korisnicima, poslovnim partnerima i regulatorima da su njihove prakse obrade podataka u skladu s Općom uredbom. To je posebno važno zbog velike pozornosti koju društvene mreže dobivaju u vezi s privatnošću i zaštitom osobnih podataka.

7.5. Odstupanja za posebne situacije

U određenim situacijama u kojima ne postoji odluka Komisije o primjerenosti stupnja zaštite podataka u trećim zemljama niti je voditelj ili izvršitelj obrade predvidio odgovarajuće zaštitne mjere prethodno navedene, postoje navedene iznimke u je kojima ipak moguć prijenos osobnih podataka u treću zemlju. Ispitanik u tim situacijama mora dati privolu koja je prema Općoj uredbi definirana kao: dobrovoljno, posebno, informirano i nedvosmisleno izražavanje želja

[65] European Data Protection Board, Guidelines 172018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679, 25. svibnja 2018., dostupno na: https://www.edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_1_2018_certification_en.pdf (1. listopada 2024.).
[66] Čl.42. Opće uredbe.
[67] Čl.47. Opće uredbe.
[68] Čl.42.,st.7. Opće uredbe.

ispitanika kojim on izjavom ili jasnom potvrdnom radnjom daje pristanak za obradu osobnih podataka koji se na njega odnose.[69]

Privola mora biti slobodno dana, što znači da korisnik ne smije biti pod pritiskom, prisilom ili doveden u situaciju neravnoteže moći. Društvene mreže moraju omogućiti korisnicima da odbiju davanje privole bez negativnih posljedica, poput gubitka pristupa osnovnim funkcijama platforme. Primjerice, korisnici trebaju imati mogućnost korištenja osnovnih usluga društvene mreže iako ne pristanu na dijeljenje svojih podataka za potrebe ciljanja oglasa. Privola mora biti specifična, što znači da mora biti vezana uz jasno definiranu svrhu obrade podataka. Društvene mreže ne smiju tražiti opću privolu za sve vrste obrade podataka, već moraju jasno navesti svrhu za svaku pojedinačnu obradu. Posebna privola mora biti osigurana za praćenje korisničkih aktivnosti radi personaliziranog oglašavanja i za prijenos podataka u treće zemlje.[70] Informiranost privole zahtijeva da korisnicima budu dostupne jasne i razumljive informacije o tome koje podatke društvene mreže prikupljaju, kako će ih obrađivati i s kim će ih dijeliti. Korisnici moraju biti svjesni implikacija davanja privole, uključujući rizike prijenosa njihovih podataka u treće zemlje koje nemaju usporedivu razinu zaštite osobnih podataka. Društvene mreže moraju transparentno objasniti moguće posljedice takvog prijenosa.[71]

Privola mora biti nedvosmislena, što znači da korisnici moraju izričito dati svoj pristanak putem aktivne radnje, poput označavanja kvačice ili klika na opciju „prihvaćam“. Unaprijed označene kvačice ili pretpostavljen pristanak ne smatraju se valjanom privolom prema Općoj uredbi. Na društvenim mrežama, korisnici moraju imati mogućnost aktivnog pristanka na uvjete obrade podataka tijekom registracije ili u postavkama profila.

Dodatno, privola mora biti povratna i lako opoziva. Korisnici moraju imati pravo povući svoju privolu u bilo kojem trenutku, a društvene mreže dužne su osigurati jednostavan i jasan postupak za povlačenje privole.[72]

---

[69] Čl.4. Opće uredbe.
[70] Čl.7. Opće uredbe.
[71] Čl.13. Opće uredbe.
[72] Čl.7.,st.3. Opće uredbe.

Privola je ključna i u kontekstu međunarodnog prijenosa podataka. Ako društvene mreže prenose podatke korisnika izvan Europske unije, primjerice u SAD, one moraju osigurati da korisnici budu jasno informirani o rizicima takvog prijenosa. U slučaju zemalja koje nemaju usporedivu razinu zaštite osobnih podataka, poput SAD-a, privola mora biti specifična i informirana, a korisnicima se mora objasniti svrha prijenosa, primatelji podataka i mehanizmi zaštite koji su poduzeti.

8. AKTIVNOSTI EUROPSKE KOMISIJE VEZANE UZ PRIJENOS PODATAKA IZMEĐU EU-SAD

Europska komisija predstavlja izvršno tijelo EU, središnje odgovorno za oblikovanje, predlaganje i provedbu politika EU-a. Osnovna funkcija Europske komisije je predlaganje zakonodavnih akata. Komisija inicira i oblikuje prijedloge zakona koji su usklađeni s ciljevima EU-a i potrebama njenih građana. Ti prijedlozi prolaze kroz proces odobravanja u Europskom parlamentu i Vijeću EU-a čime se osigurava demokratski legitimitet donošenja zakona. Jedan od najznačajnijih zakonodavnih akata koji je predložila Komisija je Opća uredba.

Komisija također osigurava pravilnu provedbu zakona EU-a u svim državama članicama. Kao čuvarica Ugovora o funkcioniranju Europske unije, nadgleda usklađenost nacionalnih zakonodavstava s pravnim okvirom EU-a. U slučaju povrede zakona, Komisija može pokrenuti pravni postupak protiv država članica pred Sudom Europske unije kako bi osigurala poštivanje pravila. Još jedna značajna zadaća Komisije je upravljanje proračunom EU-a.

Na međunarodnoj razini, Europska komisija zastupa EU u pregovorima i sklapanju međunarodnih sporazuma. Primjer toga su trgovinski ugovori i sporazumi o zaštiti osobnih podataka s trećim zemljama. Komisija ima ključnu ulogu u osiguravanju da takvi sporazumi budu u skladu s visokim standardima zaštite osobnih podataka uspostavljenim u EU-u.[73] Komisija je zadužena za donošenje odluka o primjerenosti, a razvila je i odobrila različite mehanizme prijenosa osobnih podataka između Europske unije i Sjedinjenih Američkih Država

Prijenos osobnih podataka između Europske unije i Sjedinjenih Američkih Država (SAD) dugo je bio izazov zbog različitih pristupa zaštiti privatnosti i podataka u ta dva pravna sustava. Dok EU ima stroge i jedinstvene standarde zaštite podataka temeljene na Općoj uredbi, SAD se oslanja na sektorski pristup regulaciji zaštite osobnih podataka gdje različiti sektori primjenjuju različita pravila, a jedinstveni nacionalni zakon o zaštiti podataka ne postoji. Ta razlika u

[73] Europska komisija, *O Europskoj komisiji*, dostupno na: https://commission.europa.eu/about_hr (12. siječnja 2025.).

regulativnom pristupu stvara brojne pravne i operativne prepreke za trgovačka društva koje posluju na obje strane Atlantskog oceana.

Kako bi riješile ove probleme, Europska komisija i vlasti SAD-a pokušale su uspostaviti različite mehanizme za osiguranje sigurnog prijenosa osobnih podataka. Među njima bili su okvir Sigurne luke, Sustav zaštite privatnosti i najnoviji Okvir EU-SAD za zaštitu podataka. Međutim, svaki od tih mehanizama suočio se s kritikama i izazovima što ukazuje na složenost usklađivanja dvaju pravnih sustava koji imaju različite prioritete u zaštiti podataka i nacionalnoj sigurnosti.

8.1. Sigurna luka (engl. Safe Harbour Framework)

Do odluke Europskog suda pravde iz 2015. godine zaštita prijenosa podataka iz EU u SAD osiguravala se putem Sigurne luke koji se temeljio na Direktivi 95/46/EZ Europskog parlamenta i Vijeća od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom podataka i o slobodnom protoku takvih podataka.[74] Prema toj direktivi, država članica Europske Unije, mora osigurati da 3. država u koju se prenose podaci koji se obrađuju ili se trebaju obrađivati nakon prijenosa, ima primjerenu razinu zaštite podataka. Pri ocjenjivanju razine zaštite podataka, sve okolnosti trebaju se uzeti u obzir.

2000. godine Europska komisija donosi odluku o primjerenosti zaštite koju donose principi Sigurne luke i uključuje česta pitanja koja postavlja Ministarstvo trgovine Sjedinjenih Američkih Država.[75] Ta odluka primjenjuje se samo na primjerenost zaštite koju pružaju Sjedinjene Američke Države.

Također 2000. godine, Ministarstvo trgovine SAD-a izdalo je USA Harbor Privacy Principles koji su predstavljali osnovu za tadašnji okvir Sigurne luke (Safe Harbor) između Europske unije i Sjedinjenih Američkih Država. Ovi principi bili su osmišljeni kako bi uskladili

[74] Direktiva 95/46/EZ Europskog parlamenta i Vijeća od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom podataka i o slobodnom protoku takvih podataka, SL L 281, 23.11.1995, p. 31–50 (dalje u tekstu: Direktiva 95/46).
[75] 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441), OJ L 215, 58/08/2000, p.7-47.

prakse zaštite osobnih podataka američkih organizacija s europskim standardima utvrđenima Direktivom 95/46/EZ o zaštiti podataka.[76] Cilj je bio omogućiti siguran prijenos osobnih podataka između EU i SAD-a. Ključni elementi USA Harbor Privacy Principles su:

1. Obavijest (Notice): organizacije su bile obvezne obavijestiti pojedince o prikupljanju njihovih podataka, svrsi obrade, vrstama podataka koji se prikupljaju te trećim stranama kojima se podaci mogu otkriti. Također, trebale su pružiti informacije o kontaktima za podnošenje upita ili prigovora.

2. Izbor (Choice): pojedinci su imali pravo odlučiti hoće li njihovi podaci biti korišteni za sekundarne svrhe ili dijeljeni s trećim stranama. Organizacije su bile obvezne poštovati odluke pojedinaca u vezi s takvim korištenjem.

3. Daljnji prijenos (Onward Transfer): prijenos osobnih podataka trećim stranama bio je dopušten samo ako su te strane bile usklađene s principima *sigurne luke* ili su se pridržavale drugih standarda zaštite podataka koji su kompatibilni s europskim zakonodavstvom.

4. Pristup (Access): organizacije su morale omogućiti pojedincima pristup njihovim osobnim podacima, kao i pravo na ispravak, izmjenu ili brisanje netočnih ili nepotpunih podataka.

5. Sigurnost (Security): organizacije su bile obvezne osigurati odgovarajuću zaštitu podataka od gubitka, zloupotrebe, neovlaštenog pristupa, otkrivanja, izmjene ili uništenja.

6. Integritet podataka (Data Integrity): prikupljeni podaci morali su biti relevantni i točni u odnosu na svrhe za koje su prikupljeni te redovito ažurirani.

7. Provedba (Enforcement): organizacije su morale osigurati mehanizme za nadzor pridržavanja principa, rješavanje pritužbi pojedinaca te sankcioniranje neusklađenosti.

Američke organizacije koje su se željele uključiti u okvir Sigurne luke mogle su to učiniti dobrovoljno, no prijavom su postajale zakonski obvezane poštivati navedene principe.

[76] 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441), OJ L 215, 58/08/2000, p.7-47.

Organizacije su morale javno objaviti svoje pridruženje Sigurnoj luci, a nadzor nad provedbom osiguravale su institucije poput Federalne trgovinske komisije (dalje u tekstu: FTC).

Nakon Schrems I. odluke koja je označila kraj Sigurne luke, donosi se novi okvir poznat kao EU-SAD Štit privatnosti (*Privacy Shield*) koji je pokušao unaprijediti standarde zaštite podataka.

8.2. Krovni sporazum EU i SAD-a (engl. Umbrella Agreement)

Krovni sporazum EU i SAD-a iz 2016. godine je sporazum Europske unije i SAD-a koji se odnosi na zaštitu podataka koji se razmjenjuju između dviju strana u kontekstu provedbe zakona i pravosudne suradnje kako bi se olakšala suradnja policijskih i pravosudnih tijela u borbi protiv organiziranog kriminala, terorizma i *cyber* kriminala.[77] Osobni podaci razmijenjeni između EU-a i SAD-a za potrebe provođenja zakona moraju biti zaštićeni na jednak način, neovisno o tome je li osoba građanin EU-a ili SAD-a. Sporazum je potpisan 2016. godine nakon višegodišnjih pregovora kao reakcija na zabrinutost u EU oko zaštite osobnih podataka u SAD-u. Cilj je bio stvoriti pravni okvir koji će osigurati ravnotežu između potreba za razmjenom podataka radi sigurnosti i borbe protiv kriminala s jedne strane i zaštite privatnosti pojedinaca s druge strane.

Velika novost koju sporazum uvodi je mogućnost sudske zaštite građana EU u SAD-u.

8.3. Schrems I. odluka

Europski sud pravde 6. listopada 2015. na temelju prigovora austrijskog državljana Maximilian Schremsa, po kojem je odluka i dobila ime protiv Facebooka[78], odlučuje da odluke o primjerenosti nisu valjane što znači da su pravila Sigurne luke nedovoljna za primjerenu zaštitu

[77] Europska komisija, Statement by Commissioner Vera Jourova on the European Parliament consent vote on the conclusion of the EU-U.S data protection "Umbrella Agreement", 1. prosinca 2016., dostupno na: https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_16_4182.
[78] Maximilian Schrems protiv Data Protection Commissioner, uz sudjelovanje Digital Rights Ireland Ltd, ECLI:EU:C:2015:650 , 6. listopada 2015.

podataka koji se prenose iz EU. Schrems je podnio prigovor protiv Irskog nadležnog tijela za zaštitu podataka u sumnji da Facebook Ireland prenosi podatke u SAD, a SAD u svjetlu Snowdenovih otkrića ne pruža dovoljno razinu zaštite građanima EU.

8.3.1. Snowdenova otkrića

Edward Snowden, bivši suradnik američke Nacionalne sigurnosne agencije (dalje u tekstu: NSA), 2013. godine otkrio je tajne dokumente koji su razotkrili masovni nadzor i špijunske aktivnosti koje je američka vlada provodila na globalnoj razini.[79] Ova otkrića izazvala su globalan šok i otvorila raspravu o privatnosti, vladinom nadzoru, ljudskim pravima i nacionalnoj sigurnosti. Snowden je otkrio da NSA provodi širok nadzor nad telefonskim razgovorima, elektroničkom poštom i internetskom aktivnošću, ne samo u Sjedinjenim Američkim Državama, već i diljem svijeta. Otkrio je da NSA prati komunikacije milijuna ljudi putem programa kao što su *PRISM*, koji je omogućavao prikupljanje podataka izravno od velikih tehnoloških kompanija kao što su Google, Facebook, Microsoft i Apple.

8.3.2. PRISM program

Tajni program nadzora koji je pokrenula američka NSA u suradnji sa Saveznim istražnim uredom (dalje u tekstu: FBI), prvi put otkriven je 2013. godine kroz Snowdenova otkrića i otada se smatra jednim od najkontroverznijih elemenata globalnog nadzora. *PRISM* je uspostavljen kako bi omogućio NSA-i prikupljanje i analiziranje podataka o komunikacijama korisnika s ciljem identifikacije i praćenja terorističkih prijetnji, *cyber* kriminala i drugih sigurnosnih izazova. Program je navodno usmjeren na nadzor komunikacija osoba izvan SAD-a, iako su u procesu nadzora neizbježno prikupljeni i podaci američkih građana. Putem *PRISM*-a, NSA je mogla pristupiti širokom rasponu podataka, uključujući e-poruke, video pozive, glasovne komunikacije,

[79] Macaskill, E.; Dance, G., *NSA files: decoded, What the revelations mean for you*, 1. studenoga 2013., dostupno na: https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1 (28. rujna 2024.).

fotografije, *chat* razgovore, povijest pretraživanja i druge osobne informacije. Podaci su se prikupljali direktno s poslužitelja pružatelja usluga što je izazvalo veliku zabrinutost u pogledu privatnosti.[80] *PRISM* program djelovao je na temelju zakona poznatog kao "*FISA Amendments Act"* iz 2008. godine[81], konkretno njegovog odjeljka 702. Ovaj zakon omogućuje američkim obavještajnim agencijama da prikupljaju strane obavještajne podatke o osobama izvan SAD-a bez prethodnog sudskog naloga. Međutim, ako bi podaci američkih građana bili uključeni, nadzorna agencija morala bi poduzeti korake da zaštiti privatnost tih podataka. *PRISM* i drugi programi masovnog nadzora potaknuli su rasprave o potrebi reforme zakona o nadzoru. "*USA Freedom Act"* iz 2015. godine donio je određene promjene u načinu na koji NSA prikuplja i pohranjuje podatke, osobito ograničivši masovno prikupljanje meta-podataka o telefonskim pozivima.[82]

PRISM program otvorio je globalnu raspravu o ravnoteži između nacionalne sigurnosti i prava na privatnost u digitalnom dobu. Iako se taj propis temelji na nužnosti sredstava za borbu protiv terorizma i međunarodnih prijetnji, obavještajne agencije prešle su granice prihvatljivog nadzora, dovodeći u pitanje povjerenje među vladama, tehnološkim društvima i javnosti.

Ova otkrića također su potaknula globalne inicijative za jačanje zaštite privatnosti.

8.3.3. Schrems protiv Facebook Ireland

Od 2011. godine, irski Povjerenik za zaštitu podataka zaprimio je ukupno 23 pritužbe u razdoblju od dvije godine. Međutim, Povjerenik je odbio istražiti prijavljene povrede jer je Europska komisija donijela Odluku 2000/520 prema kojoj je SAD uspostavio Sigurnu luku pa Povjerenik nije ovlašten preispitivati tu odluku jer nacionalna regulatorna tijela nisu ovlaštena

[80] Britannica, National Security Agency, 9. listopada 2024., dostupno na: https://www.britannica.com/technology/computer-security.
[81] FISA Amendments Act of 2008, H.R.6304, dostupno na: https://www.congress.gov/bill/110th-congress/house-bill/6304.
[82] USA Freedom Act of 2015, H.R. 2048, dostupno na: https://www.congress.gov/114/bills/hr2048/BILLS-114hr2048eh.pdf.

preispitivati odluke tijela EU.[83] Kao rezultat toga, Maximilian Schrems pokrenuo je pravni postupak protiv Povjerenika.

Podnio je tužbu pred Zemaljskim građanskim sudom u Beču protiv Facebook Ireland Limited.[84] Također je na internetu objavio poziv ostalim korisnicima Facebooka da mu se pridruže ako smatraju da je njihovo pravo jednako povrijeđeno. Predmet je došao do Vrhovnog suda koji je naposlijetku uputio zahtjev za prethodnu odluku Sudu Europske unije.

Visoki sud Irske, pred kojim se vodio postupak, želi utvrditi sprječava li odluka Komisije nacionalno nadzorno tijelo da istraži pritužbu u kojoj se tvrdi da treća zemlja ne osigurava odgovarajuću razinu zaštite i, ako je potrebno, obustavi osporeni prijenos podataka. Sud europske unije istaknuo je da postojanje odluke Europske komisije kojom se utvrđuje da treća zemlja osigurava odgovarajuću razinu zaštite osobnih podataka ne može eliminirati ili smanjiti ovlasti nacionalnih nadzornih tijela.[85] Sud je naveo da nijedna odredba Direktive 95/46 ne sprječava nacionalna nadzorna tijela u nadzoru nad prijenosom osobnih podataka u treće zemlje, čak i ako je donesena odluka Komisije. Nacionalna nadzorna tijela, kada razmatraju pritužbu, moraju biti u mogućnosti neovisno ispitati usklađenost prijenosa podataka s Direktivom 95/46. Međutim, samo Sud Europske unije ima ovlast proglasiti nevažećom odluku EU-a, poput odluke Komisije. Ako nacionalno tijelo ili osoba koja je podnijela pritužbu smatraju da je odluka Komisije nevažeća, moraju moći pokrenuti postupak pred nacionalnim sudovima, koji potom mogu uputiti slučaj Sudu Europske unije. Konačna odluka o valjanosti odluke Komisije pripada Sudu Europske unije.

Sud Europske unije utvrdio je da američki zakoni o zaštiti podataka ne pružaju istu razinu zaštite kao što to čini Opća uredba u EU. Konkretno, zabrinutost je postojala zbog mogućnosti da američke vlasti imaju pristup osobnim podacima građana EU-a bez primjerene pravne zaštite, prema sporazumu Sigurna luka, građani EU-a nisu imali adekvatne mogućnosti za traženje pravde ili zaštite svojih prava u SAD-u. U presudi se istaknulo da američki zakoni, uključujući zakone o

[83] Odluka Europske komisije C(2000) 2441, L 215/7, Službeni list Europske unije, 26. srpnja 2000.
[84] Facebook Ireland Limited sa sjedištem u Irskoj društvo je kći Facebook Inc. sa sjedištem u SAD-u.
[85] Maximilian Schrems protiv Data Protection Commissioner, uz sudjelovanje Digital Rights Ireland Ltd, C-362/14, 6. listopada 2015. dostupno na: https://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=HR&mode=lst&dir=&occ=first&part=1&cid=5146896.

nacionalnoj sigurnosti, omogućuju širok pristup podacima koji se prikupljaju od strane vlade što može dovesti do povreda privatnosti građana EU-a. Sud europske unije smatrao je da ti zakoni ne pružaju dovoljno visok stupanj zaštite protiv neovlaštenog pristupa podacima i stoga poništio odluku Europske komisije kojom je Sigurna luka proglašena primjerenom.

8.4. EU-SAD sustav zaštite privatnosti (engl. Privacy Shield)

2016. godine na temelju odluke Europskog suda pravde iz 2015. godine da je dotadašnja zaštita Sigurne luke nevaljana i prema kojoj je potrebno donijeti nove mehanizme zaštite prijenosa podataka između Europske Unije i Sjedinjenih Američkih Država, započinje se rad na novom okviru zaštite podataka transatlantskih prijenosa podataka u komercijalne svrhe koji je rezultirao Sustavom zaštite privatnosti. [86] Europski sud u svojoj je odluci donio i zahtjeve koje je potrebno ispuniti u novom sustavu zaštite koje je Sustav zaštite privatnosti reflektirao.[87]

Sustav je postavljao strože uvjete u odnosu na Sigurnu luku uključujući zahtjeve za veću transparentnost, obavezu poduzeća da pružaju informacije o tome kako prikupljaju i koriste osobne podatke, i mehanizme za zaštitu prava ispitanika.

Ministarstvo trgovine SAD-a i Federativna trgovinska komisija SAD-a dobili su veliku ulogu u nadzoru i primjeni novog sustava zaštite, kao i obvezu suradnje s europskim tijelima za zaštitu podataka.

Iako javne vlasti i dalje mogu imati pristup osobnim podacima u svrhu nacionalne sigurnosti, pristup mora biti ograničen jasnim i preciznim uvjetima, ograničenjima i nadzorom. Javne vlasti ne mogu imati opći pristup podacima.

---

[86] Europska komisija, *EU-U.S. Privacy Shield: Frequently Asked Questions*, 12. srpnja 2016., dostupno na: https://ec.europa.eu/commission/presscorner/detail/hr/memo_16_2462.

[87] Maximilian Schrems protiv Data Protection Commissioner, uz sudjelovanje Digital Rights Ireland Ltd, C-362/14, 6. listopada 2015. dostupno na: https://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=HR&mode=lst&dir=&occ=first&part=1&cid=5146896.

Sustav zaštite privatnosti omogućio je prijenos osobnih podataka iz EU-a u SAD bez potrebe za dodatnim pravnim mjerama pod uvjetom da su američke tvrtke sudjelovale u programu i poštovale načela Sustava zaštite privatnosti. Američke vlasti, uključujući Ministarstvo trgovine, bile su odgovorne za praćenje usklađenosti kompanija s načelima Sustava zaštite privatnosti. Ovo je uključivalo provođenje revizija i nadzor kompanija koje su se prijavile.

Načela Sustava zaštite privatnosti uključuju stroge obveze za kompanije koje obrađuju podatke, a Ministarstvo trgovine SAD-a redovito će pregledavati sudionike kako bi osiguralo da se pridržavaju pravila o zaštiti podataka. Sporazum je transparentan i uključuje mehanizme nadzora, uz mogućnost sankcija i uklanjanja kompanija s popisa Sustava zaštite privatnosti ako se pravila ne poštuju. SAD se obvezao održavati ažuriran popis članova Sustava zaštite privatnosti i ukloniti kompanije koje više nisu dio tog okvira. Ministarstvo trgovine osigurat će da tvrtke koje više nisu članice Sustava zaštite privatnosti i dalje primjenjuju njegova načela na osobne podatke koje su primile dok su bile članice sve dok zadržavaju te podatke.

Uvjeti za prijenos podataka trećim stranama stroži su, a treće strane moraju osigurati istu razinu zaštite ili obavijestiti kompanije ako više nisu u mogućnosti to činiti. Ograničenja zadržavanja podataka sada su jasnija, omogućujući kompanija da čuvaju podatke samo dok su potrebni za svrhu prikupljanja.

Da bi bila podobna za samocertificiranje prema Sustavu zaštite privatnosti, kompanija u SAD-u mora biti podložna istražnim i provedbenim ovlastima FTC-a ili Ministarstva prometa SAD-a (dalje u tekstu: DoT). U budućnosti se mogu uključiti i druga američka regulatorna tijela. To znači da, primjerice, neprofitne organizacije, banke, osiguravajuće tvrtke i pružatelji telekomunikacijskih usluga (u vezi s aktivnostima zajedničkih operatera) koji ne potpadaju pod nadležnost FTC-a ili DoT-a ne mogu samocertificirati prema Sustavu zaštite privatnosti.[88]

U vezi s pristupom podacima od strane vlade SAD-a, Ured direktora Nacionalne obavještajne službe dao je pisane obveze da neće biti neselektivnog masovnog nadzora podataka prenesenih u SAD u okviru sporazuma. Prikupljanje podataka u velikom obujmu može se koristiti

[88] Europski odbor za zaštitu podataka, *EU-U.S. Data privacy framework, F.A.Q. For European Business*, 16. srpnja 2024., dostupno na: https://www.edpb.europa.eu/system/files/2024-07/edpb_dpf_faq-for-businesses_en.pdf.

samo pod specifičnim uvjetima, uz minimiziranje nepotrebnih informacija i postojanje zaštitnih mjera. Također, Državni tajnik John Kerry obvezao se uspostaviti institut pravobranitelja koji će neovisno razmatrati pritužbe građana EU-a vezane uz nacionalnu sigurnost i osigurati da se zakoni poštuju ili ispravljaju u slučaju kršenja.

Kako bi se osiguralo pravilno funkcioniranje sporazuma, predviđena je godišnja zajednička revizija koju će provoditi Europska komisija i Ministarstvo trgovine SAD-a, uz sudjelovanje stručnjaka za nacionalnu sigurnost i europskih tijela za zaštitu podataka. Sustav zaštite privatnosti kontinuirano će se pregledavati kako bi se osigurala adekvatna razina zaštite podataka, a u slučaju da to više ne bude slučaj, Europska komisija poduzet će odgovarajuće mjere uključujući suspenziju odluke o primjerenosti.

Svaki građanin koji smatra da su njegovi podaci zloupotrijebljeni u okviru Sustava zaštite privatnosti, imat će nekoliko pristupačnih načina za rješavanje sporova. U idealnom slučaju, pritužba će biti riješena od strane same kompanije. Kompanije koje sudjeluju u Sustavu zaštite privatnosti mogu izabrati između besplatnog alternativnog rješavanja sporova ili dobrovoljnog podvrgavanja nadzoru europskih tijela za zaštitu podataka. Građani također mogu uputiti svoje pritužbe tijelima EU-a za zaštitu podataka koja će ih proslijediti Ministarstvu trgovine SAD-a i/ili FTC-u kako bi osigurali istragu i rješavanje pritužbi. Ovi slučajevi trebaju biti riješeni u razumnom vremenskom okviru s rokom za odgovor Ministarstva trgovine SAD-a u slučajevima koje DPA proslijedi SAD-u, dok je FTC obećao dati prioritet pritužbama građana.

Ako nijedan drugi mehanizam ne riješi slučaj, kao posljednja mogućnost bit će dostupna arbitraža. U slučaju pritužaba koje se odnose na prijenos podataka iz sigurnosnih razloga, građanima će biti na raspolaganju pravobranitelj koji je neovisan o američkim obavještajnim službama. Tijekom procesa usvajanja dodatno je pojašnjena funkcija i neovisnost pravobranitelja, osobito njegova suradnja s drugim neovisnim tijelima nadležnim za istrage.

8.5. Schrems II. odluka

Nakon što je Europski sud 2015. donio odluku da je Sigurna luka nedovoljna za primjerenu zaštitu podataka koji se prenose iz EU u SAD, uveo se novi mehanizam zaštite Sustav zaštite privatnosti 1. kolovoza 2016. godine. Time se obuhvaćeni svi propusti Sigurne luke, ali je Europski parlament izrazio svoje nezadovoljstvo[89], a i Europski odbor za zaštitu podataka kritizirao je Sustav zaštite privatnosti.[90] I predsjednik Komisije za ljudske slobode Europskog parlamenta također je kritizirao Sustav zaštite privatnosti nakon posjeta SAD-u. Europska komisija odbila je sve kritike uvjeravajući sve da je zaštita podataka SAD-u primjerena nakon treće godišnje evaluacije Sustava zaštite privatnosti.[91]

Maximilan Schrems krajem 2015. godine preformulirao je prigovor tako da je tvrdio da nadzorni programi SAD-a miješaju se s pravom na privatnost i zaštitu podataka kao i sudsku zaštitu što znači da se prijenos podataka u SAD ne može opravdati.[92] Za vrijeme postupka, Sustav zaštite privatnosti postao je relevantan za slučaj, što je potaknulo Sud Europske unije da se očituje i o valjanosti tog instrumenta.

Dana 16. srpnja 2020., Sud europske unije proglasio je nevažećom odluku Europske komisije o Sustavu zaštite privatnosti i potvrdio valjanost standardnih ugovornih klauzula uz postavljanje strožih uvjeta za prijenose temeljene na standardnim ugovornim klauzulama.

Programi zaštite u SAD-u, kao što su *PRISM* i *UPSTREAM*, nemaju ograničenja da ne diraju u osobne podatke, odnosno da se obrađuju samo u situacijama kad je to nužno. Ti programi imaju puno veću slobodu zadiranja u osobne podatke, tako da se zaštita podataka prenesenih u

---

[89] Rezolucija Europskog parlamenta od 5. srpnja 2018. o primjerenosti zaštite u okviru europsko-američkog sustava zaštite privatnosti (2018/2645(RSP)).

[90] Europski parlament, *EU-US relations in data protection, AI and security: MEPs conclude visit to US*, 28. veljače 2020., dostupno na: https://www.europarl.europa.eu/news/en/press-room/20200228IPR73609/eu-us-relations-in-data-protection-ai-and-security-meps-conclude-visit-to-us (8. listopada 2024.).

[91] Europski odbor za zaštitu podataka, *EU-U.S Privacy Shiels - Third Annual Joint Review,* 12. studenoga 2019., dostupno na: https://www.edpb.europa.eu/sites/default/files/files/file1/edpbprivacyshield3rdannualreport.pdf_en.pdf (7. listopada 2024.).

[92] Data Protection Commissioner protiv Facebook Ireland Ltd, Maximmilliana Schremsa, uz sudjelovanje The United States of America, Electronic Privacy Information Centre, BSA Business Software Alliance Inc., Digitaleurope, C-311/18, 16. srpnja 2020., dostupno na: https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=hr&mode=lst&dir=&occ=first&part=1&cid=5146442.

SAD ne može smatrati jednako strogom kao u EU.[93] Dodatan problem u cijeloj situaciji je što Europski građani nemaju nikakav mehanizam zaštite protiv vlasti SAD-a, ne mogu se nikako zaštiti od povrede podataka prenesenih u SAD.

Sud je odlučio da prijenos podataka na temelju standardnih ugovornih klauzula nije nevaljan, i dalje se može provoditi, samo se prije prijenosa mora osigurati jednaka razina zaštite u SAD kao ona predviđena Općom uredbom.

Unatoč manjku reforme režima zaštite podataka u SAD-u, Europska komisija postigla je novi dogovor sa SAD-om i predstavila prijedlog za još jedan okvir EU-a i SAD-a za zaštitu podataka. Nakon što je 11. svibnja 2023. Odbor za građanske slobode, pravosuđe i unutarnje poslove (*LIBE - Committee on Civil Liberties, Justice and Home Affairs*) podnio prijedlog, Europski parlament donio je Rezolucija Europskog parlamenta od 11. svibnja 2023. o primjerenosti zaštite koju pruža okvir EU-a i SAD-a za zaštitu podataka 2023/2501 (dalje u tekstu: Rezolucija o primjerenosti zaštite) u kojoj je zaključio da se okvirom EU-a i SAD-a za zaštitu podataka ne postiže bitno ekvivalentna razina zaštite i pozvao Komisiju da nastavi pregovore sa svojim kolegama iz SAD-a, ali da se suzdrži od donošenja zaključka o primjerenosti dok se u potpunosti ne provedu sve preporuke iz Rezolucije o primjerenosti zaštite i mišljenja Europskog odbora za zaštitu podataka.[94]

Kao rezultat ovih rasprava, SAD je 7. listopada 2022. donio "*Izvršnu naredbu 14086"* pod nazivom "*Poboljšanje zaštitnih mjera za aktivnosti američke obavještajne službe (EO 14086)*" (dalje u tekstu: Izvršna naredba 14086).[95] Komisija je pažljivo analizirala američke zakone i praksu i zaključuje da SAD osigurava odgovarajuću razinu zaštite za osobne podatke i 10. srpnja 2023. usvaja treći okvir EU-a i SAD-a za zaštitu podataka, donosi novu odluku o primjerenosti.

---

[93] Bowden, Mr C., *The US surveillance programmes and their impact on EU citizens' fundamental rights,* Europski parlament, dostupno na: https://www.europarl.europa.eu/RegData/etudes/note/join/2013/474405/IPOL-LIBE_NT(2013)474405_EN.pdf (9. listopada 2024.), str. 8-9.

[94] Rezolucija Europskog parlamenta od 11. svibnja 2023. o primjerenosti zaštite koju pruža okvir EU-a i SAD-a za zaštitu podataka 2023/2501(RSP), dostupno na: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0204_HR.html.

[95] Executive Order (E.O.)14086 of October 7, 2022, on Enhancing Safeguards for United States Signals Intelligence Activities.

8.6. Novi okvir za zaštitu podataka između EU-a i SAD-a – (engl. Data Privacy Framework)

Okvir EU-SAD za privatnost podataka (dalje u tekstu: EU-SAD DPF) temelji se na sustavu certificiranja putem kojeg se američke organizacije obvezuju na skup načela privatnosti uključujući Dopunska načela (zajedno: Načela) - koja je izdalo američko Ministarstvo za trgovinu i koja su sadržana u Dodatku I ove Odluke.[96] Da bi bila prihvatljiva za certificiranje prema EU-SAD DPF-u, organizacija mora podlijegati istražnim i provedbenim ovlastima Federalne trgovinske komisije ili američkog Ministarstva prometa. Načela se primjenjuju odmah nakon certificiranja.

Američke kompanije mogu potvrditi svoje sudjelovanje u EU-SAD DPF-u obvezivanjem na poštivanje detaljnih obveza u vezi s privatnošću. Kako bi provjerili je li samo-certifikacija aktivna i primjenjiva, izvoznici podataka u Europskom gospodarskom prostoru moraju provjeriti je li kompanija u SAD-u na Popisu za EU-SAD DPF objavljenom na web stranici američkog Ministarstva trgovine.[97] Ovaj popis također uključuje registar kompanija koje su uklonjene s popisa pod nazivom neaktivni sudionici navodeći razloge njihovog uklanjanja. Izvoznik podataka iz Europskog gospodarskog prostora ne može se osloniti na EU-SAD DPF za prijenos osobnih podataka takvim kompanijama. Kompanije koje su uklonjene s Popisa EU-SAD DPF podataka moraju i dalje primjenjivati Načela EU-SAD DPF na osobne podatke primljene tijekom sudjelovanja u EU-SAD DPF-u sve dok zadrže te podatke. Za prijenos osobnih podataka tvrtkama u SAD-u koje nisu (ili više nisu) samo-certificirane prema EU-SAD DPF-u, mogu se koristiti drugi temelji za prijenos iz Poglavlja V. Opće uredbe, poput obvezujućih korporativnih pravila ili standardnih ugovornih klauzula.

Vlada SAD-a uspostavila je novi dvostupanjski mehanizam za podnošenje pritužbi s neovisnim i obvezujućim ovlastima kako bi se riješile pritužbe bilo koje osobe čiji su podaci preneseni iz Europskog gospodarskog prostora u kompanije u SAD-u u vezi s prikupljanjem i korištenjem njihovih podataka od strane američkih obavještajnih agencija.

---

[96] Europski odbor za zaštitu podataka, *op. cit.* u bilj. 39.
[97] Dostupno na: https://www.dataprivacyframework.gov/list.

Za prihvaćanje pritužbe nije potrebno da osobe dokažu da su njihovi podaci zapravo prikupljeni od strane američkih obavještajnih agencija. Pojedinci mogu podnijeti pritužbu svojoj nacionalnoj agenciji za zaštitu podataka koja će osigurati pravilno prosljeđivanje pritužbe i pružanje svih daljnjih informacija vezanih za postupak, uključujući ishod, podnositelju pritužbe. Time se osigurava da se pojedinci mogu obratiti nadležnom tijelu u svojoj zemlji, na svom jeziku. Pritužbe će Europski odbor za zaštitu podataka proslijediti SAD-u.

Pritužbe će prvenstveno istražiti službenik za zaštitu građanskih sloboda američke obavještajne zajednice. Ova osoba odgovorna je za osiguravanje usklađenosti američkih obavještajnih agencija s privatnošću i temeljnim pravima.

Pojedinci također imaju mogućnost žalbe na odluku službenika za zaštitu građanskih sloboda pred novostvorenim Sudom za reviziju zaštite podataka (dalje u tekstu: Sud za reviziju). Sud za reviziju sastavljen je od članova izvan Vlade SAD-a, koji su imenovani na temelju specifičnih kvalifikacija, a mogu biti smijenjeni samo zbog valjanih razloga i ne mogu primati upute od vlade. Sud za reviziju ima ovlasti za istraživanje pritužbi građana EU-a, uključujući pristup relevantnim informacijama od obavještajnih agencija, i može donositi obvezujuće odluke o ispravljanju. Primjerice, ako Sud za reviziju utvrdi da su podaci prikupljeni u suprotnosti s mjerama zaštite predviđenim Izvršnom naredbom 14086, može narediti brisanje podataka.

U svakom slučaju, Sud za reviziju odabrat će posebnog savjetnika s relevantnim iskustvom koji će podržati Sud za reviziju i osigurati da su interesi podnositelja pritužbe zastupljeni, i da Sud za reviziju bude dobro informiran o činjeničnim i pravnim aspektima slučaja. To će osigurati zastupljenost obje strane i uvesti važna jamstva u smislu pravičnog suđenja i odgovarajućeg postupka.

Kada službenik za zaštitu građanskih sloboda ili Sud za reviziju završi istragu, podnositelj pritužbe bit će obaviješten da nije utvrđena povreda zakona SAD-a ili da je povreda utvrđena i ispravljena. U kasnijoj fazi, podnositelj pritužbe bit će obaviješten kada informacije o postupku

pred Sudom za reviziju, poput obrazložene odluke, više ne podliježu zahtjevima povjerljivosti i mogu se odbiti.[98]

8.7. Budućnost zaštite osobnih podataka pri prijenosu EU-SAD

Nakon nekoliko pokušaja i promašaja, uspostavljen je učinkovit i održiv sustav za prijenos podataka između EU-a i SAD-a kojim su zasad zadovoljni svi uključeni koji provode zaštitu osobnih podataka kao i oni na koje se zaštita odnosi.[99] Ali upitna je njegova dugoročna održivost. Ljudi su skeptični. Schrems vjeruje da će i novi sustav pasti u vodu ako SAD ne promijeni svoj pristup privatnosti. Dok je u EU-u zaštita podataka temeljno pravo, u SAD-u se privatnost regulira fragmentirano, bez univerzalnog pravnog okvira. Vlada SAD-a prema mišljenjima mnogih koristi svoje ovlasti preširoko. Također, prema The Information Technology and Innovation Foundation, SAD bi koštalo oko 122 milijarde dolara godišnje kad bi uveli zakonodavstvo slično Općoj uredbi.[100]

[98] Provedbena odluka komisije (EU) 2023/1795 od 10. srpnja 2023. u skladu s Uredbom (EU) 2016/679 Europskog parlamenta i Vijeća o primjerenoj razini zaštite osobnih podataka u skladu s okvirom EU-a i SAD-a za privatnost podataka (C(2023)4745), L 231/118, Službeni list Europske unije.
[99] Connolly, M., *Will the EU-US Data Privacy Framework Survive Schrems III?*, 87-124 , Trinity College Law Review (Vol 27) (2024), dostupno na: https://03020cmp-y-https-heinonline-org.baze.pravo.hr/HOL/Page?collection=usjournals&handle=hein.journals/trinclr27&id=97&men_tab=srchresults (13. listopada 2024.), str. 112-116.
[100] Ibid.

9. PRIMJERI PROBLEMA U PRIJENOSU PODATAKA IZMEĐU EU-SAD

9.1. Cambridge Analytica

Prije predsjedničkih izbora u SAD-u 2016. godine, trgovačko društvo Cambridge Analytica, specijalizirana za analizu podataka sa sjedištem u Londonu, surađivala je s tadašnjim kandidatom za predsjednika Donaldom Trumpom. Trgovačko društvo je koristilo podatke o 50 milijuna korisnika Facebooka kako bi analiziralo i predvidjelo njihove političke preferencije te utjecalo na način na koji će glasati. Ono što je problematično jest da su ovi podaci prikupljeni bez znanja i pristanka korisnika što predstavlja kršenje privatnosti. Iako američki zakoni zahtijevaju od kompanija da prijave povrede zaštite podataka, u ovom slučaju nema dokaza da je Facebook obavijestio vlasti ili korisnike o ovom incidentu.

Cambridge Analytica i njegova društvo-majka Communication Laboratories (SCL) koristili su podatke 270 000 korisnika Facebooka. Neki od podataka bili su imena korisnika, lokacija, podaci o prijateljima na Facebooku i o sadržajima koji su označili sa 'sviđa mi se', sve preko naizgled bezopasne aplikacije *This Is Your Digital Life* koju je razvio Aleksandr Kogan. *This Is Your Digital Life* zabavan je test osobnosti. Kako bi pristupili testu, korisnici su morali pristati na dijeljenje svojih osobnih poruka koje su razmjenjivali s prijateljima na Facebooku. Podatke te aplikacije Kogan je dao društvu Cambridge Analytica bez dopuštenja korisnika Facebooka.

Umjesto prijave, Facebook je zatražio da Koganova aplikacija i Cambridge Analytica jamče da su podatke izbrisali.[101] Povreda je ipak utvrđena i Facebook je kažnjen s 500 000 funta prema *"Data Protection Act"*[102], propisu koje je donijelo Ujedinjeno Kraljevstvo 1998. godine.[103] To je najviši iznos za koji je Facebook mogao biti kažnjen. Taj iznos je zaista malen i teško će

[101] Whittaker, Z., *Trump-linked data firm Cambridge Analytica harvested data on 50 million Facebook profiles to help target voters*, ZDNET, 17. ožujka 2018., dostupno na: https://www.zdnet.com/article/facebook-suspends-analytics-firm-that-helped-trump-campaign/ (17. rujna 2024.).
[102] Koch, R., *The GDPR meets its first challenge: Facebook,* GDPR.EU, dostupno na: https://gdpr.eu/the-gdpr-meets-its-first-challenge-facebook/?cn-reloaded=1&cn-reloaded=1 (12. listopada 2024.).
[103] Data Protection Act 1998, c.29, srpanj 1998., dostupno na: https://www.legislation.gov.uk/ukpga/1998/29?view=plain.

motivirati društva da se pridržavaju pravila s obzirom na iznos prihoda Facebooka koji je u 2023. godini iznosio gotovo 135 milijuna američkih dolara, a zarada nešto malo više od 39 milijuna američkih dolara.[104]

9.2. Slučaj Google 2019. u Francuskoj

Slučaj Google iz 2019. godine jedan je od najpoznatijih primjera provedbe Opće uredbe. Francuski regulator za zaštitu podataka (CNIL) izrekao je Googleu kaznu od 50 milijuna eura zbog kršenja Opće uredbe što je u to vrijeme bila najveća kazna prema ovoj uredbi. Slučaj se usredotočio na način na koji je Google obrađivao osobne podatke korisnika prikupljene kroz njihove Android uređaje, osobito u kontekstu personaliziranih oglasa. Glavne pritužbe podnijele su organizacije za zaštitu privatnosti NOYB i La Quadrature du Net koje su tvrdile da Google nije osigurao potrebnu transparentnost i valjanu privolu korisnika. Glavni problemi koje je CNIL identificirao uključivali su nedostatak transparentnosti jer je korisnicima bilo teško razumjeti na koji način Google prikuplja i obrađuje njihove podatke. Informacije su bile raštrkane po različitim dokumentima i sučeljima čime je otežano jasno sagledavanje procesa. Privola korisnika za personalizirane oglase nije bila specifična i jasno dana. Google je automatski uključivao opciju za personalizirane oglase bez jasnog izbora za korisnike da daju ili uskrate privolu. Također, Google je prikupljao velike količine osobnih podataka i koristio ih za personalizaciju usluga bez dostatnog obrazloženja svrhe obrade i bez osiguranja valjane privole.

Nakon toga, Google je revidirao obavijesti o privatnosti, uključujući pojednostavljivanje informacija i pružanje jasnijih objašnjenja korisnicima o načinu obrade podataka. Dodali su opcije za lakše upravljanje privolama za oglase i pružili korisnicima veću kontrolu nad osobnim podacima. [105]

---

[104] Dixon, S. J., *Annual revenue and net income generated by Meta Platforms from 2007 to 2023*, Statista, 4. ožujka 2024., dostupno na: https://www.statista.com/statistics/277229/facebooks-annual-revenue-and-net-income/ (12. listopada 2024.).

[105] Europski odbor za zaštitu podataka, The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC, 21. siječnja 2019., dostupno na: https://www.edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en, 12. siječnja 2025.

10. AKTIVNOSTI EUROPSKOG ODBORA ZA ZAŠTITU PODATAKA

Europski odbor za zaštitu podataka neovisno je tijelo osnovano u okviru Opće uredbe. Njegova glavna svrha je osigurati dosljednu primjenu i provedbu pravila o zaštiti podataka diljem EU, kao i nadgledanje i usmjeravanje nacionalnih nadzornih tijela za zaštitu podataka. Obvezujuće odluke Europskog odbora za zaštitu podataka pravne su odluke koje se donose kako bi se osigurala usklađenost s Općom uredbom i drugim zakonima o zaštiti podataka.[106] Upućuje ih nacionalnim nadzornim tijelima u svrhu rješavanja sporova u vezi primjene Opće uredbe. Također daje opće smjernice, preporuke i najbolje prakse da rasvijetli i promovira pravila o zaštiti podataka. Daje mišljenja Europskoj komisija i nacionalnim nadzornim tijelima. Promovira i podržava suradnju nadzornih tijela.

Kada nacionalno tijelo nadzora iz jedne države članice provodi istragu ili postupak u vezi s obradom podataka koja uključuje više država, dužno je konzultirati ostale nadzorne vlasti prema mehanizmu suradnje utvrđenom u Općoj uredbi.

Ako se nadzorna tijela ne mogu dogovoriti o pitanju, Europski odbor za zaštitu podataka može preuzeti slučaj i donijeti obvezujuću odluku. Odluka se donosi nakon što se raspravlja o relevantnim čimbenicima i svim relevantnim informacijama.

[106] Europski odbor za zaštitu podataka, mrežne stranice, dostupno na: https://www.edpb.europa.eu/about-edpb/what-we-do/tasks-and-duties_en.

10.1. Odluke, opće smjernice i preporuke Europskog odbora za zaštitu podataka - važan doprinos zaštiti podataka u kontekstu društvenih mreža

10.1.1. Google

2021. godine Europski odbor za zaštitu podataka utvrdio je da Google ne obavještava na dovoljno jasan način korisnike o načinu na koji prikuplja podatke i kako se oni koriste.[107] Ova procjena dovela je do zabrinutosti oko transparentnosti u načinu na koji je Google komunicirao s korisnicima, posebno u vezi s obradom osobnih podataka. Europski odbor za zaštitu podataka istaknuo je važnost pružanja jasnih i razumljivih informacija o politikama privatnosti, kao i o tome koje vrste podataka se prikupljaju, u koje svrhe i kako se ti podaci dalje obrađuju.

10.1.2. WhatsApp - Odluka o obavijesti i transparentnosti 2021.

U 2021. godini, Europski odbor za zaštitu podataka istaknuo je da WhatsApp nije pružio jasne i razumljive informacije o načinu na koji se osobni podaci koriste, posebno u vezi s dijeljenjem podataka s drugim kompanijama unutar Facebook grupacije.[108] Ova odluka naglasila je važnost transparentnosti u komunikaciji s korisnicima ističući da korisnici imaju pravo znati kako se njihovi podaci obrađuju i s kim se dijele. Europski odbor za zaštitu podataka potaknuo je WhatsApp da poboljša svoje politike privatnosti osiguravajući da korisnici budu jasno obaviješteni o svim aspektima obrade njihovih podataka, uključujući svrhe i pravne osnove za takvo dijeljenje.

10.1.3. Odluka o pravu na pristup 2021.

U istoj godini, Europski odbor za zaštitu podataka je donio odluku koja je zahtijevala da WhatsApp osigura korisnicima jednostavan pristup svojim pravima na pristup, ispravak i brisanje

[107] Europski odbor za zaštitu podataka, Odluka br. 263 o transparentnosti i korištenju podataka korisnika od strane Googlea, 1. srpnja 2021., dostupno na: https://www.edpb.europa.eu/decision-no-263_en, (26. listopada 2024.).
[108] Europski odbor za zaštitu podataka, Binding Decision 5/2022 on the dispute submitted by the Irish SA regarding WhatsApp Ireland Limited (Art. 65 GDPR), 5. prosinca 2022., dostupno na: https://www.edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-52022-dispute-submitted_en (26. listopada 2024.).

podataka.[109] Ovo uključuje obvezu WhatsApp-a da korisnicima omogući lako ostvarenje njihovih prava prema Općoj uredbi čime se osigurava da korisnici imaju kontrolu nad svojim osobnim podacima i da mogu reagirati u slučaju nepravilnosti ili nezadovoljstva vezano uz obradu njihovih informacija.

10.1.4. WhatsApp i COVID-19

Tijekom 2020. godine, Europski odbor za zaštitu podataka naglasio je potrebu za zaštitom privatnosti korisnika prilikom korištenja aplikacija za komunikaciju, posebno u kontekstu zdravstvenih podataka povezanih s pandemijom COVID-19.[110] Europski odbor za zaštitu podataka ukazao je na važnost poštivanja Opće uredbe i prava korisnika, čak i u izvanrednim situacijama poput pandemije. Ovo je uključivalo preporuke za dodatne mjere zaštite kako bi se osiguralo da podaci o zdravlju korisnika ostanu povjerljivi i da se s njima postupa u skladu s najstrožim standardima zaštite privatnosti.

10.1.5. TikTok

Europski odbor za zaštitu podataka je također naglasio važnost zaštite osobnih podataka djece i maloljetnika.[111] Ovo uključuje potrebu za dobivanjem pristanka roditelja ili skrbnika prije obrade podataka maloljetnika kako bi se osigurala dodatna zaštita ranjivih korisnika. Ukazivao je na potrebu za provjerom dobi korisnika i implementacijom mjera za zaštitu maloljetnika od neprimjerenog sadržaja. Ove mjere usmjerene su na smanjenje rizika od izlaganja maloljetnika

[109] Europski odbor za zaštitu podataka, Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDP, 28. srpnja 2024., dostupno na: https://www.edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-12021-dispute-arisen_en (26. listopada 2024.).

[110] Europski odbor za zaštitu podataka, Statement on the processing of personal data in the context of the COVID-19 outbreak, 19. ožujka 2020., dostupno na: https://www.edpb.europa.eu/sites/default/files/files/news/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf (26. listopada 2024.).

[111] Europski odbor za zaštitu podataka, Binding Decision 2/2023 on the dispute submitted by the Irish SA regarding TikTok Technology Limited (Art. 65 GDPR), 2. kolovoza 2023., dostupno na: https://www.edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-22023-dispute-submitted_en (27. listopada 2024.).

štetnim ili neprimjerenim informacijama i osiguranje da se s njihovim podacima postupa na etički i zakonit način.

10.1.6. META

2021. godine, Europski odbor za zaštitu podataka upozorio je na rizike koji proizlaze iz dijeljenja podataka između različitih platformi i naglasio potrebu za pojašnjenjem načina na koji se ti podaci koriste.[112] Postojala je zabrinutost zbog mogućnosti zloupotrebe osobnih informacija kada se one prenose između različitih aplikacija i servisa unutar iste grupacije. Europski odbor za zaštitu podataka istaknuo je da je neophodno osigurati da korisnici budu u potpunosti informirani o tome kako se njihovi podaci dijele i koriste unutar grupe, i koje su točno svrhe obrade.

Odluka je posebno zahtijevala od Instagrama da implementira jasnije politike privatnosti koje bi korisnicima omogućile da razumiju sve aspekte obrade njihovih podataka. To uključuje detaljne informacije o načinu na koji se podaci prikupljaju, dijele i koriste, kao i o mogućim rizicima koji mogu nastati kao rezultat takvih praksi.

Osim toga, Europski odbor za zaštitu podataka potaknuo je Instagram da razmotri implementaciju dodatnih mehanizama koji bi omogućili korisnicima da imaju kontrolu nad svojim podacima, uključujući opcije za prilagodbu postavki privatnosti i davanje ili povlačenje pristanka na obradu podataka. Ovaj pristup ne samo da povećava sigurnost korisničkih informacija, već također osnažuje korisnike da aktivno sudjeluju u zaštiti svojih prava na privatnost.

[112] Europski odbor za zaštitu podataka Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subject, 8. listopada 2019., dostupno na: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf (27. listopada 2024.).

11. KOMPARATIVAN PRIKAZ PROBLEMA IZMEĐU SJEDINJENIH AMERIČKIH DRŽAVA I KINE

Sličan problemu Europske unije s prijenosom podataka u SAD, ima SAD s prijenosom podataka u Kinu u vezi TikTok društvene mreže. Ideja SAD-a bila je da vlada Kine prema svojim pozitivnim propisima može samo zahtijevati podatke od TikToka koje želi ili smatra potrebnim bez posebnih strogih uvjeta, ne bi morala ilegalno pristupiti uzimanju podataka. 2020. godine nastao je problem u vezi toga. Zasad TikTok još uvijek nije zabranjen u SAD-u, i Kina i SAD nastoje osigurati primjerenu zaštitu podataka kako bi svi bili zadovoljni. TikTok je objavio javno da vlada Kine nije ni u jednom trenutku zatražila podatke.[113]

2021. godine LinkedIn i Yahoo napustili su kinesko tržište zbog poslovnih izazova i pravnog okruženja. Nisu specificirali problem, ali mediji i znanstvenici pretpostavljaju da je to zbog velikog zahtjeva Kine da svi podaci koji se prikupljaju i obrađuju budu spremljeni unutar granica države i da se ne prenose izvan Kine. *Data Localization* pohranjivanje je i obrada podataka unutar granica države. Pravo zaštite podataka u Kini temelji se na Općoj uredbi, samo što Kina ide korak dalje i zabranjuje prijenos podataka izvan zemlje ako nema za to opravdanog razloga, a prema vladi Kine skoro nikad nema. Dok su LinkedIn i Yahoo napustili Kinu, Apple je izgradio centar za prikupljanje podataka unutar granica Kine i nastavio pružati usluge i prodavati proizvode u Kini. Uspostavljanje takvih centara skupo je pa mnoga trgovačka društva radije napuštaju tržište, izgradnja takvih centara nekima se ne isplati očito. Tako su i Amazon, Facebook i Microsoft potrošili milijarde dolara u EU. Zabrana iznošenja podataka iz države zapravo olakšava curenje podataka i *cyber* napade jer je sve na jednom mjestu, nije raštrkano po mnogim poslužiteljima. Također, takvi serveri imaju najčešće slabiju infrastrukturu i manje prihode što olakšava napadačima pristup podacima.[114]

---

[113] Hoffman, D. A., *Schrems II and TikTok: Two Sides of the Same Coin,* 14. svibnja 2021., North Carolina Journal od law & technology (Vol 22, Issue 4), dostupno na: https://03020cmp-y-https-heinonline-org.baze.pravo.hr/HOL/Page?public=true&handle=hein.journals/ncjl22&div=23&start_page=573&collection=usjournals&set_as_cursor=2&men_tab=srchresults (27. rujna 2024.), str. 601.-609.

[114] Lu, W., *Data Localization: From China and Beyond,* Indiana Journal of Global Legal Studies, 183-203, vol 31, issue 1 2024), dostupno na: https://03020cmp-y-https-heinonline-

12. ZAKLJUČAK

Zaštita osobnih podataka na društvenim mrežama i međunarodni prijenos podataka postali su temeljne teme u suvremenom digitalnom društvu. Povezanost ljudi, organizacija i država putem društvenih mreža omogućila je ubrzan razvoj globalne ekonomije, ali i otvorila brojna pitanja o sigurnosti podataka, transparentnosti obrade, kao i balansu između nacionalne sigurnosti i temeljnih prava.

Europska unija, sa svojom Općom uredbom o zaštiti podataka, postavila je zlatni standard u regulaciji privatnosti i zaštite podataka što je mnogim državama i organizacijama poslužilo kao model za izgradnju vlastitih zakonodavnih okvira. Međutim, unatoč uspjesima, primjena ovih visokih standarda u globalnom kontekstu, osobito u suradnji sa Sjedinjenim Američkim Državama, nailazi na značajne izazove. Razlike u pristupima zaštiti privatnosti – temeljno pravo u EU nasuprot fragmentiranom sektorskom pristupu u SAD-u – stvaraju nesklad koji često dovodi do pravnih nesigurnosti.

Primjeri poput Schrems I. i Schrems II. odluka ističu ključne prepreke, poput masovnog nadzora i nedostatka učinkovitih pravnih lijekova za građane EU-a. Iako je najnoviji EU-SAD DPF donio određeni napredak, njegov opstanak ovisi o spremnosti obje strane na kontinuiran dijalog i reforme. Kritike Maxa Schremsa i analize koje ukazuju na visoke troškove usklađivanja američkog zakonodavstva sa standardima Opće uredbe jasno pokazuju da će budućnost ovakvih sustava ovisiti o političkoj volji, tehničkim inovacijama i povećanju svijesti o važnosti zaštite podataka.

Društvene mreže, kao značajni subjekti u ovoj globalnoj dinamici, suočene su s dvostrukim izazovom – prilagodbom nacionalnim i međunarodnim zakonima, i osiguravanjem povjerenja svojih korisnika. Njihov poslovni model, temeljen na obradi i monetizaciji velikih količina osobnih podataka, mora se prilagoditi zahtjevima za većom transparentnošću, specifičnom i informiranom privolom te kontrolom korisnika nad vlastitim podacima. Skandali poput Cambridge Analytice i

---

org.baze.pravo.hr/HOL/Page?handle=hein.journals/ijgls31&id=7&collection=usjournals&index= (7. rujna 2024.), str. 187-190.

povreda podataka na platformama poput Facebooka dodatno su naglasili važnost regulacije i provedbe zakona.

U budućnosti, održavanje povjerenja korisnika i zaštita njihovih podataka zahtijevat će više od pravnih intervencija. Potrebna je sinergija između zakonodavnih okvira, tehnoloških rješenja i etičkog poslovanja. Sustav za anonimnu obradu podataka i napredne metode enkripcije mogu doprinijeti povećanju sigurnosti podataka, dok će međunarodni sporazumi morati osigurati veću konzistentnost i usklađenost u različitim pravnim sustavima.

Iako izazovi u prijenosu podataka između EU-a i SAD-a ostaju značajni, oni također pružaju priliku za razvoj globalno koherentnih standarda zaštite privatnosti. U vremenu kada više od polovice svjetske populacije koristi društvene mreže, održavanje sigurnosti i privatnosti podataka nije samo pravna ili tehnička potreba, već je ključno za očuvanje povjerenja, slobode i ljudskog dostojanstva u digitalnom dobu.

LITERATURA

ČLANCI

1. Agencija Europske unije za temeljna prava i Vijeće Europe, *Priručnik o europskom zakonodavstvu i zaštiti podataka. Izdanje iz 2018.*, travanj 2018., dostupno na: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_hr.pdf

2. Bowden, Mr C., *The US surveillance programmes and their impact on EU citizens' fundamental rights*, Europski parlament, dostupno na: https://www.europarl.europa.eu/RegData/etudes/note/join/2013/474405/IPOL-LIBE_NT(2013)474405_EN.pdf (9. listopada 2024.)

3. Bratman, B. E., *BRANDEIS AND WARREN'S THE RIGHT TO PRIVACY AND THE BIRTH OF THE RIGHT TO PRIVACY,* Tennessee Law Review, Vol.69:623, 2002., str. 623-651, dostupno na: https://scholarship.law.pitt.edu/cgi/viewcontent.cgi?article=1062&context=fac_articles (10. listopada 2024.)

4. Britannica, National Security Agency, 9. listopada 2024., dostupno na: https://www.britannica.com/technology/computer-security

5. Connolly, M., *Will the EU-US Data Privacy Framework Survive Schrems III?*, 87-124 , Trinity College Law Review (Vol 27) (2024), dostupno na: https://03020cmp-y-https-heinonline-org.baze.pravo.hr/HOL/Page?collection=usjournals&handle=hein.journals/trinclr27&id=97&men_tab=srchresults (13. listopada 2024.), str. 87-124

6. Data Protection Commissioner protiv Facebook Ireland Ltd, Maximmilliana Schremsa, uz sudjelovanje The United States of America, Electronic Privacy Information Centre, BSA Business Software Alliance Inc., Digitaleurope, C-311/18, 16. srpnja 2020., dostupno na:

https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=hr&mode=lst&dir=&occ=first&part=1&cid=5146442.

7. Dixon, S. J., *Annual revenue and net income generated by Meta Platforms from 2007 to 2023*, Statista, 4. ožujka 2024., dostupno na: https://www.statista.com/statistics/277229/facebooks-annual-revenue-and-net-income/ (12. listopada 2024.)

8. European Commission, *Digital Single Market - Communication on Exchanging and Protecting Personal Data in a Globalised Worls Questions and Answers*, dostupno na: https://ec.europa.eu/commission/presscorner/detail/en/memo_17_15 (15. rujna 2024.)

9. Europska komisija, *O Europskoj komisiji*, dostupno na: https://commission.europa.eu/about_hr (12. siječnja 2025.).

10. Europska komisija, *EU-U.S. Privacy Shield: Frequently Asked Questions*, 12. srpnja 2016., dostupno na: https://ec.europa.eu/commission/presscorner/detail/hr/memo_16_2462

11. Europska komisija, Statement by Commissioner Vera Jourova on the European Parliament consent vote on the conclusion of the EU-U.S data protection "Umbrella Agreement", 1. prosinca 2016., dostupno na: https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_16_4182

12. European Commission, *Codes of conduct and certification mechanisms*, dostupno na: https://ec.europa.eu/programmes/erasmus-plus/project-result-content/2cf83d56-345f-4f36-989b-8bfd8461f023/Module%206%20Codes%20of%20conduct%20and%20certification%20mechanisms.pdf

13. Europski odbor za zaštitu podataka, The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC, 21. siječnja 2019., dostupno na: https://www.edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en, 12. siječnja 2025.

14. Europski odbor za zaštitu podataka, *EU-U.S Privacy Shiels - Third Annual Joint Review*, 12. studenoga 2019., dostupno na: https://www.edpb.europa.eu/sites/default/files/files/file1/edpbprivacyshield3rdannualreport.pdf_en.pdf (7. listopada 2024.)

15. Europski odbor za zaštitu podataka, Statement on the processing of personal data in the context of the COVID-19 outbreak, 19. ožujka 2020., dostupno na: https://www.edpb.europa.eu/sites/default/files/files/news/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf (26. listopada 2024.)

16. Europski odbor za zaštitu podataka, *EU-U.S. Data privacy framework, F.A.Q. For European Business*, 16. srpnja 2024., dostupno na: https://www.edpb.europa.eu/system/files/2024-07/edpb_dpf_faq-for-businesses_en.pdf

17. Europski parlament, *EU-US relations in data protection, AI and security: MEPs conclude visit to US*, 28. veljače 2020., dostupno na: https://www.europarl.europa.eu/news/en/press-room/20200228IPR73609/eu-us-relations-in-data-protection-ai-and-security-meps-conclude-visit-to-us (8. listopada 2024.)

18. Europski parlament, Informativni članci o EU, *Mala i srednja poduzeća*, dostupno na: https://www.europarl.europa.eu/factsheets/hr/sheet/63/mala-i-srednja-poduzeca (11. siječnja 2025.).

19. Hoffman, D. A., *Schrems II and TikTok: Two Sides of the Same Coin,* 14. svibnja 2021., North Carolina Journal od law & technology (Vol 22, Issue 4), 573.-616. dostupno na: https://03020cmp-y-https-heinonline-org.baze.pravo.hr/HOL/Page?public=true&handle=hein.journals/ncjl22&div=23&start_page=573&collection=usjournals&set_as_cursor=2&men_tab=srchresults (27. rujna 2024.)

20. Joshi, D., *Privacy Theory 101: Warren and Brandeeis's 'The Right to Privacy' - Law Affect and the 'Right to be Let Alone',* Centre for Law & Policy Research, 25. rujna 2020., dostupno na: https://clpr.org.in/blog/privacy-theory-101-warren-and-brandeiss-law-affect-and-the-right-to-be-let-alone/ (10. listopada 2024.)

21. Koch, R., *The GDPR meets its first challenge: Facebook,* GDPR.EU, dostupno na: https://gdpr.eu/the-gdpr-meets-its-first-challenge-facebook/?cn-reloaded=1&cn-reloaded=1 (12. listopada 2024.)

22. Korff, D.; Georges, M., *Priručnik za DPO-ove, Smjernice za službenike za zaštitu osobnih podataka u javnom i gotovo isključivo-javnom sektoru o tome kako osigurati usklađenost s Općom*

Uredbom o zaštiti podataka Europske unije, rujan 2018., str.17, dostupno na: https://azop.hr/wp-content/uploads/2020/12/prirucnik-_za_dpo-t4data-hrv.pdf

23. Lu, W., *Data Localization: From China and Beyond,* Indiana Journal of Global Legal Studies, 183-203, vol 31, issue 1 2024), dostupno na: https://03020cmp-y-https-heinonline-org.baze.pravo.hr/HOL/Page?handle=hein.journals/ijgls31&id=7&collection=usjournals&index = 183.-202. str. (7. rujna 2024.)

24. Macaskill, E.; Dance, G., *NSA files: decoded, What the revelations mean for you*, 1. studenoga 2013., dostupno na: https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1 (28. rujna 2024.)

25. Petrosyan, A., *Worldwide digital population 2024*, Statista, 4. listopada 2024., dostupno na: https://www.statista.com/statistics/617136/digital-population-worldwide/ (10. listopada 2024.)

26. RH, Ministarstvo uprave, PRIJEDLOG ZAKONA O PROVEDBI OPĆE UREDBE O ZAŠTITI PODATAKA S KONAČNIM PRIJEDLOGOM ZAKONA, Zagreb, ožujak 2018., dostupno na: https://vlada.gov.hr/UserDocsImages/2016/Sjednice/2018/04%20travnja/90%20sjednica%20VRH/90%20-%201.pdf

27. Službene internetske stranice Europskog vijeća i Vijeća Europske unije, *Zaštita podataka u EU-u*, 3. srpnja 2024., dostupno na: https://www.consilium.europa.eu/hr/policies/data-protection/#rights

28. Whittaker, Z., *Trump-linked data firm Cambridge Analytica harvested data on 50 million Facebook profiles to help target voters*, ZDNET, 17. ožujka 2018., dostupno na: https://www.zdnet.com/article/facebook-suspends-analytics-firm-that-helped-trump-campaign/ (17. rujna 2024.)

KNJIGE

1. Dragičević, D., *Pravna informatika i pravo informacijskih tehnologija,* Narodne novine, Zagreb, listopad 2015.

PROPISI

1. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Dara, European Treaty Series – No. 108

2. Data Protection Act 1998, c.29, srpanj 1998., dostupno na: https://www.legislation.gov.uk/ukpga/1998/29?view=plain

3. Direktiva 95/46/EZ Europskog parlamenta i Vijeća od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom podataka i o slobodnom protoku takvih podataka, SL L 281, 23.11.1995, p. 31–50

4. Direktiva (EU) 2015/1535 Europskog parlamenta i Vijeća od 9. rujna 2015. o utvrđivanju postupka pružanja informacija u području tehničkih propisa i pravila o uslugama informacijskog društva, L241/1, Službeni list Europske unije

5. European Data Protection Board, Guidelines 172018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679, 25. svibnja 2018., dostupno na: https://www.edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_1_2018_certification_en.pdf (1. listopada 2024.)

6. European Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441), OJ L 215, 58/08/2000, p.7-47

7. (Europska) Konvencija za zaštitu ljudskih prava i temeljnih sloboda, MU 18/97, 6/99, 14/02, 13/03, 9/05, 1/06, 2/10, 13/17

8. Europski odbor za zaštitu podataka, Odluka br. 263 o transparentnosti i korištenju podataka korisnika od strane Googlea, 1. srpnja 2021., dostupno na: https://www.edpb.europa.eu/decision-no-263_en, (26. listopada 2024.)

9. Europski odbor za zaštitu podataka, Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDP, 28. srpnja 2024., dostupno na: https://www.edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-12021-dispute-arisen_en (26. listopada 2024.)

10. Europski odbor za zaštitu podataka, Binding Decision 5/2022 on the dispute submitted by the Irish SA regarding WhatsApp Ireland Limited (Art. 65 GDPR), 5. prosinca 2022., dostupno na: https://www.edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-52022-dispute-submitted_en (26. listopada 2024.)

11. Europski odbor za zaštitu podataka, Binding Decision 2/2023 on the dispute submitted by the Irish SA regarding TikTok Technology Limited (Art. 65 GDPR), 2. kolovoza 2023., dostupno na: https://www.edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-22023-dispute-submitted_en (27. listopada 2024.)

12. Europski odbor za zaštitu podataka Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subject, 8. listopada 2019., dostupno na: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf (27. listopada 2024.)

13. Executive Order (E.O.)14086 of October 7, 2022, on Enhancing Safeguards for United States Signals Intelligence Activities

14. FISA Amendments Act of 2008, H.R.6304, dostupno na: https://www.congress.gov/bill/110th-congress/house-bill/6304

15. Konvencija za zaštitu ljudskih prava i temeljnih sloboda te Protokola br. 1, Protokola br. 4, Protokola br. 6 i Protokola br. 7 uz tu Konvenciju, Narodne novine 6/1999

16. Odluka Europske komisije C(2000) 2441, L 215/7, Službeni list Europske unije, 26. srpnja 2000

17. Odluka o objavi Opće deklaracije o ljudskim pravima, Narodne novine 12/2009

18. Povelja Europske unije o temeljnim pravima, 7. lipnja 2016., Službeni list Europske unije, 2016/C, 202/02

19. Protokol kojim se mijenja i dopunjuje Konvencija za zaštitu osoba glede automatizirane obrade osobnih podataka, Strasbourg, 10. listopada 2018., Niz ugovora Vijeća Europe - Br. 223

20. Provedbena odluka komisije (EU) 2023/1795 od 10. srpnja 2023. u skladu s Uredbom (EU) 2016/679 Europskog parlamenta i Vijeća o primjerenoj razini zaštite osobnih podataka u skladu s okvirom EU-a i SAD-a za privatnost podataka (C(2023)4745), L 231/118, Službeni list Europske unije

21. Resolution 217A(III), Universal Declaration of Human Rights, A/RES/217(III)

22. Rezolucija Europskog parlamenta od 5. srpnja 2018. o primjerenosti zaštite u okviru europsko-američkog sustava zaštite privatnosti (2018/2645(RSP))

23. Rezolucija Europskog parlamenta od 11. svibnja 2023. o primjerenosti zaštite koju pruža okvir EU-a i SAD-a za zaštitu podataka 2023/2501(RSP), dostupno na: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0204_HR.html

24. UREDBA (EU) 2016/679 EUROPSKOG PARLAMENTA I VIJEĆA od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka)

25. UREDBA (EU) 2018/1725 EUROPSKOG PARLAMENTA I VIJEĆA od 23. listopada 2018. o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama, tijelima, uredima i agencijama Unije i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Uredbe (EZ) br. 45/2001 i Odluke br. 1247/2002/EZ, Službeni list Europske unije L 295/39

26. USA Freedom Act of 2015, H.R. 2048, dostupno na: https://www.congress.gov/114/bills/hr2048/BILLS-114hr2048eh.pdf

27. Ustav Republike Hrvatske NN 56/90, 135/97, 08/98, 113/00, 124/00, 28/01, 41/01, 55/01, 76/10, 85/10, 05/14

28. Vijeće Europe, USA Harbor Privacy Principles, Issued by the U.S. Department of Commerce, 21. srpnja 2000.

29. Zakon o elektroničkoj trgovini, Narodne novine 173/03, 67/08, 36/09, 130/11, 30/14, 32/19

30. Zakon o informacijskoj sigurnosti, Narodne novine 79/07, 30. srpnja 2007.

31. Zakon o potvrđivanju Konvencije za zaštitu osoba glede automatizirane obrade osobnih podataka i Dodatnog protokola uz Konvenciju za zaštitu osoba glede automatizirane obrade osobnih podataka u vezi nadzornih tijela i međunarodne razmjene podataka, Narodne novine 4/2005, 11. svibnja 2005.

32. Zakon o provedbi Opće uredbe o zaštiti podataka Narodne Novine 42/18, 9. svibnja 2018.

33. Zakon o strancima, Narodne novine 133/2020, 2. prosinca 2020.

34. Zakon o zaštiti osobnih podataka, Narodne novine 103/2003, 18. listopada 2023.

SUDSKE ODLUKE

1. Data Protection Commissioner protiv Facebook Ireland Ltd, Maximmilliana Schremsa, uz sudjelovanje The United States of America, Electronic Privacy Information Centre, BSA Business Software Alliance Inc., Digitaleurope, C-311/18, 16. srpnja 2020., dostupno na: https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=hr&mode=lst&dir=&occ=first&part=1&cid=5146442

2. Maximilian Schrems protiv Data Protection Commissioner, uz sudjelovanje Digital Rights Ireland Ltd, C-362/14, 6. listopada 2015. dostupno na: https://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=HR&mode=lst&dir=&occ=first&part=1&cid=5146896

Izjava o izvornosti

Ja, Tamara Horak, pod punom moralnom, materijalnom i kaznenom odgovornošću, izjavljujem da sam isključiva autorica diplomskog rada te da u radu nisu na nedozvoljeni način (bez pravilnog citiranja) korišteni dijelovi tuđih radova te da se prilikom izrade rada nisam koristila drugim izvorima do onih navedenih u radu.

Tamara Horak, v.r.