

- Neslužbeni prijevod -

“Bolja zaštita pojedinaca u kontekstu međunarodnog protoka podataka: potreba za demokratskim i učinkovitim nadzorom obavještajnih službi”

Zajednička izjava koju su donijeli

Alessandra Pierucci, predsjednika Odbora Konvencije 108

i

Jean-Philippe Walter, Povjerenik za zaštitu podataka

Vijeća Europe

STRASBOURG, 7. rujna 2020.

Godinama nakon otkrića Edwarda Snowdena koja su razotkrila razmjere masovnog nadzora koje provode tijela javne vlasti, digitalizacija naših društava se nastavila ubrzanim tempom, a isti je dodatno ubrzan zbog trenutne zdravstvene krize tijekom koje su mnogi od nas bili prisiljeni učiti, raditi i družiti se na daljinu.

Kako naši životi postaju sve digitalniji, a online usluge isprepletene na međunarodnoj razini, naši osobni podaci prelaze regionalne i nacionalne granice i postaje teško osigurati učinkovitu zaštitu osobnih podataka. Pravo na privatnost i zaštitu podataka su temeljna prava. Ta prava su ključna za učinkovito funkcioniranje demokratskih društava i postaju sve važnija u digitalnom dobu.

Pravo na privatnost opće je priznato člankom 12. Deklaracije o ljudskim pravima i člankom 17. Međunarodnog pakta o građanskim i političkim pravima. Na regionalnoj razini, Vijeće Europe nedavno je proslavilo 70. obljetnicu Europske konvencije o ljudskim pravima, koja u članku 8. predviđa zaštitne mjere o pravu na poštovanje privatnog života. Također, i Europska unija je uključila pravo na privatnost i zaštitu podataka u Povelju o temeljnim pravima.

Ta prava ne smiju biti ugrožena: ona samo mogu biti zakonito ograničena, pod posebnim i strogim uvjetima, kao što je to npr. u slučajevima kad postoji prijetnja za nacionalnu sigurnost ili kao što se događalo u posljednje vrijeme, za naše zdravlje.

Takva ograničenja naših temeljnih prava, prava na privatnost i zaštitu podataka, usko su ograničena te je potrebno poduzeti niz zaštitnih mjera kako bi takva ograničenja bila dopuštena, a istovremeno zaštićena bit temeljnih prava i sloboda.

Sud Europske unije nedavno je podsjetio na presudnu važnost odgovarajućih zaštitnih mjera, provedivih prava na međunarodnoj razini i učinkovita pravna sredstva kad se osobni podaci obrađuju u svrhe javne sigurnosti, obrane i državne sigurnosti. U svojoj presudi „Schrems II”¹ od 16. srpnja 2020. godine, Sud je potvrdio da u slučajevima kad se osobni podaci prenose izvan Europske unije, mora biti osigurana razina zaštite u bitnome ekvivalentna onoj koju u Europskoj uniji jamči Opća uredba o zaštiti podataka, tumačena u svjetlu Povelje o temeljnim pravima.

Sud je zaključio da takva razina zaštite nije osigurana u okviru „Štita privatnosti”², sporazuma o prijenosu osobnih podataka između EU i vlade SAD-a, jer ograničenja odnosna na zaštitu podataka koji se prenose iz EU, kako proizlazi iz nacionalnog zakonodavstva SAD-a vezano za uporabu takvih podataka od strane javnih tijela SAD-a i tijela za provedbu zakona, „ne zadovoljavaju uvjete koji su u bitnome isti uvjetima koje propisuje EU zakonodavstvo, sukladno načelu proporcionalnosti, jer programi nadzora koji se baziraju na tim odredbama nisu ograničeni na prikupljanje i obradu samo nužno potrebnih osobnih podataka”³.

Ova odluka ima implikacije i na druge transfere osim na one između EU-a i SAD-a te nameće pitanja vezana za međunarodne transfere podataka, a ujedno predstavlja još jednu priliku za jačanje općeg okvira za zaštitu podataka i ukazuje na potrebu za globalnim pravnim instrumentima za obavještajne službe.

Globalno pitanje

Nakon presude u slučaju Schrems II, pojavili su se prijedlozi iz utjecajnih krugova za potrebom donošenja odluke o pravno obvezujućem međunarodnom sporazumu o zaštiti privatnosti i osobnih podataka.

Taj instrument postoji: riječ je o Konvenciji 108 +.

¹ Data Protection Commissioner protiv Facebook Ireland Limited i Maximilian Schrems (Predmet C-311/18, “Schrems II”).

²Odluka 2016/1250 o o primjerenosti zaštite u okviru europsko-američkog sustava zaštite privatnosti, poništena 16. srpnja 2020.

³Sud Europskeunije, priopćenje za javnost 91/20 od 16. srpnja 2020.

Konvencija Vijeća Europe o zaštiti pojedinaca u vezi s automatskom obradom osobnih podataka (poznatija kao „Konvencija 108“⁴) jedini je pravno obvezujući multilateralni instrument za zaštitu privatnosti i osobnih podataka, otvoren svakoj zemlji u svijetu.

Konvencija 108 otvorena je za potpisivanje 1981. godine i od tada je utjecala na različite međunarodne, regionalne (npr. EU) i nacionalne zakone o privatnosti. Trenutačno ima 55⁵ država članaka i Odbor koji broji više od 25 promatrača te predstavlja globalni forum s više od 70 zemalja sa šest kontinenata koje rade zajedno na zaštiti podataka.

Konvencija 108 nedavno je modernizirana kako bi se taj značajni instrument prilagodio novoj stvarnosti sve povezanijeg svijeta te kako bi se ojačala učinkovita provedba Konvencije. Protokol⁶ o izmjeni Konvencije 108 otvoren je za potpisivanje 10. listopada 2018. u Strasbourgu te su ga od tada potpisale i ratificirale brojne zemlje⁷.

Stupanjem na snagu Protokola o izmjeni Konvencije 108, ostvarit će se dva ključna cilja: olakšavanje protoka podataka i poštovanje ljudskih prava i temeljnih sloboda, uključujući ljudski integritet i dostojanstvo u digitalnom dobu.

Konvencija 108 + (Konvencija 108 izmijenjena protokolom) treba postati međunarodni standard o privatnosti i zaštiti podataka u digitalnom dobu i predstavlja održivo sredstvo za olakšavanje međunarodnih prijenosa podataka uz jamčenje odgovarajuće razine zaštite za pojedince na globalnoj razini.

Iskorištavanja potencijala predmetne konvencije je na tvorcima politika i vladama diljem svijeta.

Posebni izvjestitelj Ujedinjenih naroda za pravo na privatnost prof. Joseph A. Cannataci već je dvaput preporučio⁸ „svim državama članicama UN-a da pristupe Konvenciji 108 +”.

Osim njezine globalne prirode, još dvije važne značajke Konvencije 108 + posebno su važne u razmatranjima nakon odluke Schrems II i njezinih posljedica na međunarodnoj razini.

⁴ Tekst iz 1981. dostupan na: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108>

⁵ Popis članica dostupan na https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=64GsTZPR

⁶ Protokol o izmjeni Konvencije 108 dostupan na: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf

⁷ 36 zemalja potpisnica i 6 ratifikacija, popis zemalja potpisnica dostupan na: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures>

⁸ Izvješće za 2018. o pravu na privatnost (izvješće A/73/45712) i Godišnje izvješće od 1. ožujka 2019. godine Vijeću UN-a za ljudska prava (izvješće A/HRC/40/63).

Prvo, u kontekstu prijenosa podataka iz EU-a i potrebe za učinkovitim osiguranjem odgovarajuće razine zaštite koja je bitnome ekvivalentna onoj koja je osigurana unutar Unije, važno je podsjetiti da se uvodna izjava 105. Opće uredbe o zaštiti podataka izričito upućuje na Konvenciju u kontekstu režima primjerenosti. Pri odlučivanju o razini zaštite podataka zemlje koja traži odluku o primjerenosti trebalo bi uzeti u obzir pristupanje treće zemlje Konvenciji. Važnost Konvencije u kontekstu procjene primjerenosti izričito je priznata u Općoj uredbi o zaštiti podataka. Ako je zemlja potpisnica Konvencije, to bi također moglo olakšati procjenu od slučaja do slučaja koju trgovačka društva moraju učiniti u kontekstu standardnih ugovornih klauzula⁹ u pogledu bitno jednake razine zaštite koju treba jamčiti.

Drugo, što se tiče specifičnog pitanja obrade osobnih podataka za potrebe nacionalne sigurnosti i obrane, Konvencija 108 + sadrži čvrst sustav provjera i ravnoteža u članku 11. kojim se dopunjuje njezino potpuno horizontalno područje primjene (članak 3. Konvencije 108 +)¹⁰.

Prava utvrđena Konvencijom mogu se ograničiti samo ako je to predviđeno zakonom i ako ograničenje predstavlja nužnu i razmjernu mjeru u demokratskom društvu, na temelju određenih i ograničenih razloga, uključujući nacionalnu sigurnost i obranu.

Članak 11. stavak 3. posebno se odnosi na aktivnosti obrade u svrhu nacionalne sigurnosti i obrane, a zahtjev da takve aktivnosti obrade podliježu neovisnom i učinkovitim preispitivanju i nadzoru, jasno je utvrđen Konvencijom.

Iako Konvencija 108 + pruža čvrst međunarodni pravni okvir za zaštitu osobnih podataka, njome se ne rješavaju u potpunosti i izričito neki od izazova koje u našem digitalnom dobu predstavljaju dosad neviđene mogućnosti nadzora. Već godinama se poziva¹¹ na sveobuhvatan međunarodnopravni instrument za ljudska prava koji regulira rad obavještajnih službi te se više ne može ignorirati potreba za jakim zaštitnim mjerama na međunarodnoj razini koji će dopuniti i precizirati mjere iz Konvencije 108 +.

⁹ Vidi paragraf 134 u Odluci Shrems II

¹⁰ Konvencija se primjenjuje na svaku obradu osobnih podataka u privatnom i javnom sektoru, uključujući sigurnosno-obavještajne službe

¹¹ Deklaracija iz 2013. Odbora ministara o opasnostima za temeljna prava koje proizlaze iz tehnologija za praćenje i drugih tehnologija za <https://www.garanteprivacy.it/documents/10160/2603116/Declaration+of+the+Committee.pdf> ,

- Rezolucija 2045 (2015) o masovnom nadzoru Parlamentarne skupštine Vijeća Europe (PACE) koje poziva na multilateralni „obavještajni kodeks“: <http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTMLen.asp?fileid=21692&lang=en>

- Izvješće iz 2016. Vijeću za ljudska prava UN-a o posebnog izvjestitelja za pravo na privatnost, Joseph A. Cannataci: <https://undocs.org/en/A/HRC/31/64>

- Izvješće iz 2014. Generalnoj skupštini UN-a posebnog izvjestitelja o promociji i zaštiti ljudskih prava i sloboda u kontekstu protuterorizma, Ben Emmerson: <https://daccessods.un.org/TMP/5945256.35242462.htm>

Čvrst temelj za buduća razmišljanja

Europski sud za ljudska prava već više od 60 godina kroz svoju opsežnu sudsku praksu razvija važne zaštitne mjere za zaštitu prava na privatnost, kako je navedeno u članku 8. Europske konvencije o ljudskim pravima, uključujući u nizu ključnih slučajeva koji se odnose na opsežno praćenje komunikacija¹² obavještajnih službi. Članak 13. o pravu na učinkoviti pravni lijek još je jedna ključna zaštita za pojedinca.

Kako bi se utvrdilo jesu li interferencije s pravom na privatni život ili korespondenciju potrebne u demokratskom društvu i uspostavlja li se pravedna ravnoteža između različitih uključenih interesa, Sud ispituje je li miješanje u skladu sa zakonom, postoji li legitiman cilj te je li nužno i razmjerno cilju koji se želi postići. Pritom je razvio precizne zaštitne mjere i uvjete koje obavještajne službe moraju poštovati.

Eksponencijalno povećanje trgovine i razmjene informacija u današnjem digitalnom dobu zahtijeva jamčenje snažnijih mjera za zaštitu osobnih podataka, gdje god da se prenose. Postoji snažna potreba da se na međunarodnoj razini riješi složeno i osjetljivo pitanje demokratskog i učinkovitog nadzora obavještajnih službi.

Odluka Schrems II posebno stavlja fokus na dva zahtjeva: potrebu za pravnim lijekovima (tj. djelotvornim i izvršivim pravima pojedinaca pred neovisnim i nepristranim sudom¹³) te u pogledu opsega određenih programa nadzora, nedostatak ograničenja pristupa osobnim podacima za državna tijela, čime se krši načelo stroge nužnosti i proporcionalnosti ograničenja ljudskih prava¹⁴.

Sud Europske unije zaključio je da „pravo te treće zemlje ne predviđa potrebna ograničenja i zaštitne mjere u pogledu uplitanja koja su odobrena njezinim nacionalnim zakonodavstvom i ne osigurava učinkovitu sudsku zaštitu od takvih uplitanja¹⁵“, kao što je to već učinio u svojoj prvoj odluci „Schrems I¹⁶“ kojom se poništava prethodni sporazum o „Sigurnoj luci“ između EU-a i SAD-a.

¹² Vidi dokument o masovnom nadzoru https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf i sudsku praksu Izvješće o nacionalnoj sigurnosti https://www.echr.coe.int/Documents/Research_report_national_security_ENG.pdf

¹³ Vidi paragrafe 191 et seq. iz Schrems II odluke

¹⁴ Vidi paragrafe 179, 180, 183 do 185 iz Schrems II odluke

¹⁵ Vidi paragraf 168 iz Schrems II odluke

¹⁶ Maximillian Schrems protiv Data Protection Commissioner (Predmet C-362/14, “Schrems I”)

Na razini Ujedinjenih naroda, države članice u Rezoluciji 68/167 o pravu na privatnost u digitalnom dobu¹⁷ naglašavaju „da se nezakonitim ili proizvoljnim nadzorom i/ili presretanjem komunikacija, kao i nezakonitim ili proizvoljnim prikupljanjem osobnih podataka, kao vrlo nametljivim djelima, krše prava na privatnost i slobodu izražavanja te mogu proturječiti načelima demokratskog društva” i pozivaju sve zemlje da „stvore uvjete za sprečavanje takvih kršenja, što uključuje i da osiguraju da relevantno nacionalno zakonodavstvo ispunjava obveze iz međunarodnog prava ljudskih prava”.

Stvaranje takvih uvjeta danas podrazumijeva da se zemlje na međunarodnoj razini moraju dogovoriti o tome u kojoj mjeri nadzor koji provode obavještajne službe može biti odobren, pod kojim uvjetima i u skladu s kojim zaštitnim mjerama, zajedno s neovisnim i učinkovitim nadzorom.¹⁸

Sudskom praksom Europskog suda za ljudska prava utvrđeno je da, kako bi bilo dopušteno, miješanje u prava pojedinaca mora ispunjavati niz uvjeta i posebno se mora temeljiti na pravu (što znači da okolnosti i uvjeti moraju biti definirani pravnim odredbama, a posljedice moraju biti predvidljive za pojedince) te moraju biti razmjerne i nužne u demokratskom društvu. Pojedinci moraju imati koristi od učinkovitih pravnih lijekova:

„s obzirom na rizik da sustav tajnog nadzora za zaštitu nacionalne sigurnosti može potkopati ili čak uništiti demokraciju pod okriljem njezine obrane, Sud mora biti uvjeren da postoje primjerena i učinkovita jamstva protiv zlouporabe (vidjeti Klaß i druge, 1978., § 49-50). Ta procjena ovisi o svim okolnostima predmeta, kao što su priroda, opseg i trajanje mogućih mjera, razlozi potrebni za njihovo naručivanje, tijela nadležna za njihovo odobrenje, provedbu i nadzor te vrsta pravnog lijeka predviđena nacionalnim pravom”¹⁹.

Došlo je vrijeme za primjenu brojnih kriterija koje su razvili sudovi, uključujući Vrhovni sud SAD-a, u pogledu onoga što predstavlja odgovarajuća i učinkovita jamstva, učinkovitu odgovornost i neovisni nadzor obavještajnih službi²⁰ te za pronalaženje konsenzusa o tom ključnom pitanju na globalnoj razini.

¹⁷ Rezolucija je dostupna na: <https://undocs.org/A/RES/68/167>

¹⁸ Vidi rad „Demokratski i učinkovit nadzor nad nacionalnim sigurnosnim službama“ objavljen od strane Povjerenika Vijeća Europe za ljudska prava:

<https://rm.coe.int/democratic-and-effective-oversight-of-national-security-servicesissue/16806daadb>

¹⁹ Big Brother Watch and Others v. the United Kingdom, 13/09/2018, §18

²⁰Vidi istraživanje objavljeno od strane Agencije EU za temeljna prava o „Nadzoru od strane obavještajnih službi: zaštitne mjere i pravna sredstva u EU“, svezak I, svezak II.

Idealno postavljen forum

Statut Vijeća Europe osigurava materijalan i teritorijalan opseg djelovanja koji je potreban za ovaj važan posao.

Statut omogućuje Vijeću Europe da radi na globalnim pitanjima, uz sudjelovanje zemalja iz svih dijelova svijeta (kao što je to slučaj s Konvencijom 108 + ili Budimpeštanskom konvencijom o borbi protiv kibernetičkog kriminala koja trenutno broji 65 članova²¹), te da radi na pitanjima nacionalne sigurnosti i obrane koja su izvan nadležnosti Europske unije²².

Vijeće Europe je već obavilo opsežan rad na borbi protiv terorizma. Udruživanje stručnjaka za nacionalnu sigurnost pod jednim krovom i stručnjaka za zaštitu podataka neće biti teško, kao što je to već učinjeno sa stručnjacima za provedbu zakona i zaštitu podataka u kontekstu rada Odbora za kibernetički kriminal.

Ovo je ključan trenutak za zemlje diljem svijeta za uspostavu puta za sljedećih 70 godina zaštite ljudskih prava. Prepoznajući vitalnu važnost zaštite podataka i značaj prekograničnih prijenosa podataka u današnjem digitalnom okruženju, zemlje bi trebale pristupiti Konvenciji 108 + te također iskoristiti jedinstven potencijal koji nudi Vijeće Europe i priliku koja se pruža za rješavanje pitanja djelovanja obavještajnih službi, a sve pod okriljem svjetski ugledne organizacije za ljudska prava.

Alessandra Pierucci i Jean-Philippe Walter

²¹Popis dostupan na:

https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=LwuEXVvQ

²² Članak 4. stavak 2. Ugovora o Europskoj uniji