16/EN
WP 238

Mišljenje 01/2016 o nacrtu odluke o primjerenosti europsko-američkog sustava zaštite privatnosti

Doneseno 13. travnja 2016.

SAŽETAK

Europska komisija je 29. veljače 2016. objavila Komunikaciju, nacrt odluke o primjerenosti i priložene tekstove koji čine novi okvir za transatlantsku razmjenu osobnih podataka u komercijalne svrhe: europsko-američki sustav zaštite privatnosti (dalje u tekstu: sustav zaštite privatnosti), kojim se nastoje zamijeniti prijašnja američka načela o „sigurnoj luci" koja je poništio Sud Europske unije (dalje u tekstu: CJEU) 6. listopada 2015., u predmetu Schrems.

U skladu s člankom 30. stavkom 1. točkom (c) Direktive 95/46/EZ, Radna skupina prema članku 29. (dalje u tekstu: Radna skupina) procijenila je te dokumente kako bi dala svoje mišljenje o nacrtu odluke o primjerenosti. Radna skupina procijenila je komercijalne aspekte kao i moguća odstupanja od načela sustava zaštite privatnosti za potrebe nacionalne sigurnosti, kaznenog progona i javnih interesa.

Radna skupina uzela je u obzir pravni okvir EU-a koji se primjenjuje na zaštitu podataka određen Direktivom 95/46/EZ i temeljna prava na privatni život i zaštitu podataka utvrđena člankom 8. Europske konvencije o ljudskim pravima i člancima 7. i 8. Povelje Europske unije o temeljnim pravima. Razmotrila je i pravo na djelotvoran pravni lijek i na pošteno suđenje utvrđeno člankom 47. Povelje te sudsku praksu povezanu s različitim temeljnim pravima.

Osim toga, analiza odražava obrazloženje CJEU-a u predmetu Schrems u pogledu Komisijine margine slobodne prosudbe o procjeni primjerenosti. Provjera i kontrole zahtjeva za primjerenost moraju se strogo provoditi, uzimajući u obzir temeljna prava na privatnost i zaštitu podataka te broj osoba na koje bi prijenosi mogli utjecati.

Sustav zaštite privatnosti treba gledati u sadašnjoj međunarodnoj situaciji, kao što je pojava velike količine podataka i sve veće potrebe za sigurnošću. Područje primjene i opseg prikupljanja i upotrebe osobnih podataka znatno su se povećali otkako je 2000. izdana izvorna Odluka o „sigurnoj luci". Europska tijela za zaštitu podataka snažno naglašavaju važnost načela koja brane.

Radna skupina prije svega pozdravlja znatna poboljšanja koja je donio sustav zaštite privatnosti u usporedbi s Odlukom o „sigurnoj luci". Napominje da su pregovarači riješili mnoge nedostatke koji se odnose na „sigurnu luku", a koje je Radna skupina istaknula u svojem dopisu od 10. travnja 2014. potpredsjednici Reding.

Činjenica da su načela i jamstva koja daje sustav zaštite privatnosti utvrđena u odluci o primjerenosti i u njezinim prilozima otežava pronalazak informacija i ponekad ih čini nedosljednima. Time se doprinosi općenitom pomanjkanju jasnoće u pogledu novog okvira, a isto tako otežava dostupnost za osobe čiji se podaci obrađuju, organizacije te tijela za zaštitu podataka. Slično tome, nejasan je i upotrijebljeni izričaj. Stoga Radna skupina poziva Komisiju da to učini jasnim i razumljivim za obje strane Atlantika.

Što se tiče prava koje se primjenjuje, Radna skupina naglašava da, ako se na temelju Direktive 95/46/EZ donese odluka o primjerenosti sustava zaštite privatnosti, ona treba biti usklađena s pravnim okvirom EU-a o zaštiti podataka, u pogledu područja primjene i u

pogledu terminologije. Radna skupina smatra da se mora provesti preispitivanje ubrzo nakon početka primjene Opće uredbe o zaštiti podataka, kako bi se osiguralo da će se viša razina zaštite podataka koju nudi Uredba slijediti u odluci o primjerenosti i njezinim prilozima.

O komercijalnim aspektima sustava zaštite privatnosti

Ključni je cilj Radne skupine osigurati, kada se osobni podaci obrađuju podložno odredbama sustava zaštite privatnosti, da se zadrži u načelu istovjetna razina zaštite koja se daje pojedincima. Iako Radna skupina ne očekuje da će sustav zaštite privatnosti biti puka i konačna preslika pravnog okvira EU-a, ona smatra da bi taj sustav trebao sadržavati bit temeljnih načela i, kao rezultat, osigurati „u načelu istovjetnu" razinu zaštite.

Neovisno o poboljšanjima koje nudi sustav zaštite privatnosti, Radna skupina smatra da neka ključna načela o zaštiti podataka navedena u europskom pravu nisu uključena u nacrt odluke o primjerenosti i priloge, ili da su neprimjereno zamijenjena alternativnim pojmovima.

Na primjer, načelo zadržavanja podataka nije izričito spomenuto i ne može se jasno protumačiti iz sadašnjeg teksta načela o cjelovitosti podataka i ograničenju svrhe. Nadalje, ne postoji tekst o zaštiti koju bi trebalo pružiti protiv automatiziranih pojedinačnih odluka koje se temelje isključivo na automatiziranoj obradi. Primjena načela o ograničenju svrhe na obradu podataka također je nejasna. Kako bi upotreba nekoliko važnih pojmova bila jasnija, Radna skupina predlaže da se EU i SAD usuglase o jasnim definicijama i da one budu dio pojmovnika koji treba uključiti u često postavljana pitanja o sustavu zaštite privatnosti.

S obzirom na to da će se sustav zaštite privatnosti upotrebljavati i za prijenos podataka izvan SAD-a, Radna skupina ustraje u tome da bi u daljnjim prijenosima iz subjekta u sustavu zaštite privatnosti primateljima u trećim zemljama trebalo osigurati jednaku razinu zaštite u svim aspektima sustava zaštite (uključujući nacionalnu sigurnost) i da oni ne bi trebali dovesti do niže zaštite ili zaobići načela zaštite podataka u EU-u. Ako se u okviru sustava zaštite privatnosti predvidi daljnji prijenos u treću zemlju, svaka organizacija u sustavu zaštite privatnosti trebala bi imati obvezu da, prije prijenosa, procijeni sve obvezne zahtjeve nacionalnog zakonodavstva treće zemlje koji se primjenjuju na uvoznika podataka. Općenito, Radna skupina zaključuje da za daljnje prijenose osobnih podataka iz EU-a ne postoji dovoljan okvir, posebice u pogledu njihova područja primjene, ograničenja njihove svrhe i jamstava koja se primjenjuju na prijenose posrednicima.

Naposljetku, iako Radna skupina primjećuje da su pojedincima za ostvarenje njihovih prava stavljeni na raspolaganje dodatni resursi, zabrinuta je da se novi mehanizmi pravne zaštite u praksi mogu pokazati presloženima, teškima za korištenje za pojedince u EU-u i stoga nedjelotvornima. Stoga su potrebna daljnja objašnjenja različitih postupaka pravne zaštite; osobito, kada su na to spremna, tijela EU-a za zaštitu podataka mogla bi se smatrati prirodnom kontaktnom točkom za pojedince iz EU-a u raznim postupcima jer imaju mogućnost djelovati u njihovo ime.

Odstupanja za potrebe nacionalne sigurnosti

Što se tiče pristupa javnih tijela podacima, i u EU-u i u trećim zemljama, Radna skupina podsjeća na svoju analizu relevantnih temeljnih prava iz Radnog dokumenta o opravdanosti miješanja u temeljna prava na privatnost i zaštitu podataka mjerama nadzora pri prijenosu osobnih podataka (europska temeljna jamstva) (WP237).

Velik korak unaprijed od Odluke o „sigurnoj luci" jest to da se nacrt odluke o primjerenosti sada opširno bavi mogućim pristupom podacima obrađenima u okviru sustava zaštite privatnosti za potrebe nacionalne sigurnosti i kaznenog progona. Radna skupina priznaje taj važan korak, kao i povećanu transparentnost koju nudi američka administracija u zakonodavstvu koje se primjenjuje na prikupljanje obavještajnih podataka (Prilog VI.).

Međutim, Radna skupina napominje da izjave Ureda direktora nacionalne obavještajne agencije (ODNI) SAD-a ne isključuju masovno i neselektivno prikupljanje osobnih podataka koji potječu iz EU-a. Radna skupina podsjeća na svoje dugogodišnje stajalište da se u demokratskom društvu masovan i neselektivan nadzor pojedinaca nikada ne može smatrati razmjernim i strogo nužnim, kako se zahtijeva u okviru zaštite koju nude temeljna prava koja se primjenjuju. Osim toga, iznimno je važan sveobuhvatan nadzor svih programa nadzora. Radna skupina prima na znanje da postoji tendencija za prikupljanje sve više i više podataka, masovno i neselektivno, s obzirom na borbu protiv terorizma. Imajući u vidu zabrinutost koju to izaziva u vezi sa zaštitom temeljnih prava na privatnost i zaštitu podataka, Radna skupina sa zanimanjem iščekuje skorašnje presude CJEU-u u slučajevima koji se tiču masovnog i neselektivnog prikupljanja podataka.

U pogledu pravne zaštite, Radna skupina pozdravlja uspostavljanje Pravobranitelja kao novog mehanizma pravne zaštite. To može biti veliko poboljšanje za prava pojedinaca u EU-u s obzirom na obavještajne aktivnosti SAD-a. Međutim, Radna skupina zabrinuta je da ta nova institucija nije dovoljno neovisna, da još nema primjerene ovlasti za djelotvorno obavljanje svoje dužnosti i da ne jamči zadovoljavajuće pravno sredstvo u slučaju neslaganja.

Zajedničko preispitivanje

Mehanizam godišnjeg zajedničkog preispitivanja spomenut u nacrtu odluke o primjerenosti ključan je čimbenik za sveukupnu vjerodostojnost sustava zaštite privatnosti i Radna skupina uvelike pozdravlja mogućnost koju bi to predstavljalo za preispitivanje odluke o primjerenosti. U tom pogledu Radna skupina razumije da će nacionalni predstavnici Radne skupine moći u potpunosti sudjelovati u procesu preispitivanja, ali traži objašnjenje točnih aranžmana. Potrebno je postići dogovor o načinima (uključujući izvješće koje će proizići, njegovu objavu i moguće posljedice te financiranje) puno prije prvog preispitivanja.

Zaključak

Radna skupina primjećuje velika poboljšanja sustava zaštite privatnosti u usporedbi s poništenom Odlukom o „sigurnoj luci". S obzirom na izražena pitanja koja izazivaju zabrinutost i zatražena objašnjenja, Radna skupina poziva Komisiju da riješi ta pitanja koja

izazivaju zabrinutost, utvrdi primjerena rješenja i dostavi zatražena objašnjenja kako bi se poboljšao nacrt odluke o primjerenosti i osiguralo da zaštita koju nudi sustav zaštite privatnosti doista bude u načelu istovjetna onoj u EU-u.

SADRŽAJ

1. UVOD

Nakon presude koju je donio Sud Europske unije (dalje u tekstu: CJEU) 6. listopada 2015. u predmetu Schrems[1], Radna skupina prema članku 29. (dalje u tekstu: Radna skupina) pozvala je države članice Europske unije (dalje u tekstu: EU) i ostale europske institucije da otvore rasprave s tijelima Sjedinjenih Američkih Država (dalje u tekstu: američkim) kako bi se pronašla politička, pravna i tehnička rješenja koja će omogućiti prijenose podataka na američko državno područje i kojima se poštuju temeljna prava.

Nakon više od dvije godine pregovora, 2. veljače 2016. Europska komisija i američko Ministarstvo trgovine postigli su politički dogovor o *Novom okviru za transatlantske razmjene osobnih podataka u komercijalne svrhe: europsko-američkom sustavu zaštite privatnosti* (dalje u tekstu: sustav zaštite privatnosti), kojim se žele zamijeniti prijašnja američka načela o „sigurnoj luci".

Komisija je 29. veljače 2016. objavila Komunikaciju[2], nacrt odluke o primjerenosti i priložene tekstove od kojih će se sastojati sustav zaštite privatnosti. U skladu s člankom 30. stavkom 1. točkom (c) Direktive 95/46/EZ (dalje u tekstu: Direktiva) Radna skupina procijenila je te dokumente kako bi dala svoje trenutačno mišljenje o nacrtu odluke o primjerenosti koji je pripremila Komisija, uključujući temeljne dokumente sustava zaštite privatnosti. Tijekom svoje procjene Radna skupina podijelila je rad na procjenu komercijalnog dijela sustava zaštite privatnosti i na analizu zaštitnih mjera uspostavljenih u odnosu na odstupanja od načela sustava zaštite privatnosti u svrhe nacionalne sigurnosti, kaznenog progona i javnih interesa.

Nakon presude u predmetu Schrems Radna skupina održala je nekoliko sastanaka s delegacijama iz američke administracije, predstavnicima organizacija civilnog društva iz EU-a i iz SAD-a te znanstvenicima, kako bi pripremila procjenu posljedica presude u predmetu Schrems. Tijekom procjene sustava zaštite privatnosti održani su daljnji sastanci s Europskom komisijom i predstavnicima američke administracije. Tijekom tih sastanaka pružena su neka objašnjenja, koja su također uzeta u obzir u ovom mišljenju. Radna skupina naglašava da su, u ovoj fazi, ta objašnjenja samo neformalna i da se ne može smatrati da čine sastavni dio nacrta odluke o primjerenosti jer još nisu u pismenom obliku.

Ipak, Radna skupina posebno pozdravlja opredjeljenje Ministarstva trgovine tijekom tih sastanaka za suradnju s tijelima za zaštitu podataka država članica EU-a u pogledu primjene sustava zaštite privatnosti i osiguravanje uputa i pravnog tumačenja o primjeni sustava zaštite privatnosti koji će biti objavljeni na njihovim internetskim stranicama.

[1] Predmet C-362/14 – Maximilian Schrems protiv povjerenika za zaštitu podataka, 6. listopada 2015. (dalje u tekstu: predmet Schrems).
[2] COM(2016) 117 final, 29. veljače 2016.

1.1. Opće primjedbe

1.1.1. Područje primjene procjene Radne skupine

Radna skupina je prije svega uzela u obzir primjenjivi okvir za zaštitu podataka u državama članicama Europske unije, uključujući članak 8. Europske konvencije o ljudskim pravima (dalje u tekstu: ECHR), kojim se štiti pravo na privatni i obiteljski život, i članke 7., 8. i 47. Povelje Europske unije o temeljnim pravima (dalje u tekstu: Povelja), kojima se štite pravo na privatni i obiteljski život, pravo na zaštitu osobnih podataka i pravo na djelotvoran pravni lijek i pošteno suđenje. Uzela je u obzir i relevantnu sudsku praksu i zahtjeve Direktive.

Uvjet za treće zemlje za osiguravanje odgovarajuće razine zaštite podataka dodatno je definirao CJEU u predmetu Schrems. Sud nije samo objasnio da se odredbe Direktive moraju tumačiti „u svjetlu temeljnih prava zajamčenih Poveljom”[3] , a osobito njezinim člancima 7. i 8. Naveo je također da se tekst „odgovarajuća razina zaštite” mora shvatiti kao „da traži od treće zemlje da djelotvorno osigura, temeljem domaćeg zakonodavstva ili međunarodnih obveza koje je preuzela, razinu zaštite temeljnih prava i sloboda koja je u načelu istovjetna onoj koja je zajamčena unutar Europske unije na temelju Direktive tumačene u svjetlu Povelje.”[4] Za prijašnju Odluku o „sigurnoj luci” takva procjena nikada nije učinjena s dovoljnom razinom pojedinosti. Radna je skupina stoga ocijenila nacrt odluke o primjerenosti u svjetlu zahtjeva da se izradi analiza razine zaštite temeljnih prava i sloboda koja je *u načelu istovjetna* onoj koja je zajamčena u EU-u. Radna skupina naglašava da ovo mišljenje sadržava njezina glavna pitanja koja izazivaju zabrinutost, ali da bi se, s obzirom na ograničeno vrijeme koje je prošlo od objave nacrta odluke o primjerenosti, poslije mogla pojaviti daljnja problematika.

Radna skupina priznaje da je definiranjem riječi „odgovarajuća” u članku 25. stavku 6. Direktive kao „u načelu istovjetna” CJEU dalje razradio primjerenost u predmetu Schrems. Sud je naglasio da se pojam „odgovarajuća razina zaštite” iako ne zahtijeva od treće zemlje da osigura razinu zaštite identičnu onoj koja je zajamčena u pravnom poretku EU-a, mora shvatiti kao zahtjev za treću zemlju da djelotvorno osigura, temeljem domaćeg zakonodavstva ili međunarodnih obveza koje je preuzela, razinu zaštite temeljnih prava i sloboda koja je *u načelu istovjetna* onoj koja je zajamčena unutar Europske unije na temelju Direktive tumačene u svjetlu Povelje.

1.1.2. Procjena komercijalnog dijela nacrta odluke o primjerenosti

Radna je skupina već objasnila način na koji je primijenila osnovna načela zaštite podataka u EU-u na prijenose osobnih podataka u treće zemlje u svojem Radnom dokumentu 12 „Prijenosi osobnih podataka u treće zemlje: primjena članaka 25. i 26. direktive o zaštiti podataka u EU-u”[5]. Radna skupina pokušala je naći istovjetne zaštitne mjere kojima se osigurava razina zaštite istovjetne načelima zajamčenim Direktivom, posebice u pogledu

[3] Schrems, t. 38.
[4] Schrems, t. 73.
[5] Donesen od strane Radne skupine 24. srpnja 1998., vidjeti osobito str. 6.

ograničenja svrhe, kvalitete podataka i razmjernosti, transparentnosti, sigurnosti, prava pristupa, ispravljanja i protivljenja, zadržavanja podataka i ograničenja daljnjih prijenosa. Slična metoda upotrijebljena je u mišljenjima koja je izdala Radna skupina u vrijeme procjene izvorne Odluke o „sigurnoj luci"[6] i u preporukama Radne skupine u njezinu dopisu bivšoj potpredsjednici i povjerenici EU-a za pravosuđe Viviane Reding, objavljenom 10. travnja 2014[7].

1.1.3. Procjena odstupanja za pristup javnih tijela i njihove zaštitne mjere

Procjena odstupanja za pristup javnih tijela osobnim podacima obuhvaćenima sustavom zaštite privatnosti je složena, osobito uzimajući u obzir povećanu svijest tijela za zaštitu podataka i šire javnosti o američkim programima nadzora nakon Snowdenovih otkrića. Radna skupina prepoznaje i pozdravlja napore američke administracije da poveća transparentnost programa nadzora i njihovu spremnost da uključe dodatne zaštitne mjere u sustav zaštite privatnosti. Radna skupina istodobno naglašava da se svako miješanje u temeljna prava na privatni život i zaštitu podataka u demokratskom društvu mora opravdati. CJEU je kritizirao činjenicu da Odluka o „sigurnoj luci" nije sadržavala nikakav zaključak o postojanju, u Sjedinjenim Američkim Državama, pravila koja je država donijela u cilju ograničavanja miješanja. Isto tako ne upućuje na postojanje djelotvorne pravne zaštite protiv miješanja te vrste.[8]

Stoga je Radna skupina analizirala trenutačni američki pravni okvir i praksu američkih obavještajnih službi opisane u prilozima Nacrtu odluke i uvjete pod kojima oni dopuštaju svako miješanje u temeljna prava na poštovanje privatnog života i zaštitu podataka kako su zaštićeni europskim pravnim okvirom.

Kako bi se utvrdilo bi li u demokratskom društvu bilo opravdano ikakvo miješanje, procjena je provedena u svjetlu europske sudske prakse o temeljnim pravima koja postavlja četiri temeljna jamstva[9] za obavještajne aktivnosti:

A. obrada bi trebala biti u skladu sa zakonom i na temelju jasnih, preciznih i pristupačnih pravila: to znači da bi svatko tko je u razumnoj mjeri informiran trebao biti u mogućnosti predvidjeti što bi se moglo dogoditi s njegovim podacima kada se prenesu;
B. treba pokazati potrebu i razmjernost u odnosu na opravdane ciljeve kojima se teži: potrebno je pronaći ravnotežu između cilja za koji se podaci prikupljaju i zbog kojeg im se pristupa te prava pojedinca;
C. trebao bi postojati neovisan nadzorni mehanizam, koji je i djelotvoran i nepristran: to može biti ili sudac ili drugo neovisno tijelo, dok god ima dovoljno sposobnosti da provede potrebne provjere;

[6] Vidjeti WP62, WP32, WP27, WP23, WP21, WP19, WP15 i WP7.
[7] http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140410_wp29_to_ec_on_sh_recommendations.pdf
[8] Schrems, t. 87. i 88.
[9] Europska temeljna jamstva zasnivaju se na sudskoj praksi CJEU-a i ESLJP-a i iznesena su potanje u Radnom dokumentu Radne skupine WP237, objavljenom 13. travnja 2016.

D. pojedincu moraju biti dostupni djelotvorni pravni lijekovi: svatko bi trebao imati pravo na obranu svojih prava pred neovisnim tijelom.

1.2. Nacrt odluke o primjerenosti

Radna skupina prije svega pozdravlja činjenicu da se novi postupak povezan s primjerenošću može pokrenuti manje od šest mjeseci nakon što je CJEU proglasio Odluku o „sigurnoj luci" nevažećom. S obzirom na količinu prijenosa podataka koji se svakodnevno odvijaju između EU-a i SAD-a, a koju Radna skupina prepoznaje kao vitalan dio gospodarstva na obje strane Atlantika, pravna jasnoća potrebna je što prije.

Radna skupina ipak žali što nacrt odluke o primjerenosti koji je Komisija objavila ne uključuje sveobuhvatnu procjenu domaćeg prava i međunarodnih obveza SAD-a u obliku izvješća o primjerenosti, kao što je to bila redovita praksa u prošlosti u sličnim postupcima i u skladu s člankom 25. Direktive. To je spriječilo Radnu skupinu da obavi potpunu analizu pravnog konteksta u kojem će djelovati sustav zaštite privatnosti. Ona, na primjer, primjećuje da sadašnji nacrt odluke o primjerenosti ne uključuje nalaze o propisima o privatnosti i zaštiti podataka koji postoje u SAD-u, i na saveznoj i na državnoj razini, uključujući i sektorsko zakonodavstvo, kao ni o propisima koji omogućavaju oblike javnog pristupa koji nisu povezani s nadzorom. Isto tako nije definiran odnos između prijenosa podataka u okviru sustava zaštite privatnosti i u okviru drugih postojećih nalaza o primjerenosti poput Sporazuma između EU-a i SAD-a o prijenosu i obradi podataka iz evidencije podataka o putnicima (PNR) i Sporazuma o programu za praćenje financiranja terorističkih djelatnosti (TFTP).

1.2.1. Područje primjene okvira za zaštitu podataka u EU-u i, osobito, načela Direktive 95/46/EZ

Radna skupina podsjeća da, u skladu sa zakonskim okvirom o zaštiti podataka u EU-u, a posebice u okviru Direktive (članak 4. stavak 1.), zakoni država članica ne primjenjuju se samo na aktivnosti obrade koje obavljaju voditelji obrade s poslovnim nastanom na njihovu području, nego i kada se voditelji obrade (iako nemaju poslovni nastan u EU-u) služe opremom koja se nalazi na području EU-a, osobito za prikupljanje osobnih podataka. Kao posljedica toga, zakon države članice EU-a primjenjuje se na svaku obradu koja se odvija prije prijenosa u SAD, u kontekstu aktivnosti organizacije s poslovnim nastanom u EU-u ili korištenjem opremom koja se nalazi u EU-u, a kojom se koristi organizacija koja nema poslovni nastan u EU-u. Radna skupina traži da to bude izričito navedeno u nacrtu odluke o primjerenosti.

Trebalo bi biti jasno da će se načela sustava zaštite privatnosti primjenjivati od trenutka kada se dogodi prijenos podataka. Štoviše, Radna skupina podsjeća na to da voditelji obrade podataka s poslovnim nastanom u EU-u koji prenose podatke izvršitelju obrade podataka u SAD-u i dalje podliježu zakonodavstvu EU-a o zaštiti podataka.

1.2.2. Nedostatak jasnoće dokumenata o sustavu zaštite privatnosti

Činjenica da su načela i jamstva koja daje sustav zaštite privatnosti utvrđena u odluci o primjerenosti i u njezinim prilozima otežava pronalazak informacija i ponekad ih čini nedosljednima. To doprinosi općenitom pomanjkanju jasnoće u pogledu novog okvira, a isto tako otežava dostupnost za osobe čiji se podaci obrađuju, organizacije te tijela za zaštitu podataka. Slično tome, nejasan je i upotrijebljeni izričaj. Stoga Radna skupina poziva Komisiju da to učini jasnim i razumljivim za obje strane Atlantika.

Radna skupina predlaže da se uključi poseban prilog koji će pružiti definirane temeljne pojmove koji se primjenjuju u dokumentima sustava zaštite privatnosti. Zajedničko i nedvosmisleno razumijevanje obveza koje nameće odluka o primjerenosti sustava zaštite privatnosti od presudne je važnosti za njegovo djelotvorno funkcioniranje na obje strane Atlantika, pa je Radna skupina zabrinuta da će zbog brojnih unakrsnih upućivanja, neusklađenih formulacija i složenosti okvirnih dokumenata biti poteškoća u vezi s dosljednošću, razumljivošću i jasnoćom provedbe sustava zaštite privatnosti.

Što je još važnije, dokumenti sustava zaštite privatnosti koriste se terminologijom koja nije u skladu s rječnikom koji se uglavnom upotrebljava u EU-u kada je riječ o zaštiti podataka. To nije nužno problem, dokle god je jasno kakva bi bila odgovarajuća terminologija u okviru prava EU-a (i prema američkom pravu). Radna skupina sa žaljenjem napominje da to, međutim, nije slučaj, uključujući i nacrt odluke o primjerenosti. Na primjer, riječ „pristup" upotrebljava se u poglavlju 3. nacrta odluke o primjerenosti u smislu da se podrazumijeva prikupljanje osobnih podataka, umjesto da se dopusti da netko vidi podatke koji su već prikupljeni. Pristup poduzeća podacima i pravo pojedinca na pristup dva su odvojena pojma koje ne treba miješati.

Radna skupina naglašava da se terminologija također treba upotrebljavati dosljedno u svim dokumentima, uključujući i nacrt odluke o primjerenosti. To sada nije slučaj, na primjer za pojmove „obrada" i „osobni podaci". Oba su u načelu dobro definirana u Prilogu II., ali se ne primjenjuju dosljedno u dokumentima, što rezultira nedostacima u zaštiti[10].[11]

[10] Neke klauzule samo nabrajaju neke vrste postupaka u obradi podataka umjesto da se koriste pojmom „obrada". To rezultira nedostacima u zaštiti. Na primjer, u skladu s tekstom odjeljka III. točke 6. podtočke (f) Priloga II., načela sustava zaštite privatnosti primjenjivat će se samo ako organizacija „pohranjuje, upotrebljava ili objavljuje" dobivene podatke (dakle, ne i za druge poslove obuhvaćene pojmom „obrada", kao što su prikupljanje, evidentiranje, izmjena, povlačenje, obavljanje uvida i brisanje). Sigurnost podataka odredit će se samo za „stvaranje, zadržavanje, korištenje ili širenje" osobnih podataka (odjeljak II. točka 4. Priloga II.). Definicija osobnih podataka također je ograničena na „primljene" i „zabilježene" podatke. Kao sljedeći primjer, u načelu obavijesti (odjeljak II. točka 1. podtočka (a) podtočka iv. Priloga II.) navodi se da certificirana organizacija mora obavijestiti pojedince o svrhama za koje „prikuplja i upotrebljava" podatke o njima. U Odjeljku III. točki 9. podtočki (a) podtočki 11. Priloga II. spominju se samo podaci koji se „prenose" ili kojima se „pristupa". Čak i ako se čini da u većini takvih slučajeva namjera nije ograničiti opseg načela ili stvoriti nedostatke u zaštiti, ta neusklađena terminologija za sobom povlači rizik uključivanja takvih nedostataka. Budući da je pojam „obrada" definiran u načelima, iznimno je važno da se on upotrebljava dosljedno kako bi se izbjegle sada postojeće praznine. Inače bi postojalo previše prostora za vjerojatno nenamjerno tumačenje, koje bi u suprotnom moglo dovesti do pogrešnog tumačenja teksta odluke.

[11] Definicija „osobni podaci" uključena u odjeljak I. točku 8. podtočku (a) Priloga II. odnosi se na „podatke o identificiranom pojedincu ili pojedincu čiji se identitet može utvrditi". Međutim, u dodatnom načelu navodi se da se u odnosu na podatke o ljudskim resursima načela primjenjuju samo kod „datoteka koje se mogu pojedinačno identificirati ili se istima pristupa". Radna skupina smatra da to otvara mogućnost obrade osobnih podataka na način koji nije u skladu s načelima zaštite podataka prema pravu EU-a i s općom definicijom osobnih podataka u okviru sustava zaštite privatnosti.

Radna skupina pozdravlja činjenicu da su definicije nekih pojmova koji se upotrebljavaju uključene u dokumente koji čine sustav zaštite privatnosti. Međutim, to nije slučaj za niz drugih bitnih uvjeta, uključujući „posrednika" ili „izvršitelja obrade", „šifrirane podatke", „anonimizirane podatke" i „pojedinca iz EU-a", za koje se po mišljenju Radne skupine traži jasna definicija s kojom se slažu i SAD i EU, kako bi se izbjegla zbrka u kasnijoj fazi za voditelje obrade podataka i za izvršitelje obrade podataka koji se koriste sustavom zaštite privatnosti, nadzorna tijela i širu javnost. Jednostavno rješenje bilo bi dodati pojmovnik u često postavljana pitanja o sustavu zaštite privatnosti.

Radna skupina također upućuje na legitimne razloge za obradu osjetljivih podataka u dodatnom načelu 1. (odjeljak III. točka 1. Priloga II.), u slučajevima kada neka organizacija ne mora dobiti izričit pristanak (uključivanje). Ovo dodatno načelo 1. može se shvatiti kao da navodi pojedinosti o zakonitim razlozima prikupljanja podataka u EU-u jer to je popis sličan članku 8. Direktive. Radna skupina htjela bi podsjetiti da se bilo kakva obrada (uključujući prikupljanje i prijenos) osjetljivih podataka koji podliježu pravu EU-a mora obaviti iz zakonitih razloga u skladu s člankom 8. Direktive. Sustav zaštite privatnosti ne može se tumačiti kao da nudi alternativne razloge za takvu obradu. Na primjer, prema mišljenju Radne skupine nije moguće za organizaciju iz SAD-a da prikuplja podatke podložno pravu EU-a na temelju američkog radnog prava (vidjeti odjeljak III. točku 1. podtočku (a) podtočku v. Priloga II.). Stoga Radna skupina naglašava da svako tumačenje dodatnog načela 1. može dovesti samo do njegove primjene na osjetljive podatke već prenesene nakon što su prikupljeni u EU-u iz zakonitih razloga navedenih u članku 8. Direktive.

Radna skupina naposljetku napominje nedostatak jasnoće u smislu pitanja tko se može smatrati pojedincem iz EU-a te koristiti zaštitom u okviru sustava zaštite privatnosti: svi građani EU-a ili sve osobe s prebivalištem u EU-u. To je osobito bitno u pogledu prava na pravnu zaštitu, uključujući pristup mehanizmu Pravobranitelja. Osim toga, odlukom o primjerenosti trebalo bi se rješavati pitanje u kojoj će se mjeri sustav zaštite privatnosti također primjenjivati na građane/osobe koje borave u zemljama Europskog gospodarskog prostora i Švicarskoj, koji su u prošlosti bili obuhvaćeni programom „sigurne luke".

1.2.3. Zajedničko preispitivanje i suspenzija

Radna skupina pozdravlja činjenicu da su se Europska komisija i američka administracija dogovorili da će redovito preispitivati praktičnu primjenu sustava zaštite privatnosti. To zajedničko preispitivanje godinama je poznata praksa u zajednici za zaštitu podataka u EU-u, a posebno u vezi sa sporazumima o razmjeni PNR podataka s trećim zemljama i Ugovorom TFTP. Radna skupina nadalje pozdravlja činjenicu da u tim zajedničkim preispitivanjima može sudjelovati neutvrđen broj predstavnika tijela za zaštitu podataka.

S obzirom na svoje iskustvo sa zajedničkim preispitivanjima u posljednjih nekoliko godina, Radna skupina htjela bi razjasniti da očekuje da će zajedničko preispitivanje sustava zaštite privatnosti biti opsežnije nego zajednička preispitivanja PNR-a i TFTP-a. Posebice, poželjno je da zajedničko preispitivanje uključuje sastanke s predstavnicima američkih agencija, organizacija i poduzeća i provjere na licu mjesta određenih elemenata sustava zaštite

privatnosti. Predstavnici tijela za zaštitu podataka u zajedničkom preispitivanju trebali bi biti u mogućnosti davati prijedloge za takve provjere na licu mjesta.

Radna skupina smatra da je za zajedničko preispitivanje potrebna zajednička procjena nalaza. Do sada su rezultati zajedničkih preispitivanja predstavljeni u dokumentu zaposlenika Komisije, za što nije bilo potrebno odobrenje članova tima za zajedničko preispitivanje izvan Komisije. Što se tiče zajedničkog preispitivanja sustava zaštite privatnosti, Radna skupina smatra da bi bilo dobro kada bi izvješće o nalazima doista moglo biti zajednički proizvod. Alternativno, može se uzeti u obzir objava posebnog izvješća o zajedničkom preispitivanju tijela za zaštitu podataka.

Naposljetku, što se tiče zajedničkog preispitivanja, Radna skupina podsjeća na obećanje Komisije da će troškove predstavnika Radne skupine tijekom zajedničkih preispitivanja nadoknaditi Komisija. Radna skupina pretpostavlja da će se to također primjenjivati na zajedničko preispitivanje sustava zaštite privatnosti, u svakom slučaju za razuman broj predstavnika tijela za zaštitu podataka.

Radna skupina preporučuje da se Komisija, američka administracija i Radna skupina dogovore o načinima rada za zajednička preispitivanja najkasnije tri mjeseca prije nego što bi se trebalo održati prvo zajedničko preispitivanje sustava zaštite privatnosti i da se načini rada sastave u pismenom obliku.

1.2.4. Pravni okvir EU-a koji se revidira

Odluka o primjerenosti sustava zaštite privatnosti prva je odluka o primjerenosti koja je sastavljena nakon načelnog dogovora o tekstu Opće uredbe o zaštiti podataka. Međutim, Radna skupina ustvrdila je da sustav zaštite privatnosti još ne odražava buduću situaciju. Na primjer, važni novi pojmovi, kao što su pravo na prenosivost podataka i dodatne obveze za voditelje obrade, uključujući i potrebu procjena utjecaja na zaštitu podataka i usklađenost s načelima zaštite osobnih podataka dizajnom i prethodno zadanim postavkama, nisu uključeni u sustav zaštite privatnosti. Radna bi skupina stoga željela predložiti da se sustav zaštite privatnosti, zajedno sa svim postojećim odlukama o primjerenosti preispita ubrzo nakon što se počne primjenjivati Opća uredba o zaštiti podataka. Smatra da bi bilo dobro da se u završnoj verziji odluke o primjerenosti izričito navede taj postupak preispitivanja.

2. PROCJENA KOMERCIJALNOG DIJELA NACRTA ODLUKE O PRIMJERENOSTI

2.1. Opće primjedbe

2.1.1. Poboljšanja

Radna skupina pozdravlja poboljšanja koja donosi sustav zaštite privatnosti i spremnost pregovarača da pokušaju riješiti nedostatke „sigurne luke” koje je istaknula. Posebice, u usporedbi sa „sigurnom lukom”, poboljšanja se mogu primijetiti u sljedećim elementima: umetanju nekih ključnih definicija, kao što su „osobni podaci”, „obrada” i „voditelj obrade”, mehanizmima uspostavljenim kako bi se osigurao nadzor nad Popisom organizacija u sustavu

zaštite privatnosti i sada obveznim vanjskim ili unutarnjim preispitivanjima sukladnosti. Napravljena su i poboljšanja u načelu pristupa i Radna skupina napominje da se sada osiguravaju prava ispravljanja i brisanja kada se podaci upotrebljavaju na način koji nije u skladu s načelima sustava zaštite privatnosti. Osim toga, sada je jasno da svaki pojedinac mora primiti potvrdu da se u vezi s njim obrađuju podaci i da mu se obrađeni podaci moraju priopćiti.

Radna skupina također pozdravlja jačanje pravnih jamstava kada se provode daljnji prijenosi i obveze Ministarstva trgovine SAD-a i Savezne trgovinske komisije (FTC) da provedu obveze utvrđene sustavom zaštite privatnosti.

2.1.2. Primjena sustava zaštite privatnosti na organizacije koje djeluju kao izvršitelji obrade (posrednici)

Nažalost, ostaje nejasno u kojoj su mjeri načela sustava zaštite privatnosti primjenjiva na certificirane organizacije koje primaju osobne podatke iz EU-a samo za potrebe obrade (u daljem tekstu „posrednici" ili „izvršitelji obrade"). Iako se u odredbama iz odjeljka III. točke 10. podtočke (a) Priloga II. spominju prijenosi podataka certificiranim organizacijama za takve svrhe – tj. spominje se zahtjev za sklapanje ugovora – u njima ne postoji nikakvo upućivanje na to kako će se načela sustava zaštite privatnosti primjenjivati na izvršitelje obrade (posrednike). To izaziva nesigurnost kako za certificirane američke organizacije koje primaju podatke za potrebe obrade podataka i za poduzeća iz EU-a koja obavljaju prijenose podataka certificiranim organizacijama koje djeluju kao izvršitelji obrade podataka tako i za osobe čiji se podaci obrađuju. Kao posljedica toga bit će teško utvrditi koje se dužnosti zapravo primjenjuju na organizacije u sustavu zaštite privatnosti koje obrađuju osobne podatke dobivene iz EU-a u njihovoj ulozi izvršitelja obrade. Stoga je svakako potrebno objašnjenje.

Mora se uzeti u obzir da nekoliko obveza uključenih u načela nije prikladno za izvršitelje obrade podataka, jer je uvijek voditelj obrade podataka onaj koji utvrđuje cilj i način obrade podataka (vidjeti definiciju „voditelj obrade" u odjeljku I. točki 8. podtočki (c) Priloga II.). Iz tog razloga neke obveze sadržane u načelima, ako se primijene na organizaciju koja ima ulogu posrednika, mogu biti u suprotnosti s ugovorom o obradi podataka koji je potreban prema pravu EU-a (ugovor spomenut u odjeljku III. točki 10. podtočki (a) Priloga II.). Na primjer, ugovor o obradi podataka općenito neće ovlastiti izvršitelja obrade podataka (posrednika) za daljnji prijenos podataka trećoj strani koja djeluje kao voditelj obrade, čak i u okolnostima navedenima u odjeljku II. točki 3. podtočki (a) Priloga II. Ovlasti za daljnje prijenose trećim stranama koje djeluju kao posrednici trebale bi biti izdane tek nakon prethodnog odobrenja voditelja obrade. Osim toga, u skladu sa zahtjevima prava EU-a, izvršitelj obrade (posrednik) neće moći dati pojedincima potpunu obavijest u skladu s namjerom u načelu obavijesti (odjeljak II. točka 1. Priloga II.), na primjer, jer ta organizacija ne određuje svrhe obrade.

Stoga je iznimno važno razjasniti u načelima da će u slučaju takve kontradikcije biti mjerodavne odredbe ugovora o obradi podataka, a osobito upute organizacije koja prenosi

podatke iz EU-a. Bez takvog objašnjenja načela bi se mogla tumačiti i primjenjivati na način koji nudi previše kontrolnih ovlasti posredniku u sustavu zaštite privatnosti, a to bi izvoznika podataka u EU-u dovelo u opasnost od kršenja njegovih obveza kao voditelja obrade podataka na temelju zakonodavstva EU-a o zaštiti podataka kojem podliježe pri prijenosu podataka organizaciji u sustavu zaštite privatnosti koja djeluje kao posrednik. Osim toga, taj nedostatak jasnoće daje dojam da se izvršitelj obrade može ponovo koristiti podacima kako želi.

Nadalje, trebalo bi osigurati posebna pravila za slučaj kada organizacija djeluje kao izvršitelj obrade podataka (posrednik) kako bi se osiguralo da ta organizacija poštuje upute voditelja obrade podataka. Treba jasno dati na znanje da američke organizacije koje primaju podatke samo za potrebe obrade ne mogu odlučiti obraditi podatke u vlastito ime. U nedostatku posebnih pravila koja se primjenjuju na organizacije koje djeluju kao izvršitelji obrade, teško je odrediti prema kojim bi se pravilima izvršitelji obrade (posrednici) mogli samocertificirati.

2.1.3. Ograničenja dužnosti pridržavanja načela

U odjeljku I. točki 5. Priloga II. navode se, među ostalim, izuzeća od načela kada se podaci obuhvaćeni sustavom zaštite privatnosti upotrebljavaju zbog nacionalne sigurnosti[12], javnog interesa i kaznenog progona ili kada slijede zakon, državnu regulativu ili sudsku praksu koja stvara međusobno sukobljene obveze ili eksplicitne ovlasti. Bez potpunog znanja o američkom pravu na saveznoj razini i na razini pojedinih država, teško je za Radnu skupinu procijeniti područje primjene ovog izuzeća i razmotriti jesu li ta ograničenja opravdana u demokratskom društvu. Bilo bi iznimno važno da Europska komisija u svoj nacrt odluke o primjerenosti također uključi analizu razine zaštite gdje bi se ta izuzeća primjenjivala. Radna skupina poziva Komisiju da osigura da se EU obavijesti o bilo kojem zakonu ili državnoj regulativi koja bi utjecala na pridržavanje načela, koja se primjenjuju trenutačno ili u vrijeme kada novi zakoni ili propisi u SAD-u stupe na snagu.

2.1.4. Nedostatak načela ograničenja zadržavanja podataka

Načelo ograničenja zadržavanja podataka (članak 6. stavak 1. točka (e) Direktive) temeljno je načelo u zakonodavstvu EU-a o zaštiti podataka kojim se određuje da se osobni podaci moraju čuvati samo dok je to potrebno da se ostvari svrha za koju su podaci prikupljani ili za koju se oni dalje obrađuju.

Međutim, Radna skupina u dokumentima koji čine sustav zaštite privatnosti ne može pronaći nikakvo upućivanje na potrebu da voditelji obrade podataka osiguraju brisanje podataka kada više ne bude svrhe za koju su prikupljeni ili dalje obrađeni. Dakle, kako se čini, načela certificiranim organizacijama ne nameću ograničenje za razdoblje zadržavanja podataka usporedivo s onim što se nameće načelom ograničenja zadržavanja podataka u okviru prava EU-a.

Tekst načela o cjelovitosti podataka i ograničenju svrhe (odjeljak II. točka 5. Priloga II.) ne može se ni na koji način smatrati stvaranjem obveze za organizaciju koja djeluje kao voditelj

[12] U poglavlju 3. nalazi se više primjedaba o upotrebi osobnih podataka obuhvaćenih sustavom zaštite privatnosti za potrebe nacionalne sigurnosti, a u poglavlju 4. za potrebe kaznenog progona.

obrade za brisanje podataka nakon što oni više nisu potrebni za svrhe za koje su podaci bili prikupljeni ili se dalje obrađuju ili za organizaciju koja djeluje kao izvršitelj obrade za brisanje podataka nakon prestanka ugovora o usluzi.

Radna skupina naglašava da nedostatak odredaba koje nameću ograničenje na zadržavanje podataka u okviru sustava zaštite privatnosti organizacijama daje mogućnost da zadržavaju podatke koliko god žele, čak i nakon napuštanja sustava zaštite privatnosti, što nije u skladu s temeljnim načelom ograničenja zadržavanja podataka.

2.1.5. Nedostatak jamstava za automatizirane odluke koje stvaraju pravne učinke ili znatno utječu na pojedinca

Sustav zaštite privatnosti ne daje nikakva pravna jamstva kada pojedinci podliježu odluci koja proizvodi pravne učinke ili znatno utječe na njih, a koja se temelji isključivo na automatskoj obradi podataka namijenjenih procjeni određenih osobnih aspekata koji se odnose na njih, kao što je njihova uspješnost na radu, kreditna sposobnost, pouzdanost, ponašanje itd.

Radna skupina već je u svojem Radnom dokumentu 12 naglasila potrebu da se osiguraju pravna jamstva za automatizirane odluke (koje proizvode pravne učinke ili znatno utječu na pojedinca) kako bi se osigurala odgovarajuća razina zaštite.

Ta potreba postaje još važnija jer nove tehnologije koje se stalno razvijaju omogućavaju većem broju poduzeća da razmotre primjenu automatskih sustava odlučivanja, što može dovesti do slabljenja položaja pojedinaca koji ostaju bez ikakvog pravnog lijeka protiv tih odluka koje su donesene pomoću računala. Kada odluke koje donesu isključivo ti automatizirani sustavi imaju učinak na pravnu situaciju pojedinaca ili znatno utječu na njih (na primjer, njihova stavljanja na „crnu listu” i time lišavanje osoba njihovih prava), ključno je osigurati dovoljne zaštitne mjere, uključujući pravo poznavanja logike koja je u to uključena, i zatražiti preispitivanje na neautomatiziranoj osnovi.

2.1.6. Prijelazno razdoblje za postojeće trgovinske odnose

Sustavom zaštite privatnosti predviđa se primjena načela odmah nakon certificiranja. Međutim, organizacije koje će se certificirati u prva dva mjeseca nakon stvarnog datuma stupanja na snagu okvira sustava zaštite privatnosti morat će uskladiti sve postojeće trgovinske odnose s trećim osobama s odgovornosti za daljnji prijenos načela u najkraćem mogućem roku. U svakom slučaju to bi trebale učiniti najkasnije u roku od devet mjeseci od datuma na koji se certificiraju za sustav zaštite privatnosti.

To znači da se postojeći ugovori u potrebnoj mjeri trebaju uskladiti s načelima između dva i devet mjeseci nakon certificiranja. Tijekom tog prijelaznog razdoblja dovoljni su obavješćivanje i izbor. Radna skupina ustraje na tome da se prijenosi mogu odvijati na temelju sustava zaštite privatnosti samo od trenutka kada dotična organizacija može u potpunosti poštovati sve zahtjeve sustava zaštite privatnosti. Mogućnost slanja podataka tijekom prijelaznog razdoblja, a da primatelj nije u mogućnosti u potpunosti poštovati načela

sustava zaštite privatnosti, ne može se smatrati ispunjavanjem uvjeta za pravni prijenos te stoga nije prihvatljiva.

2.2. Posebne primjedbe

2.2.1. Transparentnost

a) Opće napomene o obavješćivanju

Radna skupina pozdravlja više sveobuhvatne i detaljne zahtjeve navedene pod načelom obavješćivanja, a osobito da će obavješćivanje morati uključiti poveznicu na Popis organizacija u sustavu zaštite privatnosti ili njegovu internetsku adresu i upućivati na pravo pojedinaca na pristup i na mehanizme alternativnog rješavanja sporova[13]. Međutim, Radna skupina napominje da treba biti jasniji u vezi s drugim obuhvaćenim pravima (da se ispravlja, briše gdje postoje netočnosti ili ako su obrađeni u suprotnosti s načelima).

Dokumenti koji čine sustav zaštite privatnosti izazivaju zabrinutost u pogledu vremena kada organizacije sustava zaštite privatnosti trebaju pojedincu dostaviti obavijest. U odjeljku II. točki 1. podtočki (b) Priloga II. navodi se da „se obavijest mora dostaviti (...) kada se od osoba prvi put zatraži da daju osobne podatke organizaciji ili čim prije nakon toga, ali u svakom slučaju prije nego što organizacija upotrijebi takve informacije u neku drugu svrhu osim one za koju ih je prvotno prikupila ili obradila organizacija koja je izvršila prijenos ili prije nego što ih po prvi put otkrije trećoj osobi." Radna skupina smatra da u mnogim situacijama američka organizacija u sustavu zaštite privatnosti neće izravno prikupljati podatke od osobe čiji se podaci obrađuju pa bi vrijeme obavješćivanja trebalo biti u trenutku kada organizacija u sustavu zaštite privatnosti evidentira podatke.

Radna skupina napominje da se stvarna provedba zahtjeva s obzirom na načelo obavješćivanja i politiku zaštite privatnosti treba ocijeniti pri prvom godišnjem preispitivanju sustava zaštite privatnosti.

b) Javna dostupnost politike zaštite privatnosti

Radna skupina pozdravlja činjenicu da je sada eksplicitno da će Ministarstvo trgovine provjeriti jesu li poduzeća koja imaju javne internetske stranice objavila svoje politike zaštite privatnosti na tim internetskim stranicama ili, ako nemaju javne internetske stranice, gdje su politike zaštite privatnosti dostupne javnosti[14].

c) Objavljivanje zahtjeva privatnosti ugovora s izvršiteljima obrade

Sustav zaštite privatnosti predviđa, među uvjetima pod kojima organizacija u sustavu privatnosti može prenositi podatke izvršitelju obrade (posredniku), obvezu za

[13] Odjeljak II. točka 1. Priloga II.; Radna skupina upućuje i na drugu preporuku Komisije donesenu u Komunikaciji COM(2103) 847, kao i na dopis Radne skupine potpredsjednici Reding od 10. travnja 2014., osobito točku 4. u dijelu „Transparentnost".

[14] Vidjeti prvu preporuku Europske komisije u njezinoj Komunikaciji COM(2013) 847 i dopis Radne skupine potpredsjednici Reding, 10. travnja 2014., osobito točku 3. u dijelu „Transparentnost".

samocertificirane organizacije da „na zahtjev daju Ministarstvu sažetak ili reprezentativni primjerak odgovarajućih odredaba o privatnosti svog ugovora s posrednikom" (vidjeti odjeljak II. točku 3. podtočku (b) podtočku v. Priloga II.). Radna skupina pozdravlja ovaj zahtjev za transparentnost prema Ministarstvu trgovine.

2.2.2. Izbor

Sustav zaštite privatnosti daje pravo na izuzeće od objavljivanja osobnih informacija trećoj osobi ili od korištenja osobnim podacima u znatno drukčiju svrhu[15] (odjeljak III. točka 2. Priloga II.). Osim toga, pojedinci imaju koristi od prava „izuzeća" od korištenja osobnim informacijama u svrhu izravnog marketinga u bilo kojem trenutku (odjeljak III. točka 12. podtočka (a) Priloga II.)[16].

Osim za situaciju svrhe izravnog marketinga, ne navode se nikakvi detalji o načinu i trenutku kada se to izuzeće može ostvarivati. Radna skupina smatra da jednostavno upućivanje na postojanje ovog prava u politici zaštite privatnosti ne može biti dovoljno, ali treba ponuditi *individualiziranu* priliku da se ostvari to pravo *prije* otkrivanja ili ponovne upotrebe osobnih informacija.

Štoviše, Radna skupina naglašava da u sustavu zaštite privatnosti treba ponuditi opće pravo na prigovor (iz uvjerljivih razloga koji se odnose na određenu situaciju osobe čiji se podaci obrađuju), pri čemu se to podrazumijeva kao pravo na traženje da se prekine obrada podataka dotične osobe kad god pojedinac ima uvjerljive zakonite razloge koji se odnose na njegovu određenu situaciju[17]. Radna skupina preporučuje da se u nacrtu odluke o primjerenosti svakako jasno istakne da pravo na prigovor treba postojati u svakom trenutku i da taj prigovor ne bude ograničen na upotrebu podataka za izravni marketing[18].

Radna skupina strahuje da će nedostatak definicije onoga što se treba smatrati „znatno drukčijom" svrhom dovesti do zbrke i pravne nesigurnosti. Treba objasniti da se u svakom slučaju načelo izbora ne može upotrijebiti za izbjegavanje načela ograničenje svrhe[19]. Izbor bi trebao biti primjenjiv samo kada je svrha znatno drukčija, ali još uvijek sukladna, jer obrada za nespojivu svrhu je zabranjena (odjeljak II. točka 5. podtočka (a) Priloga II.). Mora se razjasniti da pravo na izuzeće ne može omogućiti organizaciji da se koristi podacima za nespojive svrhe. Dakle, Radna skupina preporučuje usklađivanje dotičnog teksta jedinstvenim i definiranim tekstom (na primjer, „znatno drukčije, ali ipak sukladne namjene").

Bilo bi korisno objašnjenje o tome gdje u okviru prava EU-a spada donesena odluka da se podaci obrađuju u neku drugu svrhu ili da se informacije objave. U ovoj situaciji izravno će se primjenjivati uobičajeni pravni zahtjevi EU-a u vezi s ovom obradom (kao što je zabrana

[15] Dodatno načelo 14.c.I. osigurava pravo na povlačenje iz kliničkog ispitivanja, što bi se moglo smatrati pravom na prigovor ili na povlačenje suglasnosti.
[16] To je identično onome što je navedeno u shemi „sigurne luke" (često postavljano pitanje 12.) i u tom smislu nije provedena nikakva promjena.

[18] Vidjeti dopis Radne skupine potpredsjednici Reding, u dijelu „Izbor".
[19] Konkretan primjer daljnje nespojive obrade odobrene u okviru načela izbora navodi se u okviru dodatnog načela 9.b.i. (vidjeti primjedbu Radne skupine o tome u točki koja se odnosi na „podatke o ljudskim resursima".

obrade za nespojive svrhe, kako bi se osigurao zakonit razlog za obradu i potreba informiranja pojedinca), uključujući i američke organizacije koje potpadaju u područje primjene prava EU-a. U praksi to znači da će izvoznik iz EU-a koji donosi takvu odluku morati osigurati transparentnost i zakonitost obrade u skladu s pravom EU-a. Stoga, načelo izbora primjenjivat će se samo ako je odluku donijela isključivo organizacija u sustavu zaštite privatnosti koja ne podliježe pravu EU-a.

2.2.3. Daljnji prijenosi

a) Područje primjene

Radna skupina zabrinuta je zbog situacije kada se daljnji prijenosi osobnih podataka odvijaju iz certificiranih organizacija u sustavu zaštite privatnosti u SAD-u do primatelja u trećoj zemlji.

Sustav zaštite privatnosti ne treba se smatrati samo sredstvom za prijenos podataka iz EU-a u SAD, nego će također poslužiti kao alat koji će se upotrebljavati za prijenos podataka iz SAD-a u treće zemlje. Stoga su odredbe o daljnjem prijenosu važan element sustava zaštite privatnosti koji bi trebao osigurati dostatna jamstva i primjerenu razinu zaštite kada se podaci dalje prenose izvan SAD-a. Jedno određeno pitanje povezano je s nacionalnom sigurnošću i kaznenim progonom.

Načelo odgovornosti za daljnji prijenos sustava zaštite privatnosti nije ograničeno na voditelje obrade podataka, izvršitelje obrade podataka ni posrednike s poslovnim nastanom u SAD-u koji primaju podatke. Stoga se daljnji prijenosi u treću zemlju mogu odvijati na temelju sustava zaštite privatnosti, čak i ako treća zemlja ima zakone kojima se predviđa javni pristup osobnim podacima, na primjer za potrebe nadzora. To podatke iz EU-a dovodi u rizik od neopravdanih miješanja u zaštitu temeljnih prava.

U svakom slučaju daljnjeg prijenosa u treću zemlju, svaka organizacija u sustavu zaštite privatnosti trebala bi imati obvezu da, prije prijenosa, procijeni obvezne zahtjeve nacionalnog zakonodavstva treće zemlje koje se primjenjuje na uvoznika podataka. Ako se utvrdi opasnost od znatnog negativnog učinka na jamstva, obveze i razinu zaštite koju pruža sustav zaštite privatnosti, američka organizacija u sustavu zaštite privatnosti koja djeluje kao izvršitelj obrade (posrednik) odmah obavješćuje voditelja obrade podataka u EU-u prije obavljanja bilo kojeg daljnjeg prijenosa. U tim slučajevima izvoznik podataka ima pravo suspendirati prijenos podataka i/ili raskinuti ugovor. Kada postoji takav rizik od znatnog negativnog učinka, organizaciji u sustavu zaštite privatnosti koja djeluje kao voditelj obrade ne bi trebalo biti dopušteno da obavlja daljnji prijenos podataka jer će to ugroziti njezinu obvezu da osigura jednaku razinu zaštite kao što je ona prema načelima (vidjeti odjeljak II. točku 3. podtočku (a) Priloga II.).

Slično tome, u slučaju promjene u zakonodavstvu treće zemlje za koju je vjerojatno da će imati znatni negativni učinak na jamstva, obveze i razinu zaštite koju pruža sustav zaštite privatnosti, američka organizacija u sustavu zaštite privatnosti koja djeluje kao izvršitelj

obrade (posrednik) trebala bi imati obvezu – prema sustavu zaštite privatnosti – o toj promjeni obavijestiti izvoznika podataka čim za nju sazna, a u tom slučaju izvoznik podataka ima pravo suspendirati prijenos podataka i/ili raskinuti ugovor. Prema tome, u takvom slučaju, organizaciji u sustavu zaštite privatnosti koja djeluje kao voditelj obrade ne bi trebalo biti dopušteno da obavlja daljnji prijenos jer ima obvezu pružiti jednaku razinu zaštite kao što je ona prema načelima (vidjeti odjeljak II. točku 3. podtočku (a) Priloga II.).

Radna skupina podsjeća na svoje stajalište da, ako voditelj obrade podataka u EU-u zna za neki daljnji prijenos trećoj strani izvan SAD-a čak i prije nego što se prijenos u SAD dogodi ili ako je voditelj obrade podataka u EU-u zajednički odgovoran za odluku da se omogući daljnji prijenos, prijenos treba smatrati izravnim prijenosom iz EU-a u treću zemlju izvan SAD-a. To znači da se na prijenos primjenjuju članci 25. i 26. Direktive umjesto načela daljnjeg prijenosa u sustavu zaštite privatnosti.

b) Prijenosi iz organizacije u sustavu zaštite privatnosti trećoj strani koja djeluje kao voditelj obrade

Radna skupina pozdravlja obvezu da se sklope ugovori (odjeljak II. točka 3. podtočka (a) Priloga II.) kako bi se osiguralo da će treća strana koja djeluje kao voditelj obrade pružiti najmanje jednaku razinu zaštite privatnosti kao što se zahtijeva prema načelima sustava zaštite privatnosti. Svrha je osigurati da osobni podaci i dalje budu primjereno zaštićeni, čak i nakon što se prenesu dalje. Međutim, Radna skupina ima neke primjedbe na predložene uvjete.

<u>Nedostatak upućivanja na načelo o ograničenju svrhe</u>

Radna skupina također preporučuje umetanje jasnog upućivanja na načelo o ograničenju svrhe (odjeljak II. točka 5. Priloga II.) u okviru uvjeta za daljnji prijenos trećoj strani koja djeluje kao voditelj (odjeljak II. točka 3. podtočka (a) Priloga II.). Time bi se jasno dalo na znanje da se daljnji prijenosi ne smiju odvijati kada treća strana koja djeluje kao voditelj obrade bude obrađivala podatke za nespojivu svrhu.

<u>Izuzeće od potrebe za ugovorom za prijenose unutar skupine između voditelja obrade</u>

Izuzeće od potrebe za ugovorom predviđeno je za prijenose unutar skupine između voditelja obrade. U takvom scenariju u načelima se navodi da bi se kontinuitet zaštite mogao osigurati obvezujućim korporativnim pravilima (BCR-ovi) ili „drugim instrumentima unutar skupine (npr. programima usklađenosti i kontrole)" (odjeljak III. točka 10. podtočka (b) Priloga II.). Radna skupina smatra da upućivanje na „druge instrumente unutar skupine" ne jamči pravno obvezujuće obveze koje su preuzeli drugi članovi skupine. Budući da Radna skupina i zakonodavstvo EU-a[20] uglavnom preferiraju da se prijenosi unutar skupine uređuju obvezujućim obvezama, važno je izbjeći upotrebu sustava zaštite privatnosti na način kojim se taj zahtjev zaobilazi. Radna skupina podsjeća da, u svakom slučaju, daljnji prijenosi iz

[20] U Općoj uredbi o zaštiti podataka također je naglašena i potreba za obvezujućim i provedivim obvezama bez obzira na alat koji se upotrebljava (BCR-ovi, ugovorne klauzule, kodeksi ponašanja ili certifikati).

SAD-a prema trećim zemljama, planirani čak i prije nego što se obavi prijenos u SAD, ili koji podliježu aranžmanu sa zajedničkim voditeljima obrade s voditeljem obrade iz EU-a[21], moraju se smatrati izravnim prijenosom iz EU-a u treću zemlju izvan SAD-a. Stoga su na prijenos primjenjivi članci 25. i 26. Direktive.

c) Prijenosi iz organizacije u sustavu zaštite privatnosti izvršitelju obrade trećoj osobi (posredniku)

Radna skupina pozdravlja činjenicu da je ugovor za daljnje prijenose sada obvezan za subjekte koji primaju podatke i imaju ulogu izvršitelja obrade (posrednika), bez obzira na njihovo sudjelovanje u sustavu zaštite privatnosti ili na to imaju li koristi od drugog rješenja traženja primjerenosti. Radna skupina također pozdravlja dodatne zaštitne mjere koje se odnose na te daljnje prijenose (odjeljak II. točka 3. podtočka (a). podtočka i. Priloga II.; odjeljak II. točka 3. podtočka (a) podtočka iii.; odjeljak II. točka 3. podtočka (a) podtočka iv.; odjeljak II. točka 3. podtočka (a) podtočka v.; odjeljak II. točka 7. podtočka (d)). Posljednja točka (odjeljak II. točka 7. podtočka (d) Priloga II.) odnosi se na obvezu zadržavanja odgovornosti kada se podaci otkriju nekom posredniku. Međutim, čini se da se ovo jamstvo ne primjenjuje ako je organizacija izabrala da će surađivati s tijelom za zaštitu podataka (vidjeti odjeljak III. točku 5. podtočku (a) Priloga II. sitnim tiskom). Radna skupina ne razumije razlog za takvo izuzeće te smatra da bi se odgovornost trebala primjenjivati čak i u tom slučaju.

Nedostatak upućivanja na načelo o ograničenju svrhe

Radna skupina napominje da se načelom odgovornosti za daljnji prijenos (odjeljak II. točka 3. Priloga II.) objašnjava da se osobni podaci mogu prenijeti na treću osobu koja ima ulogu posrednika samo u ograničene i određene svrhe, ali se ne kaže izričito da te ograničene i određene svrhe moraju biti u skladu s izvornim svrhama za koje su podaci prikupljeni i s uputama voditelja obrade. Ova bi točka trebala biti jasnija. Radna skupina stoga predlaže da se osigura da odluka o primjerenosti pruža više pojedinosti, na primjer umetanjem jasnog upućivanja u načelo o ograničenju svrhe (odjeljak II. točka 5. Priloga II.), prema kojem se podaci ne smiju obrađivati (uključujući objavljene podatke) za nespojive svrhe unutar načela o daljnjem prijenosu (osim načela o izuzeću).

Potreba za više dodatnih obveza za organizacije u sustavu zaštite privatnosti koje djeluju kao izvršitelj obrade (posrednik) pri daljnjem prijenosu podataka drugom izvršitelju obrade (posredniku)

Nepostojanje jasnih pravila kada organizacija u sustavu zaštite privatnosti djeluje kao posrednik (tj. u ime voditelja obrade u EU-u) podrazumijeva da postoji praznina i to može spriječiti voditelja obrade u EU-u da kontrolira situaciju. Organizacija u sustavu zaštite privatnosti koja prima podatke kao posrednik voditelja obrade iz EU-a mora poštovati upute voditelja obrade iz EU-a. To bi trebalo biti izričito navedeno u načelima kako bi se osiguralo

[21] Na primjer, za podatke o ljudskim resursima.

da će nepoštovanje tih uputa dovesti ne samo do kršenja ugovora (odjeljak III. točka 10. podtočka (a) podtočka ii. Priloga II.) nego i do kršenja načela sustava zaštite privatnosti.

Mogućnost da organizacija u sustavu zaštite privatnosti koja djeluje kao posrednik naknadno prenese podatke trećoj strani koja ima ulogu posrednika mora biti transparentna za voditelja obrade i biti predmet njegova prethodnog odobrenja. Stoga bi trebalo biti jasno navedeno da se upravo ugovorom koji posrednik potpiše s voditeljem obrade iz EU-a (na njega se upućuje u često postavljanim pitanjima br. 10. kao na „ugovor iz članka 17. ") određuje je li daljnji prijenos dopušten[22].

Sadašnji uvjeti primjenjivi na daljnji prijenos posredniku temelje se na pretpostavci da organizacija u sustavu zaštite privatnosti djeluje kao voditelj obrade i stoga može sama odlučiti o mogućoj intervenciji treće strane koja ima ulogu posrednika. Međutim, to ne bi trebalo biti moguće kada organizacija u sustavu zaštite privatnosti djeluje kao posrednik. U suprotnom slučaju voditelj obrade u EU-u bit će lišen svojih kontrolnih ovlasti.

Mjerodavne odredbe o privatnosti ugovora sklopljenog s trećom stranom koja ima ulogu posrednika moraju biti dostupne voditelju obrade i moraju osigurati najmanje jednaku razinu zaštite kao što je navedeno u ugovoru potpisanom s voditeljem obrade.

2.2.4. Načelo o cjelovitosti podataka i ograničenju svrhe

a) Razmjernost

Još bi trebalo napomenuti da Radna skupina upućuje na svoj dopis potpredsjednici Reding u kojem je napisano da je moguće da „obrada osobnih podataka, čak i uza strogo poštovanje načela obavješćivanja i izbora, ne bude razmjerna u odnosu na interese, prava i slobode osobe čiji se podaci obrađuju ili društva. Načelo razmjernosti ili razboritosti mora se poštovati u svim fazama obrade i treba se primjenjivati uz načela obavješćivanja i izbora[23]."

U sustavu zaštite privatnosti (odjeljak II. točka 5. podtočka (a) Priloga II.) navodi se da informacije moraju biti ograničene na ono što je bitno za obradu. Radna bi skupina radije htjela da se ovaj tekst promijeni u završnoj verziji odluke o primjerenosti jer sama činjenica da će podaci biti bitni za obradu nije dovoljna da obrada bude razmjerna. Kako bi se zadovoljilo načelo proporcionalnosti, obrada bi trebala biti ograničena na podatke koji su potrebni za dotičnu obradu.

b) Točnost

U načelu o cjelovitosti podataka i ograničenju svrhe (odjeljak II. točka 5. Priloga II.) također se navodi: „U mjeri u kojoj je to potrebno za tu namjenu, organizacija treba poduzeti odgovarajuće korake da podaci budu pouzdani za namjeravano korištenje, točni, potpuni i ažurirani." Radna skupina napominje da je to potpuno isti tekst koji se upotrebljava u aranžmanu „sigurne luke". Radna skupina sumnja da tekst „U mjeri u kojoj je to potrebno za

[22] Vidjeti dopis Radne skupine potpredsjednici Reding, 10. travnja 2014., točka 4. u dijelu „Daljnji prijenos".
[23] Vidjeti dopis Radne skupine potpredsjednici Reding, 10. travnja 2014., str. 8.

tu namjenu" treba biti uključen jer točnost podataka po njegovu mišljenju ne bi trebala ovisiti o namjeni obrade. Radna bi skupina radije htjela da se ta veza ne uključi u završnu verziju odluke o primjerenosti.

c) Ograničenje svrhe

Kada osobne podatke u američku organizaciju prenosi voditelj obrade podataka s poslovnim nastanom u EU-u, izvoznik podataka trebao bi američku organizaciju izričito informirati o svrhama za koje su podaci izvorno prikupljeni. To je nužno kako bi se utvrdilo događa li se promjena svrhe nakon prijenosa, čime se pokreću načela obavješćivanja i izbora i čime bi se doprinijelo raspodjeli rizika i odgovornosti.

U načelu o cjelovitosti podataka i ograničenju svrhe (odjeljak II. točka 5. Priloga II.) navodi se da organizacija ne smije obrađivati osobne informacije na način nespojiv sa svrhama za koje su prikupljeni ili koje je naknadno odobrio pojedinac. Međutim, načelo izbora (odjeljak II. točka 2. Priloga II.) osigurava izuzeće za „uporabu" osjetljivih informacija (tj. osobnih informacija u kojima se pobliže navode medicinsko ili zdravstveno stanje, rasno ili etničko podrijetlo, politička stajališta, vjerska ili filozofska uvjerenja, članstvo u sindikatima ili informacije o seksualnom životu pojedinca i podaci koji se odnose na kaznene evidencije) za svrhe koje su znatno drukčije od svrha za koje su podaci izvorno prikupljeni ili ih je pojedinac naknadno odobrio. To izuzeće nije potrebno u situacijama spomenutim u dodatnom načelu 1.a (odjeljak III. točka 1. podtočka (a) Priloga II.). Što se tiče osobnih informacija koje nisu osjetljive, predviđen je režim izuzeća.

Radna skupina napominje da se područje primjene načela o ograničenju svrhe razlikuje u okviru načela o obavješćivanju, načela o izboru i načela o cjelovitosti podataka i ograničenju svrhe. Zapravo, pojmovi „nespojiva namjena" i „znatno drukčija namjena" upotrebljavaju se u istom tekstu bez jasne definicije tih koncepata[24].

Radna skupina je veoma zabrinuta u pogledu činjenice da takva nedosljednost može dovesti do velikih poteškoća u usklađivanju načela o cjelovitosti podataka i ograničenju svrhe (odjeljak II. točka 5. Priloga II.) s načelom izbora (odjeljak II. točka 2. Priloga II.) jer jedno navodi da se podaci ne smiju obrađivati na način nespojiv sa svrhama za koje su bili prikupljeni, a drugim se predviđa mehanizam izuzeća ako se podaci obrađuju za svrhu koja je znatno drukčija od izvorne svrhe.

Dakle, načelo izbora može se protumačiti kao da se njime odobrava daljnja nespojiva obrada[25]. Prema Radnoj skupini, mora se izričito navesti da organizacija nije ovlaštena za obradu podataka za svrhu znatno drukčiju kada je ta svrha nespojiva prema načelu o

[24] Radna skupina je napomenula da se upotrebljavaju i neki drugi izrazi: „uporaba koja nije u skladu s" (odjeljak III. točka 14. podtočka (b) podtočka ii. Priloga II.), „upotrijebiti u različite svrhe" (odjeljak III. točka 9. podtočka (b) podtočka i. Priloga II.), „upotrijebi takve informacije u neku drugu svrhu osim one za koju ih je prvotno prikupila" (odjeljak II. točka 1. podtočka (b) Priloga II.). Ta nejasnoća može dovesti do nedostatka dovoljnih jamstava u odnosu na načelo o ograničenju svrhe.

[25] Također vidi primjedbu u sklopu načela izbora. Radna skupina smatra da činjenica da se pravila o daljnjem prijenosu (odjeljak II. točka 3. Priloga II.) odnose samo na načelo izbora, a ne na načelo o ograničenju svrhe, povećava rizik od takvog shvaćanja.

ograničenju svrhe. Drugim riječima, treba biti jasno da načelo izbora nije izuzeće od načela o ograničenju svrhe.

U svakom slučaju, ako se daljnja obrada može smatrati sukladnom, onda bi se trebala primjenjivati i načela o obavješćivanju i o izboru.

2.2.5. Novinarske iznimke

Novinarske iznimke u obradi osobnih podataka nalaze se u dodatnom načelu 2. (odjeljak III. točka 2. Priloga II.). Podrazumijeva se da te odredbe odražavaju zaštitu slobode govora prema američkom ustavu. Stoga se u dokumentima o sustavu zaštite privatnosti navodi da „osobne informacije pronađene u prethodno objavljenom materijalu iz medijskih arhiva ne podliježu zahtjevima načela „sigurne luke" (odjeljak III. točka 2. podtočka (b) Priloga II.). Čini se da ova odredba uključuje svaku daljnju obradu svakog voditelja obrade podataka ili izvršitelja obrade podataka, tj. da nije ograničena na daljnju obradu za novinarske svrhe. Kako je već navedeno u dopisu potpredsjednici Reding od 10. travnja 2014., Radna skupina bi voljela da je postojao ograničeniji pristup novinarskim iznimkama, više u skladu s načelom kako se ono primjenjuje u EU-u, kao i pravo na brisanje s popisa nakon predmeta Google Spain[26].

2.2.5. Pravo na pristup, ispravak i brisanje za osobe čiji se podaci obrađuju

Prema sustavu zaštite privatnosti pojedinci imaju pravo dobiti *potvrdu* o tome obrađuje li organizacija njihove podatke i na to da se im se takvi podaci *priopće* (odjeljak III. točka 8. podtočka (a) podtočka i. Priloga II.). Međutim, obveza za organizacije da odgovore na zahtjeve pojedinaca u vezi sa svrhama obrade, kategorijama osobnih podataka o kojima je riječ i primateljima ili kategorijama primatelja kojima se osobni podaci otkrivaju, vrlo je slaba. Radna skupina smatra da pojedinosti koje treba priopćiti osobi čiji se podaci obrađuju treba navesti u glavnom dijelu teksta, umjesto samo u fusnoti, i da se moraju sastaviti kao jasna obveza (povezano s Prilogom II., odjeljkom III. točkom 8. podtočkom (a) podtočkom i. podtočkom 1.).

Prema dodatnom načelu 8. „pristup treba omogućiti samo u onoj mjeri u kojoj organizacija ima pohranjene osobne informacije" (odjeljak III. točka 8. podtočka (d) podtočka ii. Priloga II.). To pravilo ne treba primjenjivati restriktivno, u smislu da se pristup mora osigurati, načelno, podacima koje neka organizacija obrađuje na bilo koji način, a ne samo pohranjenima. Stoga, u svrhu djelotvornosti prava pristupa, važno je jasno navesti da „pohranjuje" znači „obrađuje" u smislu definicije navedene u Prilogu II., odjeljku I. točki 8. podtočki (b). Potrebno je pomno ispitati primjenu ovog pravila tijekom zajedničkog preispitivanja sustava zaštite privatnosti.

I dalje postoji zabrinutost u pogledu popisa iznimaka utvrđenih Prilogom II. odjeljkom III. točkom 8. podtočkom (e) podtočkom i., koja je slična onom u često postavljanim pitanjima br. 8. „sigurne luke" i koja naginje štićenju interesa u korist organizacija. U tom smislu pojedinci

[26] Predmet C-131/12 – Google Spain protiv Agencia Española de Protección de Datos, Mario Costeja González, 13. svibnja 2014.

neće dobiti pristup vlastitim osobnim podacima iz sljedećih razloga: „kršenje obveze čuvanja profesionalnih tajni ili obveza”” (Prilog II. odjeljak III. točka 8. podtočka (e) podtočka 3.), „ugrožavanje istraga o sigurnosti zaposlenika ili žalbenih postupaka ili u vezi s planiranjem zamjene zaposlenika i korporativnim reorganizacijama” (Prilog II. odjeljak III. točka 8. podtočka (e) podtočka 4.), i „narušavanje tajnosti koja je potrebna radi praćenja, nadzora ili regulatorne funkcije povezane s dobrim upravljanjem, ili u budućim pregovorima u koje je organizacija uključena ili onima koji su u tijeku” (odjeljak III. točka 8. podtočka (e) podtočka 5. Priloga II.). Te razloge treba sagledati uz opću iznimku o povjerljivim trgovinskim informacijama koje su uključene u odjeljak III. točku 8. podtočku (c) Priloga II. Stoga pojedinac nikada neće imati pristup podacima o sebi u situacijama nabrojenima u prethodnom tekstu jer nije postignuta nikakva ravnoteža prava i interesa između onih koji se odnose na pojedinca i onih koji se odnose na organizaciju da se pronađe rješenje za zahtjev za pristup.

Radna skupina podsjeća da se pravo na pristup vlastitim podacima daje pojedincima u članku 8. stavku 2. Povelje. Iako to nije apsolutno pravo, od iznimne je važnosti za pravo na zaštitu osobnih podataka jer ono olakšava ostvarivanje drugih prava osobe čiji se podaci obrađuju, kao što su ispravak i brisanje.

Što se tiče prava na ispravak i brisanje, Radna skupina pozdravlja znatno poboljšanje koje su donijela načela sustava zaštite privatnosti, u usporedbi s načelima „sigurne luke” jer je njima predviđeno da se ta prava daju ne samo u situacijama kada su podaci netočni nego i kada su podaci obrađeni na način kojim se krše načela (odjeljak II. točka 6. Priloga II.).

2.2.6. Načelo pravne zaštite, provedbe i odgovornosti (mehanizmi pravne zaštite)

a) Djelotvorno ostvarivanje prava na pravnu zaštitu za pojedince iz EU-a

Radna skupina priznaje predanost američkih vlasti što se tiče različitih razina mehanizma pravne zaštite. Međutim, s obzirom na složenost i nedostatak jasnoće u cjelokupnoj arhitekturi ovog mehanizma, Radna skupina strahuje da, u praksi, djelotvorno ostvarivanje prava osobe čiji se podaci obrađuju može biti narušeno. Radna skupina ističe da kvaliteta mehanizma pravne zaštite treba prevladati količinu mehanizama koji su na raspolaganju pojedincima u EU-u. Tu je i zabrinutost da većina mehanizama pravne zaštite, ako ne i svi, predviđaju postupak u SAD-u, čime praćenje postupka koje provodi tijelo za zaštitu podataka u EU-u postaje još složenije.

Zapravo, mehanizam pravne zaštite predviđen sustavom zaštite privatnosti usredotočuje se ponajprije na mogućnost da osoba čiji se podaci obrađuju „ostvari svoja prava i usprotivi se slučaju nepoštovanja načela privatnosti izravnim kontaktima s američkim samocertificiranim poduzećem”[27]. Štoviše, organizacije moraju odrediti neovisno tijelo za rješavanje sporova za istragu i rješavanje pojedinačnih pritužbi. Radna skupina pozdravlja činjenicu da će to biti organizirano bez troškova za pojedinca.

[27] Europska komisija, nacrt odluke o primjerenosti, t. 30.

Alternativno, pritužbe se mogu podnijeti izravno Saveznoj trgovinskoj komisiji, iako ne postoji obveza FTC-a da se njima bave. Tijelo za zaštitu podataka također bi moglo uputiti pritužbu, a Ministarstvo trgovine se obvezalo preispitati pritužbe i poduzeti sve što može kako bi se olakšalo rješavanje pritužbi (Prilog I.), kojima će Savezna trgovinska komisija dati „prioritet u razmatranju" (odjeljak III. točka 7. podtočka (e) Priloga II.). Međutim, određivanje prioriteta pritužbi FTC-a ne daje nikakvu sigurnost osobi čiji se podaci obrađuju da će se njegove pritužbe rješavati.

Kao posljednji izbor, pojedinci će imati mogućnost zatražiti obvezujuću arbitražu. Arbitražni odbor nalazit će se u SAD-u te će podlijegati sudskoj kontroli američkih sudova.

Sustav zaštite privatnosti također pruža mogućnost da organizacija izabere suradnju s tijelima za zaštitu podataka u EU-u (odjeljak III. točka 5. podtočka (a) Priloga II.). To je čak i obvezno za podatke o ljudskim resursima prikupljene u okviru radnog odnosa (odjeljak III. točka 9. podtočka (d) podtočka ii. Priloga II.). U takvom scenariju alternativno rješavanje sporova (ADR) neće se primjenjivati (odjeljak III. točka 5. podtočka (a) Priloga II.). Sustav zaštite privatnosti ne utvrđuje jasno kako će se suradnja s tijelima za zaštitu podataka u EU-u organizirati u praksi. Konkretno, nejasno je hoće li se odbor baviti svim slučajevima ili hoće li se različitim slučajevima baviti neki drugi odbor.

Radna skupina smatra da je potrebno više pojedinosti u odluci o primjerenosti kada je riječ o nadležnosti tijela za zaštitu podataka da se bave pritužbama. To očito ovisi o osposobljenosti organizacije, ali je nejasno na koji način.

Kada organizacija djeluje kao posrednik u ime voditelja obrade u EU-u, pojedinci će u svakom slučaju imati mogućnost podnošenja prigovora nadležnom tijelu za zaštitu podataka u EU-u. Situacija će biti slična za obradu podataka o ljudskim resursima i za obradu drugih komercijalnih podataka.

Kada organizacija u sustavu zaštite privatnosti djeluje kao voditelj obrade podataka, nadležnost tijela za zaštitu podataka da se bavi pritužbom bit će ograničena na obradu podložno pravu EU-a (obrada pod odgovornošću voditelja obrade u EU-u – uključujući aranžman sa zajedničkim voditeljima obrade s američkom organizacijom – ili kada bi organizacija u sustavu zaštite privatnosti bila izravno podložna pravu EU-a, na primjer korištenjem opremom u EU-u). Međutim, za obradu podataka koja se obavlja samo prema američkom pravu primjenjivat će se isključivo mehanizmi sustava zaštite privatnosti. Kako bi se prebrodile jezične prepreke i nedostatak poznavanja američkog pravnog sustava, moglo bi biti korisno kad bi tijela za zaštitu podataka u EU-u bila nadležna djelovati kao posrednik za pritužbu pojedinca ili mu pomagati u postupcima alternativnog rješavanja sporova s američkim organizacijama ili tijekom njegovih kontakata s američkim tijelima ako to tijelo za zaštitu podataka smatra primjerenim.

Radna skupina naglašava da mehanizam objašnjen u sustavu zaštite privatnosti ne slijedi prijašnju preporuku prema kojoj bi pojedinci u EU-u trebali „biti u stanju podnositi tužbe za naknadu štete u Europskoj uniji" i „imati pravo na podnošenje tužbe pred nadležnim

nacionalnim sudom EU-u".[28] Bilo bi dobrodošlo kad bi organizacije u sustavu zaštite privatnosti uključile takvu mogućnost u svoje politike zaštite privatnosti.

Kako bi se osigurala djelotvornost, Radna skupina preporučuje da sustav treba omogućiti da tijela EU-a za zaštitu podataka zastupaju osobu čiji se podaci obrađuju i da djeluju u svoje ime ili kao posrednik. Alternativno, sustav treba sadržavati posebne odredbe o nadležnosti koje daju pravo osobama čiji se podaci obrađuju na ostvarenje njihovih prava u Europi.

b) Arbitraža

Završni arbitražni postupci još nisu dovršeni, što procjenu Radne skupine čini još složenijom. Budući da izgleda da će se program arbitraže odvijati prema američkom pravu i da će jedini jezik postupka biti engleski, može se dogoditi da tijela za zaštitu podataka EU-a žele imati pravo na pomaganje pojedincima u tom postupku.

Nadalje, uspostavljen je arbitražni postupak zato što nije bilo nikakvog osiguranja da će se pritužba rješavati jer Savezna trgovinska komisija nema dužnost rješavati svaku pritužbu. Ako neki pojedinac iz EU-a osjeti potrebu za pomoći odvjetnika, Radna skupina napominje da će on sam morati snositi troškove odvjetnika, što može spriječiti pojedince da podnesu svoju pritužbu za arbitražni postupak.

c) Nadzor, provedba i djelotvornost mehanizama pravne zaštite

<u>Uvjeti pristupa u sustav zaštite privatnosti</u>

Prema Sudu Europske unije, „pouzdanost sustava samocertificiranja […] zasniva se u osnovi na uspostavljanju djelotvornih mehanizama otkrivanja i nadzora koji omogućavaju da sva kršenja pravila kojima se osigurava zaštita temeljnih prava […]".[29]

Radna skupina napominje da se uloga sustava zaštite privatnosti Ministarstva trgovine u postupku certificiranja čini smanjenom na puku provjeru kompletnosti dokumentacije. Iako Radna skupina priznaje da samocertificiranje ne implicira sustavnu *a priori* provjeru provedbe politike zaštite privatnosti, Ministarstvo trgovine trebalo bi se obvezati barem na sustavnu provjeru da se utvrdi sadržavaju li politike zaštite privatnosti sva načela sustava zaštite privatnosti. Takva obveza spominje se u nacrtu odluke o primjerenosti, ali ne može se jasno utvrditi u dopisu s izjavom Ministarstva trgovine.[30]

Kršenje načela sustava zaštite privatnosti moglo bi proći neopaženo u duljem razdoblju i moglo bi se otkriti nakon što se izazove ozbiljna šteta za temeljna prava osobe čiji se podaci prikupljaju, možda i nepopravljiva. Dakle, taj pristup mogao bi biti u suprotnosti s europskim načelom opreznosti.

[28] Vidjeti dopis Radne skupine potpredsjednici Reding, 10. travnja 2014.
[29] CJEU, Schrems, t. 81.
[30] Europska komisija, nacrt odluke o primjerenosti, t. 34.

Transparentnost pomoću popisa sustava zaštite privatnosti i evidencije organizacija uklonjenih s popisa

Provedena su znatna poboljšanja u pogledu transparentnosti prema osobi čiji se podaci prikupljaju. Uza sve američke organizacije koje su se samocertificirale pri Ministarstvu trgovine, novi Popis organizacija u sustavu zaštite privatnosti sadržavat će i evidenciju svih organizacija uklonjenih s Popisa organizacija u sustavu zaštite privatnosti, uključujući razlog zbog kojega je organizacija uklonjena[31]. Internetska stranica sustava zaštite privatnosti Ministarstva trgovine i dalje će se više usmjeravati prema ciljnoj publici tako što će olakšavati provjeru vrste informacija obuhvaćenih samocertificiranjem organizacije i politikom zaštite privatnosti koja se primjenjuje na obuhvaćene informacije i metodu kojom se organizacija koristi za provjeru svog pridržavanja načela[32]. Radna skupina pozdravlja činjenicu da je sada eksplicitno da će Ministarstvo trgovine provjeriti objavljuju li poduzeća koja imaju javne internetske stranice svoju politiku zaštite privatnosti na tim internetskim stranicama ili, ako nemaju javne internetske stranice, tamo gdje je politika zaštite privatnosti dostupna javnosti[33]. U dokumentima također ima više informacija o sadržaju politike zaštite privatnosti[34].

Radna skupina smatra da bi mogao nastati problem ako organizacija koja je već uključena u Popis organizacija u sustavu zaštite privatnosti naknadno proširi svoj certifikat na druge kategorije podataka. U takvim slučajevima popis neće odražavati različita razdoblja primjenjivosti načela na različite kategorije podataka. To stvara rizik da pojedinci i poslovni subjekti iz EU-a ne mogu potpuno procijeniti podliježe li određeni skup podataka doista načelima sustava zaštite privatnosti i ako da, od kada. Radi izbjegavanja ovog nedostatka Radna skupina preporučuje da se u evidenciji o nekoj organizaciji na Popisu organizacija u sustavu zaštite privatnosti za svaku kategoriju osobnih podataka posebno navedu podaci o početku primjene samocertificiranja.

Radna skupina pozdravlja činjenicu da će Ministarstvo trgovine voditi evidenciju o organizacijama koje su uklonjene s Popisa organizacija u sustavu zaštite privatnosti i da će te evidencije sadržavati obrazloženje kojim se objašnjava da te organizacije više nemaju pravo na prednosti sustava zaštite privatnosti, ali moraju nastaviti primjenjivati načela na osobne podatke primljene dok su bile certificirane organizacije u sustavu zaštite privatnosti, sve dok zadržavaju takve podatke (str. 3. Priloga I.). Međutim, s obzirom na to da neke organizacije koje su uklonjene s Popisa organizacija u sustavu zaštite privatnosti mogu odlučiti vratiti ili izbrisati podatke dobivene u okviru sustava zaštite privatnosti, dok će druge organizacije zadržati podatke koje su primile u okviru sustava zaštite privatnosti, važno je osigurati veću transparentnost o ovom pitanju za pojedince. Stoga, u evidenciji o poduzećima koju vodi Ministarstvo gospodarstva treba navesti zadržava li organizacija još uvijek osobne podatke

[31] Prilog I., str. 5., i Prilog II., odjeljak II. točka 1.; Radna skupina upućuje i na četvrtu preporuku Komisije u Komunikaciji COM(2103) 847 i na dopis Radne skupine potpredsjednici Reding od 10. travnja 2014., osobito točku 5. u dijelu „Transparentnost".
[32] Prilog I., str. 8.; Radna skupina upućuje i na svoj dopis potpredsjednici Reding od 10. travnja 2014., osobito točku 2. u dijelu „Transparentnost".
[33] Prilog I., str. 3. i 4.; Radna skupina upućuje i na prvu preporuku Komisije u Komunikaciji COM(2103) 847 i dopis Radne skupine potpredsjednici Reding od 10. travnja 2014., osobito točku 3. u dijelu „Transparentnost".
[34] Prilog I., str. 5. i 6., i Prilog II., odjeljak III. točka 6.;

dobivene u okviru sustava zaštite privatnosti ili je takve podatke vratila ili izbrisala. Ako organizacija i dalje zadržava te podatke, u evidenciji treba izrijekom navesti da organizacija mora na takve podatke nastaviti primjenjivati načela.

Nadalje, u evidenciji koju vodi Ministarstvo gospodarstva treba napomenuti da te organizacije više nemaju pravo na prednosti sustava zaštite privatnosti za nove prijenose, što znači da organizacija, prema načelima, više ne smije primati osobne podatke iz EU-a.

Postupci provjere

Da bi se provjerilo je li samocerticiranje djelotvorno u praksi, organizacije mogu načiniti samoprocjenu ili provesti vanjsko preispitivanje usklađenosti. Radna skupina žali što je osposobljavanje zaposlenika potrebno samo kada se organizacija odluči za provjeru samoprocjenom (odjeljak III. točka 7. podtočka (c) Priloga II.). Čini se također da je provjera jesu li politike točne, sveobuhvatne, vidljivo istaknute, provedene i dostupne potrebna samo ako se organizacija odluči za interni postupak provjere (samoprocjene) i da je provjera koju učini neki vanjski mehanizam ograničena samo na usklađenost politikom zaštite privatnosti organizacije.

A posteriori

Radna skupina pozdravlja činjenicu da FTC i Ministarstvo trgovine imaju istražne ovlasti u slučajevima pritužbi. Štoviše, Radna skupina napominje da će Ministarstvo trgovine imati mogućnost provedbe provjera po službenoj dužnosti, osobito slanjem upitnika. Međutim, Radna skupina željela bi biti sigurna da je takav pristup dovoljan kako bi se zadovoljili zahtjevi CJEU-a za mehanizme djelotvornog otkrivanja i nadzor kršenja. Zapravo, Radna skupina još uvijek ima preostalih pitanja o konkretnim ovlastima američkih tijela kaznenog progona za provedbu inspekcija na licu mjesta u prostorijama samocertificiranih organizacija da istraže kršenja u sustavu zaštite privatnosti, o tome kako bi se mogla dobiti egzekvatura za odluku tijela u EU-u dobivena na američkom području i djeluju li sankcije u okviru sustava zaštite privatnosti odvraćajuće u praksi.

2.2.7. Obrada podataka o ljudskim resursima

Područje primjene

Dodatno načelo 9. (odjeljak III. točka 9. Priloga II.) primjenjuje se na osobne podatke o zaposleniku (bivšem ili sadašnjem) prikupljene u situaciji radnog odnosa. Prema tekstu dodatnog načela 9. točke (a) podtočke ii., načela sustava zaštite privatnosti primjenjuju se isključivo kod „datoteka koje se mogu pojedinačno identificirati ili se njima pristupa". Taj izraz „datoteka koja se može identificirati" nije u skladu s definicijom „osobnih podataka" iz dijela I. točke 8. podtočke (a) Priloga II., koja se sastoji od „podataka o identificiranoj osobi ili osobi čiji se identitet može utvrditi" te se prema tome ne slaže s definicijom koja se upotrebljava u Direktivi[35].

U dodatnom načelu 9. točka a. podtočka ii. navodi se da „Statističko izvješćivanje koje se temelji na skupnim podacima o zaposlenima i/ili upotrebi anonimnih podataka ili onih pod pseudonimom ne otvara pitanja privatnosti". Ova je izjava u suprotnosti s više Mišljenja koje je izdala Radna skupina. Radna skupina htjela bi naglasiti da se skupni podaci još uvijek mogu ponovno identificirati i stoga ih treba smatrati osobnim podacima[36].

[35] Kako je već istaknuto, ograničenje na evidencije koje su „prenesene ili kojima se pristupilo" također nije u skladu s izrazom „obrada" (odjeljak I. točka 8. podtočka (b) Priloga II.).
[36] Vidjeti Mišljenje 4/2007 o pojmu osobnih podataka i Mišljenje 05/2014 o tehnikama anonimizacije

Obavješćivanje, izbor i ograničenje svrhe

U dodatnom načelu 9. točki b. podtočki i. navodi se primjer primjene načela obavješćivanja i izbora, kada se podaci o ljudskim resursima upotrebljavaju za neku različitu svrhu. Ovaj primjer odnosi se na američku organizaciju koja se „namjerava koristiti osobnim podacima prikupljenima tijekom radnog odnosa u svrhe koje nisu vezane uz radni odnos, kao što su komercijalne obavijesti." U tom se scenariju promjena svrhe odobrava ako se poštuje načelo obavješćivanja i izbora. Prema Radnoj skupini, daljnja obrada podataka o ljudskim resursima u svrhu izravnog marketinga u većini će se slučajeva morati smatrati nespojivom svrhom i stoga suprotnom načelu o ograničenju svrhe (odjeljak II. točka 5. podtočka (a) Priloga II.). Osim toga, Radna skupina smatra da izbor ne može biti primjerena osnova za zaposlenika da „pristane" (zatraži izuzeće) na promjenu svrhe, u situaciji radnog odnosa kada takav pristanak možda ne bi bio potpuno slobodan.

Radna skupina uvelike sumnja da je glavna usmjerenost sustava zaštite privatnosti na načelo izbora kao uvjeta za daljnju upotrebu podataka za drugu svrhu u skladu sa Smjernicama OECD-a o privatnosti jer nema dovoljno jamstava da se spriječi da se taj mehanizam izuzeća također može upotrijebiti za daljnju obradu za nespojivu svrhu. U dodatnom načelu 9. točki b. podtočki iv. navodi se široko i izričito izuzeće od načela obavješćivanja i izbora „u onoj mjeri i onom razdoblju koje je potrebno da se izbjegne ugrožavanje sposobnosti organizacije pri unapređivanju, imenovanjima ili ostalim sličnim odlukama o zaposlenju." Kao prvo, korištenje podacima o ljudskim resursima za takve svrhe trebalo bi biti izričito navedeno već pri skupljanju podataka. Štoviše, tekst „ostalim sličnim odlukama o zaposlenju" previše je nejasan i širok. Posljedica toga bit će da će podaci o ljudskim resursima biti potpuno izuzeti od načela obavješćivanja i izbora kada će se obrađivati u kontekstu radnog odnosa. Taj je pojam tako širok da ne omogućava procjenu je li daljnja upotreba usklađena s izvornom svrhom. Radna skupina preporučuje brisanje tog izuzeća.

Pravo pristupa

U dodatnom načelu 9. točki (e) podtočki i. također se navodi izuzeće od primjene načela pristupa ili od sklapanja ugovora s trećom stranom koja djeluje kao voditelj obrade za podatke o ljudskim resursima kada se u slučaju povremenih operativnih potreba u kontekstu zapošljavanja, na primjer rezervacije zrakoplovne karte, hotelske sobe ili osiguranja, mogu izvršiti prijenosi osobnih podataka malog broja zaposlenika, pod uvjetom da se postupa u skladu s načelima obavješćivanja i izbora. Radna skupina ne vidi nikakvo razumno opravdanje za takvo izuzeće i preporučuje brisanje tog stavka.

2.2.8. Farmaceutski i medicinski proizvodi

Područje primjene

Sustav zaštite privatnosti smatra da prijenosi šifriranih podataka iz Europske unije u SAD kada je riječ o farmaceutskim i medicinskim proizvodima nisu prijenosi koji bi podlijegali sustavu zaštite privatnosti (odjeljak III. točka 14. podtočka (g) podtočka i. Priloga II.).

Međutim, prijenos šifriranih podataka uživa zaštitu u okviru europskog zakonodavstva o zaštiti podataka. To znači da u praksi sustav zaštite privatnosti ne može obuhvaćati takve prijenose. Radna skupina poziva Europsku komisiju da izrijekom predvidi da nacrt odluke o primjerenosti neće obuhvaćati prijenos šifriranih podataka o farmaceutskim ili medicinskim razlozima i kao posljedica toga, takvi prijenosi moraju se obuhvatiti drugim zaštitnim mjerama, kao što su standardne ugovorne klauzule (dalje u tekstu: SUK-ovi) ili BCR-ovi. Radna skupina predlaže da se to razjasni u završnoj verziji odluke o primjerenosti.

Prijenosi u regulatorne i nadzorne svrhe (odjeljak III. točka 14. podtočka (d) Priloga II.)

Radna skupina zabrinuta je da prema ovim odredbama osobni podaci koji se odnose na medicinski kontekst većinom osjetljive prirode mogu biti preneseni regulatornim tijelima u SAD-u. Budući da je sustav zaštite privatnosti osmišljen za prijenose podataka između privatnih subjekata, čini se da javno tijelo poput regulatora ili SAD-a ne zadovoljava uvjete za samocertificiranje u okviru sustava zaštite privatnosti, čime se postavlja pitanje primjerene zaštite podataka za takve prijenose. Ako je takve prijenose potrebno obaviti u regulatorne svrhe, moraju se poduzeti odgovarajuće mjere kako bi se osigurala trajna zaštita temeljnih prava osoba iz EU-a čiji se podaci obrađuju. Radna skupina naglašava da nacrt odluke o primjerenosti ne daje nikakve nalaze o ovoj točki. Stoga Radna skupina nema nikakvo jamstvo da će osjetljivi podaci o osobama iz EU-a čiji se podaci obrađuju imati primjerenu zaštitu u ovom kontekstu.

Osim toga, Radna skupina napominje da ne razumije zašto je svrha „marketing” navedena kao primjer obrade za buduća znanstvena istraživanja. Isto tako nije jasan razlog za stavljanje daljnjih prijenosa u podružnice trgovačkih društava i ostalih istraživača (odjeljak III. točka 14. podtočka (d) Priloga II.) pod naslovom „Prijenosi u regulatorne i nadzorne svrhe”. Ta je pitanja potrebno razjasniti u završnoj verziji odluke o primjerenosti.

Praćenje sigurnosti i učinkovitosti proizvoda (uključujući izvješćivanje državnih agencija) i praćenje pacijenata koji se koriste određenim lijekovima ili medicinskim proizvodima

Sustav zaštite privatnosti daje izuzeće za načela obavješćivanja, izbora, daljnjeg prijenosa i pristupa u mjeri u kojoj se pridržavanje načela ne podudara s usklađenošću s regulatornim zahtjevima. Nacrt odluke o primjerenosti ne daje nikakve nalaze u pogledu situacije u kojoj se načela o privatnosti ne podudaraju s usklađenošću s regulatornim zahtjevima. Ako bi Radna skupina mogla razumjeti da državne istrage mogu opravdati ograničenja za obavješćivanje i pravo na pristup kako bi se zaštitile istrage, Radna skupina ne vidi razlog koji bi mogao opravdati takva široka izuzeća kada obradu obavlja organizacija ili treća strana u privatnom sektoru. Na primjer, s obzirom na to da su liječenja pacijenata sve više individualizirana, takvo je široko izuzeće od načela privatnosti u slučaju praćenja pacijenata koji se koriste određenim lijekovima ili medicinskim proizvodima neprihvatljivo jer će ovakva vrsta skrbi postati uobičajena. To se također odnosi na slučajeve kada podatke upotrebljavaju farmaceutske kompanije za praćenje sigurnosti i učinkovitosti proizvoda (ispitivanje ili prodaja novih lijekova).

2.2.9. Javno dostupne informacije

Iznimka od prava na pristup u slučaju javno objavljenih informacija i informacija iz javne evidencije (odjeljak III. točka 15. podtočke (d) i (e) Priloga II.) izazivaju zabrinutost u smislu da pojedinca, pri ostvarivanju njegova prava pristupa, zanima obrađuje li neki voditelj obrade podatke o njemu i koji se podaci obrađuju, kako bi mogao kontrolirati obradu svojih podataka. Radna skupina opetovano je ponavljala da prema pravu EU-a osobe čiji se podaci obrađuju uvijek imaju pravo pristupa svojim podacima i, kada je to potrebno, zahtijevati ispravljanje ili brisanje podataka ako podaci nisu bili obrađeni na zakonit način ili ako su nepotpuni ili netočni, neovisno o tome jesu li osobni podaci bili objavljeni[37]. Ako se zahtjev pojedinca za pristup odbije uz obrazloženje da su podaci dobiveni iz javno dostupnih izvora ili iz javnih evidencija, pojedinac bi izgubio sposobnost za kontroliranje točnosti podataka i jesu li podaci uopće objavljeni na zakonit način.

Međutim, sustav zaštite privatnosti izuzima javne evidencije i javno dostupne informacije iz načela obavješćivanja, izbora, pristupa i odgovornosti za daljnje prijenose (odjeljak II. točka 15. podtočka (b) Priloga II.). Ta izuzeća čine se suviše širokima u usporedbi s Direktivom i izazivaju zabrinutost jer narušavaju, među ostalim, mogućnosti pojedinaca da kontroliraju točnost svojih podataka i da ograniče širenje svojih podataka.

2.3. Zaključci

Radna skupina priznaje da su američka tijela i Europska komisija donijele znatna poboljšanja u komercijalne aspekte za prijenos podataka između dvaju kontinenata. Uzimajući u obzir prethodnu analizu, Radna skupina ipak smatra da je komercijalni dio sustava zaštite privatnosti u mnogim točkama potrebno dodatno objasniti. Na primjer, nedostatak izričitog načela zadržavanja podataka, razlog je za zabrinutost. Stoga je Radna skupina izrazito zabrinuta u pogledu toga može li sustav zaštite privatnosti osigurati razinu zaštite koja je u načelu istovjetna onoj u EU-u.

U odluci o primjerenosti trebaju se dodatno razjasniti načela o ograničenju svrhe i izbora. Preostaju rizici od praznina u okviru nekoliko načela, uglavnom u pogledu daljnjih prijenosa, mehanizma rješavanja pritužbi i obrade podataka o ljudskim resursima i farmaceutskih podataka. Osim toga, potrebno je dodatno razraditi kako se načela sustava zaštite privatnosti trebaju primjenjivati na izvršitelje obrade podataka (posrednike) i potrebno je obratiti posebnu pozornost da se osigura jasna i nedvosmislena primjena terminologije.

3. PROCJENA JAMSTAVA NACIONALNE SIGURNOSTI NACRTA ODLUKE O PRIMJERENOSTI

3.1. Zaštitne mjere i ograničenja primjenjiva na tijela nacionalne sigurnosti SAD-a

Uplitanja u temeljna prava na privatni život i zaštitu podataka mogu biti dopuštena, pod uvjetom da je takvo uplitanje opravdano u demokratskom društvu. To znači da načela

[37] Vidjeti WP20, str. 4.

privatnosti nisu apsolutna i da odstupanja mogu biti moguća, no samo ako su odgovarajuća (bitna) jamstva zadovoljena. U skladu s ciljem povećanja zaštite privatnosti, organizacije trebaju što više nastojati u potpunosti i transparentno provoditi ta načela, također i tako da u svojim postupcima zaštite privatnosti navode kada će se redovito primjenjivati iznimke od načela, koje dopušta pravni okvir SAD-a. Iz istog razloga, ako je mogućnost odabira dopuštena prema načelima i/ili zakonodavstvu SAD-a, očekuje se da se organizacije odluče za veću zaštitu tamo gdje je moguće.

U Prilogu II. odjeljku I. točki 5. navodi se da „poštovanje načela privatnosti može biti ograničeno: (a) u onoj mjeri koja je potrebna da se ispune uvjeti nacionalne sigurnosti, javnog interesa ili kaznenog progona; (b) zakonom, vladinom uredbom ili sudskom praksom koji proizvode proturječne obveze ili izričita dopuštenja, ako pri korištenju takvog dopuštenja organizacija može dokazati da je njezino nepoštovanje načela ograničeno u mjeri potrebnoj da se ostvare pretežući zakoniti interesi koje podupire takvo dopuštenje ili (c) ako direktiva ili nacionalno pravo države članice predviđa iznimke ili odstupanja, uz uvjet da se takve iznimke ili odstupanja primjenjuju u sličnim kontekstima.

Pitanje je jesu li odstupanja spomenuta u Prilogu II. opravdana u demokratskom društvu. Prema nacrtu odluke o primjerenosti sustava zaštite privatnosti, Komisija je utvrdila da „u Sjedinjenim Američkim Državama uspostavljena su pravila za ograničavanje svakog uplitanja, za potrebe nacionalne sigurnosti, u temeljna prava osoba čiji se osobni podaci prenose iz Unije u Sjedinjene Američke Države na temelju sustava zaštite privatnosti na one koji su strogo nužni za postizanje predmetnog legitimnog cilja.”[38]

Koristeći se okvirom opisanom u točki 1.2 ovog Mišljenja i uzimajući u obzir izjave tijela vlasti SAD-a i zaključke Komisije, Radna skupina ocijenila je trenutačni pravni okvir SAD-a, prakse obavještajnih agencija SAD-a i uvjete na temelju kojih dopuštaju svako uplitanje u temeljna prava u pogledu privatnog života i zaštite podataka kako su zaštićeni na temelju europskog pravnog okvira. Ova se ocjena temelji na analizi Predsjedničkog ukaza br. 28. (PPD-28), Izvršnog naloga br. 12333 (EO12333) i različitih pravnih osnova uspostavljenih Zakonom o nadzoru stranih obavještajnih službi (FISA – članak 104., članak 402., članak 215., članak 501. i članak 702.). Radna skupina oslonila se na Prilog VI. sustava zaštite privatnosti koji se sastoji od dopisa koji je pripremio Ured Direktora nacionalne obavještajne agencije (ODNI) u pogledu mjera zaštite i ograničenja primjenjivih na tijela nacionalne sigurnosti SAD-a uz sažimanje informacija koje je pribavila Europska komisija u pogledu SAD-ova prikupljanja informacija elektroničkim izviđanjem.

3.2. Jamstvo A – Obrada treba biti u skladu sa zakonom i temeljena na jasnim, preciznim i pristupačnim pravilima

Prema europskom pravu, uplitanje mora biti u skladu sa zakonima, utvrđenim politikama i postupcima te dovoljno jasno i pristupačno (unutar granica diskrecijske odluke dodijeljene pojedinačnim zemljama) kako bi se građanima dala odgovarajuća naznaka u pogledu

[38] Nacrt odluke Komisije na temelju Direktive 95/46/EZ Europskog parlamenta i Vijeća o primjerenosti zaštite koju ju pruža sustav zaštite privatnosti uspostavljen između EU-a i SAD-a, t. 75

okolnosti u kojima i uvjeta pod kojima javna tijela vlasti imaju ovlasti pribjeći mjerama nadzora.[39]

Radna skupina primjećuje da se prikupljanje informacija elektroničkim izviđanjem provodi na temelju dostupnog pravnog okvira. Svi zakoni navedeni u Prilogu VI. (Predsjednički ukaz br. 28., FISA, Zakon o slobodi SAD-a, FOIA) dostupni su internetom općoj javnosti (u SAD-u i izvan njega). Prilog VI. daje sažetak upravljačkog pravnog okvira, ograničenja prikupljanja, zadržavanja i ograničenja diseminacije te informacije o usklađenosti, nadzoru, transparentnosti i pravnoj zaštiti. Pravni sustav SAD-a za obavještajne aktivnosti sastoji se od nekoliko različitih dokumenata, uključujući izvješća, politike i postupke pojedinačnih agencija koje treba analizirati kako bi se steklo razumijevanje načina provedbe aktivnosti u teoriji i praksi. U tom pogledu, Radna skupina koncentrirala se na ograničen broj točaka koje smatra ključnima.

3.2.1. Izvršni nalog br. 12333 i Predsjednički ukaz br. 28.

Opseg područja primjene Izvršnog naloga br. 12333 (EO12333) je širok; načelno, svako prikupljanje stranih obavještajnih podataka može se odvijati po diskrecijskoj odluci predsjednika SAD-a na temelju Naloga. Ipak, tvrdi se da se nakon uvođenja FISA-e Izvršnim nalogom br. 12333 može jedino koristiti za prikupljanje podataka izvan područja SAD-a. Radna skupina primjećuje da Izvršni nalog br. 12333 ne daje puno pojedinosti o svojem zemljopisnom području primjene, mjeri u kojoj se podaci mogu prikupljati, zadržavati ili dalje širiti i o prirodi kaznenih djela koja mogu dovesti do nadzora ili o vrsti informacija koje se mogu prikupljati ili upotrebljavati.

Prema shvaćanju Radne skupine, glavna svrha Predsjedničkog ukaza br. 28. (PPD-28) je propisati ograničenja za prikupljanje i obradu osobnih podataka, bez obzira na to kojim se programom nadzora koristi i gdje su podaci pribavljeni.

Predsjednički ukaz br. 28. je ukaz predsjednika Sjedinjenih Američkih Država kojim se određuju načela dosljednosti prema kojima će se prikupljanje podataka elektroničkim izviđanjem ovlastiti i provoditi, no Predsjednički ukaz br. 28. nije pravni temelj za prikupljanje. Predsjednički ukaz br. 28. djeluje nametanjem tih načela tijelima obavještajne zajednice radi primjene u njihovim politikama i postupcima. Taj se ukaz primjenjuje na prikupljanje informacija elektroničkim izviđanjem, bez obzira na lokaciju podataka u vrijeme prikupljanja , unutar ili izvan SAD-a. Stoga se on također primjenjuje na podatke prikupljene za potrebe prikupljanja informacija elektroničkim izviđanjem pri prijenosu iz EU-a u SAD.

[39] ESLJP Zakharov, t. 247.: „Sud je prethodno utvrdio da uvjet 'predvidivosti' zakona ne ide tako daleko da prisiljava države da donesu zakonske odredbe kojima se detaljno navode svi postupci koji mogu dovesti do odluke o podvrgavanju pojedinca tajnom nadzoru na temelju 'nacionalne sigurnosti'. Po prirodi stvari, prijetnje nacionalnoj sigurnosti mogu varirati prema karakteru i mogu biti neočekivane ili ih može biti teško definirati unaprijed (vidjeti predmet Kennedy, prethodno citiran, t. 159.)." Istodobno, Sud je također naglasio da bi kod pitanja koja utječu na temeljna prava također bilo suprotno vladavini prava, jednom od osnovnih načela demokratskog društva ugrađenom u Konvenciju, kada bi diskrecijska prava dana izvršnoj vlasti u sferi nacionalne sigurnosti bila izražena u obliku vlasti bez ikakvog nadzora. Posljedično, zakon mora naznačiti područje primjene svakog takvog diskrecijskog prava danog nadležnim tijelima i način njegova izvršavanja s dovoljnom jasnošću, uzimajući u obzir legitiman cilj predmetne mjere kako bi se pojedincu dala odgovarajuća zaštita od arbitrarnog uplitanja.

Posebice, Predsjednički ukaz br. 28. navodi da će prikupljanje informacija elektroničkim izviđanjem biti prilagođeno načinu na koji je izvedivo[40]. U pogledu upotrebe podataka, njime se određuju postupci minimalizacije podataka (uključujući uvjete za zadržavanje i diseminaciju podataka), sigurnosti podataka i pristupa relevantnog osoblja [tj. pravila koja sadržavaju mjere zaštite kojima se ograničavaju rizici zloupotrebe i neprikladne upotrebe], kvalitete podataka i nadzora. Ta se jamstva primjenjuju bez obzira na državljanstvo osoba čiji se podaci obrađuju, tj. bez obzira na to je li riječ o državljanima SAD-a.

Mjere zaštite koje su uspostavljene Predsjedničkim ukazom br. 28. također su primjenjive tijekom prijenosa podataka u SAD. Prilog VI. sadržava obvezu ODNI-a da kada obavještajna zajednica SAD-a prikuplja podatke s prekoatlantskih kabela pri prijenosu u Sjedinjene Američke Države „ona to čini uz poštovanje ograničenja i mjera zaštite navedenih u ovom dokumentu, uključujući uvjete koje navodi Predsjednički ukaz br. 28."[41]. Radna skupina primjećuje kako i dalje postoji manjak utvrđene sudske prakse koja određuje zakonitost prikupljanja informacija elektroničkim izviđanjem u pogledu informacija prenošenih kabelima kada ga provodi bilo koja zemlja. U svakom slučaju, SAD ne potvrđuje i ne niječe da se koristi prikupljanjem informacija prenošenih kabelima elektroničkim izviđanjem.

Koncept „prikupljanja informacija elektroničkim izviđanjem" nije definiran Predsjedničkim ukazom br. 28. ili nekim drugim primjenjivim tekstom.

3.2.2. Zakon o nadzoru stranih obavještajnih službi

Sveukupno, tekst FISA-e čini se jasnijim i preciznijim. Ipak, tumačenje brojnih odredbi u svjetlu Predsjedničkog ukaza br. 28. i njihova praktična primjena u velikoj mjeri ovise o provedbi koju vrše različitih agencija. Dok puno izvješće o provedbi novih mjera zaštite još uvijek nije dostupno, izaslanici SAD-a obavijestili su predstavnike Radne skupine da je provedba mjera zaštite iz Predsjedničkog ukaza br. 28. zaista dovršena i da se izvršava na sličan način širom obavještajne zajednice SAD-a.

Točnije, članak 501. razmjerno je jasan u pogledu obavještajnih aktivnosti za koje je moguće dati ovlasti: „proizvodnja opipljivih predmeta (uključujući knjige, snimke, papire, dokumente i druge predmete)." Ipak, treba primijetiti kako činjenica da definicija „opipljivih predmeta" uključuje „druge predmete", što područje primjene ovog ovlaštenja čini prilično širokim.

Članak 702. kojom je dopušteno prikupljanje podataka od osoba koje nisu državljani SAD-a za koje se razumno vjeruje da se nalaze izvan Sjedinjenih Američkih Država kako bi se pribavili strani obavještajni podaci[42] ne pruža jednaku razinu pojedinosti kao članak 501. U pogledu njegova područja primjene, članak 702. usmjeren je prema pružateljima usluga elektroničkih komunikacija s poslovnim nastanom u SAD-u radi prikupljanja stranih

[40] „Prikupljanje informacija elektroničkim izviđanjem treba biti prilagođeno načinu na koji je izvedivo. Pri određivanju treba li prikupljati informacije elektroničkim izviđanjem, Sjedinjene Američke Države razmotrit će raspoloživost drugih informacija, uključujući one iz diplomatskih i drugih izvora. Prednost se daje takvim odgovarajućim i mogućim alternativama prikupljanju informacija elektroničkim izviđanjem." (Članak 1.(d))

[41] Prilog VI. sustava zaštite privatnosti, dopis Ureda Direktora nacionalne obavještajne agencije (ODNI) u pogledu zaštitnih mjera i ograničenja primjenjivih na tijela nacionalne sigurnosti SAD, str. 2.

[42] Zakonik SAD-a, glava 50., čl. 1881a (D)(1)

obavještajnih podataka o osobama smještenima izvan SAD-a. Definicija „stranih obavještajnih podataka" je široka. Ona uključuje, između ostaloga, „informacije u pogledu strane sile ili stranog teritorija koji se odnosi na vođenje inozemnih poslova Sjedinjenih Američkih Država"[43] što ukazuje na određenu nesigurnost u pogledu vrste informacija koje se u praksi mogu prikupljati.

Unatoč ukidanju tajnosti dokumenata, izvješća Kongresu i izvješća o nadzoru Nadzornog odbora za zaštitu privatnosti i građanskih sloboda (dalje u tekstu: PCLOB), primjena FISA-e, uključujući područje primjene i upotrebe navedenih uvjeta odabira ostaje nejasno i zbunjujuće. Upotreba navedenih uvjeta za odabir („zadanih čimbenika za odabir") navodi se u izvješću PCLOB-a[44], no Radna skupina smatra da to ne odgovara pravilima određivanja ciljeva u skladu s člankom 702[45]. Ne navodi ih se u općenito pristupačnim pravilima, bar u onoj mjeri u kojoj je Radna skupina to mogla potvrditi.

3.2.3. Zaključak

Sveukupno, Radna skupina primjećuje da su primjenjivi tekstovi koji se odnose na obavještajne aktivnosti dostupni internetom i da su tijela vlasti SAD-a poduzela i poduzimaju važne korake prema transparentnosti.

Radna skupina potvrđuje kako je od 2013. objavljen velik broj dokumenata, kao što su politike, postupci, odluka FISC-a i drugi dokumenti s kojih je skinuta oznaka tajnosti. Štoviše, PCLOB je objavio važna izvješća o aktivnostima provedenima na temelju članka 702. i Zakona o slobodi SAD-a. Slično izvješće očekuje se o aktivnostima na temelju Izvršnog naloga br. 12333.

Nekoliko zakonodavnih priloga, koji bi mogli rasvijetliti implikacije Izvršnog naloga za osobe izvan Sjedinjenih Američkih Država i sve primjenjive mjere zaštite, je tajno i kao takvi nisu pristupačni javnosti ili osobama na koje moguće utječe njihova primjena. U slučajevima gdje je s njih skinuta oznaka tajnosti, oni daju samo ograničenu vrijednost i uvid u obavještajne aktivnosti.

Unatoč naporima uloženima u objašnjavanje funkcioniranja Izvršnog naloga br. 12333 nakon otkrivanja informacija u slučaju Snowden, posebno donošenjem Predsjedničkog ukaza br. 28., trenutačna praktična primjena Izvršnog naloga br. 12333 ostaje nejasna. Radna skupina primjećuje da Prilog VI. sustava zaštite privatnosti ne daje detaljne informacije o funkcioniranju Izvršnog naloga br. 12333.

Premda Radna skupina pozdravlja otklanjanje ograničenja Predsjedničkim ukazom br. 28., teško je razmotriti je li pravni okvir SAD-a za nadzor dovoljno predvidiv, tj. sadržava li „odgovarajuću naznaku/naznake u pogledu okolnosti u kojima i uvjetima u kojima su tijela javne vlasti ovlaštene pribjeći svim takvim mjerama" i očekuje se dodatno pojašnjenje, uključujući objavu izvješća PCLOB-a o Izvršnom nalogu br. 12333.

[43] Zakonik SAD-a, glava 50., čl. 1801 (e)(2)
[44] Izvješće PCLOB-a o programu nadzora provođenom na temelju članka 702. FISA-e, str. 32.
[45] Zakonik SAD-a, glava 50., čl. 1881a(D)

3.3. Jamstvo B – Potrebno je pokazati potrebu i razmjernost u pogledu legitimnih ciljeva

3.3.1. Predsjednički ukaz br. 28

Predsjednički ukaz br. 28. uvodi ograničenja u pogledu svrhe zbog koje se osobni podaci mogu koristiti i uvjeta u kojima ih se može dijeliti te utjecaja prikupljanja podataka elektroničkim izviđanjem bez obzira ne primijenjeni pravni temelj.

Posebice, članak 1. Predsjedničkog ukaza br. 28. određuje da SAD-ovo prikupljanje informacija elektroničkim izviđanjem uvijek mora biti „prilagođeno načinu na koji je izvedivo". Premda se priznaje to ograničenje, teško je odrediti znači li „prilagođeno načinu na koji je izvedivo" da je svako prikupljanje podatka potrebno i razmjerno.

Predsjednički ukaz br. 28. priznaje da je većina prikupljanja i dalje dopuštena „kako bi se identificiralo nove ili nastajuće prijetnje i druge vitalne informacije vezane za nacionalnu sigurnost koje su često skrivene unutar velikog i složenog sustava modernih globalnih komunikacija".[46] Radna skupina primjećuje kako Predsjednički ukaz br. 28. navodi da „informacije 'masovno' prikupljene elektroničkim izviđanjem znači ovlašteno prikupljanje velikih količina informacija prikupljenih elektroničkim izviđanjem koje se, zbog tehničkih ili operativnih razloga, prikupljaju bez upotrebe razlikovnih čimbenika (npr. posebni identifikator, uvjeti odabira itd.)."

Predsjednički ukaz br. 28. nameće ograničenja upotrebe „masovnog" prikupljanja informacija elektroničkim izviđanjem u pogledu svrhe korištenja. Tih šest svrha zbog kojih podaci mogu biti „masovno" prikupljani, uključujući borbu protiv terorizma i drugih oblika teških (međunarodnih) kaznenih djela. Analiza Radne skupine upućuje da je to ograničenje svrhe prilično široko (i moguće previše široko) da bi se smatralo usmjerenim.

Predsjednički ukaz br. 28. nije otklonio mogućnost neselektivnog masovnog prikupljanja osobnih podataka i da veličina takvih mogućnosti prikupljanja ostaje nejasna i potencijalno široka. U tom pogledu, Radna skupina primjećuje kako Prilog VI. ODNI-ja potvrđuje da se „sve aktivnosti masovnog prikupljanja u pogledu komunikacija internetom koje obavještajna zajednica SAD-a izvršava elektroničkim izviđanjem primjenjuju na malom dijelu interneta[47] i stoga bi cijenila davanje daljnjih dokaza u pogledu mjera transparentnosti."

3.3.2. Zakon o nadzoru stranih obavještajnih službi

Članci 215. i 702. FISA-e u pogledu postupaka za minimalizaciju uvedeni su kako bi se državljane SAD-a zaštitilo od dalekosežnog pristupa vlade njihovim podacima. Ta se

[46] Članak 2. Predsjedničkog ukaza br. 28. i Prilog VI. sustava zaštite privatnosti, dopis Ureda Direktora nacionalne obavještajne agencije (ODNI) u pogledu zaštitnih mjera i ograničenja primjenjivih na tijela nacionalne sigurnosti SAD, str. 3.
[47] Prilog VI. sustava zaštite privatnosti, dopis Ureda Direktora nacionalne obavještajne agencije (ODNI) u pogledu zaštitnih mjera i ograničenja primjenjivih na tijela nacionalne sigurnosti SAD-a, str. 4. Radna skupina podsjeća u ovom pogledu na izvješće o nalazima europskih supredsjedatelja ad hoc radne skupine EU-a i SAD-a o zaštiti osobnih podataka koja navodi da „Komunikacijski podaci čine vrlo mali dio globalnog internetskog prometa" s obzirom na to da se „velika većina globalnog internetskog prometa sastoji od prijenosa (streaming) i preuzimanja sadržaja, kao što su televizijske serije, filmovi i sport" (točka 3.1.2. izvješća) 44.

ograničenja službeno ne primjenjuju na strance, premda su dužnosnici vlade SAD-a opetovano izjavljivali na javnim i privatnim sastancima s predstavnicima Radne skupine da je područje primjene postupaka minimalizacije od tada u praksi prošireno tako da obuhvaća sve osobe, bez obzira na njihovo državljanstvo ili uobičajeno mjesto boravka.

Članak 702. određuje da će ovlašteno pribavljanje „biti provođeno na način koji je dosljedan s četvrtim amandmanom na Ustav Sjedinjenih Američkih Država, što ograničava prikupljanje podataka na one koji su u skladu s načelom razumne pretrage. U tom pogledu, ne pravi se nikakva razlika između društava iz SAD-a i onih izvan SAD-a." Drugim riječima, pod uvjetom da se četvrti amandman primijeni na sve podatke prikupljane u SAD-u, „masovno" prikupljanje koje se odvija u SAD-u bilo bi „nerazumno" i stoga neustavno.

Radna skupina pozdravlja zaključke izvješća PCLOB-a da „u praksi, 'osobe koje nisu državljani SAD-a' također uživaju pogodnosti ograničenja pristupa i zadržavanja koja postavljaju postupke minimalizacije i/ili usmjeravanja različitih agencija zbog troška i teškoća povezanih s identificiranjem i uklanjanjem informacija o osobama koje su državljani SAD-a kod opsežnih skupova podataka, što znači da se cjelokupnim skupom podataka rukuje u skladu s višim standardima SAD-a."

Radna skupina također primjećuje da, prema zaključcima PCLOB-a, „program ne djeluje tako da masovno prikuplja komunikacije". Statističko izvješće o transparentnosti za 2014. koje je izdao ODNI potvrđuje ovaj zaključak. Dodatno, u skladu s izvješćem PCLOB-a, „zadani čimbenici za odabir", kao što su adresa e-pošte ili telefonski broj, upotrebljavaju se za usmjeravanje nadzora[48].

Odgovarajuća dostupna javna pravila koja se odnose na usmjeravanje ipak ne daju takva pravila usmjeravanja i jedini im je cilj izbjeći usmjeravanje na državljane SAD-a ili osobe s prebivalištem u SAD-u. Štoviše, pogodnosti koje se prema PCLOB-u primjenjuju na osobe koje nisu državljani SAD-a u praksi nisu zakonski obvezujuće ili zakonski utvrđene jer dostupno zakonodavstvo, koje se odnosi na usmjeravanje, ne određuje takva pravila usmjeravanja i jedini mu je cilj izbjegavanje usmjeravanja na državljane SAD-a ili osobe s prebivalištem u SAD-u.

Radna skupina nadalje podsjeća da, za potrebe članka 702., osobe nisu samo pojedinci već i skupine, subjekti, udruge, korporacije ili strane sile. Štoviše, činjenica da je prikupljanje opravdano time što je „znatna svrha prikupljanja pribavljanje stranih obavještajnih podataka" ostavlja određenu nesigurnost u pogledu njegove svrhe i potrebe. Ipak, Radna skupina pozdravlja informacije dane u Prilogu VI. da je 2014. ukupan broj pojedinaca na temelju članka 702. bio približno 90 000 pojedinaca[49]. Prvo preispitivanje sustava zaštite privatnosti pružit će priliku za davanje dodatnih dokaza o pravilima usmjeravanja.

Još uvijek ne postoji nedvosmislena sudska praksa o legalnosti masovnog i neselektivnog prikupljanja podataka i kasnije upotrebe osobnih podataka za potrebe borbe protiv kriminala,

[48] Izvješće PCLOB-a o programu nadzora provođenom na temelju članka 702. FISA-e, str. 32.
[49] Prilog VI., str. 11.

uključujući pitanje pod kojim se okolnostima takvo prikupljanje i upotreba osobnih podataka može odvijati. Očekuje se da Sud EU-a odgovori na ovo pitanje bar u određenoj mjeri tijekom 2016. i u spojenim predmetima Tele2 Sverige AB protiv Post- och telestyrelsen i Secretary of State for the Home Department v. Davisa i drugih[50] i u savjetu koji će dati u pogledu valjanosti PNR sporazuma s Kanadom.[51] U međuvremenu, Radna skupina podsjeća da je ona dosljedno smatrala da masovno i neselektivno prikupljanje podataka u bilo kojem slučaju ne može biti smatrano razmjernim.[52]

3.3.3. Zaključak

Unatoč ograničenjima uspostavljenima uvođenjem Predsjedničkog ukaza br. 28., ostaju postojati razlozi za zabrinutost Radne skupine u pogledu razmjernosti prikupljanja podataka. Prije svega, postoje naznake da SAD nastavlja masovno i neselektivno prikupljati podatke ili barem ne isključuje da bi to ipak bilo moguće u budućnosti. Radna skupina dosljedno je smatrala da takvo prikupljanje podataka nije u skladu s pravom EU-a i stoga nije prihvatljivo.

Drugo, Radna skupina primjećuje i da se usmjerena obrada podataka ili obrada koja je „prilagođena načinu na koji je izvediva" ipak može smatrati masovnom. Pitanje treba li takvo masovno prikupljanje podataka biti dopušteno ili ne trenutačno je predmetom postupka pred Sudom EU-a. Iz tog razloga, Radna skupina neće donijeti konačnu procjenu zakonitosti usmjerene, no masovne obrade podataka. Ipak, naglašava da kada bi usmjerena, no masovna obrada podataka bila dopuštena, načela usmjeravanja trebaju se primjenjivati i na prikupljanje i na kasniju upotrebu tih podataka i ona ne mogu biti ograničena samo na upotrebu. U svakom slučaju, potrebno je pojašnjenje nacrta odluke o primjerenosti u pogledu šest ciljeva navedenih u Predsjedničkom ukazu br. 28. o tome koji se podaci mogu „masovno" prikupljati. Radna skupina, u ovom trenutku, nije uvjerena da su ti ciljevi dovoljno ograničeni kako bi se osiguralo da je prikupljanje podatka zaista ograničeno na ono što je potrebno i razmjerno.

3.4. Jamstvo C – Treba postojati neovisan mehanizam nadzora

SAD nema jedinstveno tijelo za nadzor na federalnoj razini čiji je zadatak nadzor nad implikacijama obavještajnih programa i programa nadzora za privatnost i zaštitu podataka. Umjesto toga, obavještajne aktivnosti SAD-a podliježu procesu nadzora na više razina: može se razlikovati unutarnji i vanjski nadzor. Radna skupina priznaje da je praksa izvješćivanja tijela za nadzor u SAD-u vrlo detaljna i većinom javna.

3.4.1. Unutarnji nadzor

Sve obavještajne i sigurnosne agencije imaju članove osoblja koji su odgovorni za osiguravanje usklađenosti s njihovim zakonodavnim okvirom, uključujući glavne inspektore čiji je primarni zadatak ocjenjivanje sveukupne usklađenosti rada agencija sa zakonodavstvom, uključujući zakone povezane s privatnošću i zaštitom podataka, no bez

[50] Sud EU-a, spojeni predmeti C-203/15 i C-698/15
[51] Sud EU-a, predmet A-1/15
[52] Radna skupina 215 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf

ograničavanja na njih. Glavni inspektori ustrojeni su zakonom i imenovao ih je (ili će ih uskoro imenovati) Predsjednik, nakon čega slijedi potvrda Senata, kako bi se osigurala njihova organizacijska neovisnost i da svoja izvješća podnose Kongresu. Radna skupina smatra da će glavni inspektori stoga vjerojatno zadovoljiti kriterij organizacijske neovisnosti kako ga je definirao Sud EU-a i Europski sud za ljudska prava (ESLJP), bar od trenutka kada se novi proces imenovanja primijeni na sve. U ovom trenutku ostaju određena pitanja u pogledu glavnih inspektora koje su imenovali ravnatelji agencija koje nadziru.

Glavni inspektor može dati preporuke koje se potom mogu uputiti Ministarstvu pravosuđa i PCLOB-u ili čak kongresnom odboru koji mogu provesti preporuke. Ako glavni inspektor utvrdi kršenje propisa, ono može biti obrađeno unutarnjim mjerama i mjerama određenima politikama ili prijavljeno Kongresu. Glavni inspektor ima ovlasti, primjerice za izvršavanje revizije i kontrola.

Radna skupina primjećuje da izvješća glavnog inspektora mogu biti uskraćena javnosti i da glavni inspektor može biti spriječen u podnošenju izvješća ako je informacija koja je predmet nadzora tajna. Ipak, izvješća će u svakom trenutku podlijegati nadzoru Kongresa, što je bitna mjera zaštite čak i ako ne pruža osnovu za pojedinačnu primjenu pravnih lijekova.

Sve agencije imaju službenike za zaštitu privatnosti i građanske slobode koji pomažu s obveznim sustavom samostalnog izvješćivanja s nadzorom Kongresa.

Sveukupno, uspostavljeni mehanizmi unutarnjeg nadzora mogu se smatrati prilično robusnima; ipak, kako bi se opravdalo uplitanje u temeljna prava na privatnost i zaštitu podataka, nadzor treba biti u potpunosti neovisan. I premda Radna skupina poštuje i cijeni rad različitih službenika za zaštitu privatnosti i građanske slobode, ona ne može zaključiti da oni zadovoljavaju potrebnu razinu neovisnosti kako bi djelovali kao neovisni nadzornici.

3.4.2. Vanjski nadzor

Vanjski nadzor sastoji se od nekoliko različitih mehanizama: pravosudni nadzor na temelju članaka 501. i 702. osigurava sud FISA-e (dalje u tekstu: FISC), nadzor kongresnih užih odbora za obavještajne službe i zadatke koje izvršava PCLOB.

Radna skupina podsjeća da u idealnom slučaju, kako su već naveli Sud EU-a i ESLJP, nadzor treba biti u rukama suca kako bi se zajamčile neovisnost i nepristranost postupaka. Donedavno je FISC postupak bio *ex parte* postupak bez mogućnosti saslušanja predmetnih pojedinaca ili čak bez da oni budu svjesni predmeta. Danas je FISC postupak i dalje *ex parte,* no nakon donošenja Zakona o slobodi SAD-a, uvedeni su *amici curiae* za FISC. *Amici curiae* djeluju neovisno, no nisu ustrojeni radi obrane određenih pojedinaca koji bi mogli biti uključeni u predmet.

Zakon o slobodi SAD-a stvorio je skupinu *amici curiae* za savjetovanje FISC-a o važnim predmetima. Sud je odabrao pet pravnika koji su pribavili odgovarajuća sigurnosna odobrenja i koji pružaju tehničke savjete, prisustvuju raspravama FISC-a, daju informacije i vode

raspravu o meritumu predmeta s gledišta privatnosti i građanskih prava. Ipak, oni to čine samo u važnim predmetima ili kada se pojave nova pravna pitanja.[53]

Članak 215. gotovo u potpunosti podliježe *ex ante* (ali ne ex post) pravosudnom nadzoru jer svi programi koji se koriste člankom 215. kao temeljem za prikupljanje podliježu odobrenju FISC-a. Izvješće PCLOB-a navodi da se „članak 702. razlikuje od ovog tradicionalnog okvira elektroničkog nadzora FISA-e u pogledu primijenjenih standarda i u pogledu nedostatka individualiziranih FISC-ovih odluka. Prema tom zakonu, glavni državni odvjetnik i direktor nacionalne obavještajne službe jednom godišnje daju potvrde kojima se ovlašćuje ciljanje osoba koje nisu državljani SAD-a za koje se razumno vjeruje da se nalaze izvan Sjedinjenih Američkih Država radi pribavljanja stranih obavještajnih podataka bez navođenja FISC-u određenih osoba koje nisu državljani SAD-a koje će biti ciljane. […] Također ne postoji zahtjev da vlada prikaže vjerojatni uzrok vjerovanja da je meta članka 702. strana sila ili predstavnik strane sile kako to zahtijeva tradicionalna FISA."[54]

Unutar Kongresa, uži odbori za obavještajne službe također imaju zadatak nadzora u pogledu odobravanja obavještajnih aktivnosti, posebno izglasavanjem proračuna. Odbori za obavještajne službe Senata i predstavničkog doma dobivaju tajna izvješća o obavještajnim aktivnostima. Glavni državni odvjetnik mora podnijeti izvješće tim odborima svakih šest mjeseci o prikupljanju informacija elektroničkim izviđanjem u vezi s FISA-om. Radnoj skupini ostaje nejasno u kojoj su mjeri sposobni raspravljati o obradi osobnih podataka pojedinačnih osoba, posebno osoba koje nisu državljani SAD-a.

PCLOB je neovisan dio izvršne grane vlade SAD-a kojoj su povjerena dva temeljna ovlaštenja: (1) pregledavanje i analiziranje aktivnosti koje poduzima izvršna grana vlasti radi zaštite [SAD-a] od terorizma, osiguravajući da je potreba za takvim aktivnostima u ravnoteži s potrebom zaštite privatnosti i građanskih sloboda i (2) osiguravanje da se pitanja sloboda razmatraju na odgovarajući način pri razvijanju i provedbi zakona, propisa i politika povezanih s naporima za zaštitu nacije od terorizma. Radna skupina primjećuje da PCLOB ima ovlasti izdavanja sudskih naloga i pristupa tajnim informacijama. Dok izvršava svoj zadatak, također provjerava učinkovitost programa. Njegov se nadzor ne izvršava prije, već nakon događaja. PCLOB je demonstrirao svoje neovisne ovlasti izrazivši neslaganje s Predsjednikom Sjedinjenih Američkih Država oko pravnih pitanja. Posebice, utvrdio je da članak 215. programa telefonskih metapodataka nema zakonito ovlaštenje i zaključio da nije učinkovit jer nije bilo dokaza o ometanju napada. PCLOB je također izvršio cjelogodišnju provjeru programa 702 i utvrdio da je zakonit, jasno dopušten zakonom i da je dokazano da je članak 702. vrlo učinkovit, čak i u pitanjima terorizma. Konačno, djelovao je u pogledu zahtjeva transparentnosti i utvrdio kako nekoliko činjenica s oznakom tajnosti nije trebalo imati takvu oznaku. Protumačeno je da će PCLOB u bliskoj budućnosti izvješćivati o provedbi Predsjedničkog ukaza br. 28. U tom pogledu, on smatra da za zadržavanje informacija o strancu činjenica kako je ta osoba stranac nije dovoljna.

[53] Zakon o slobodi GLAVA IV. -- REFORME SUDA ZA NADZOR STRANIH OBAVJEŠTAJNIH PODATAKA, članak 401. Imenovanje *amici curiae*
[54] Izvješće PCLOB-a o programu nadzora na temelju članka 702. FISA-e, str. 24. i 25.

Radna skupina konačno primjećuje da Izvršni nalog br. 12333 ne određuje nikakav pravosudni pregled, nadzor ili mehanizme pravne zaštite za programe nadzora provođene na osnovi njega.

3.4.3. Zaključak

Nacrt odluke o primjerenosti pokazuje kako je višeslojni pristup mehanizama unutarnjeg i vanjskog nadzora uspostavljen u SAD-u. Premda funkcioniranje mehanizama nadzora može biti zbunjujuće, Radna skupina se uvjerila kako su, općenito uzevši, uspostavljeni dovoljni mehanizmi unutarnjeg nadzora. Ipak, Radna skupina zabrinuta je da ne postoji dovoljan nadzor nad programima nadzora poduzetima na temelju Izvršnog naloga br. 12333.

Radna skupina primjećuje da je na njezinu prijašnju kritiku kako postupci pred FISC-om nisu kontradiktorni odgovoreno samo u određenoj mjeri uvođenjem *amici curiae* koji imaju zadatak „promicati zaštitu privatnosti pojedinaca i građanske slobode". Ipak, FISC ne pruža učinkovit pravosudni nadzor usmjeravanja aktivnosti protiv osoba koje nisu državljani SAD-a. Ostaju i neke sumnje u pogledu sposobnosti FISC-a da učinkovito ocjenjuje usmjeravanje aktivnosti i postupke minimalizacije, kako je naveo i PCLOB[55].

3.5. Jamstvo D – Učinkoviti pravni lijekovi trebaju biti dostupni pojedincima

3.5.1. Pravosudni lijekovi

3.5.1.1. Uvjet aktivne legitimacije

Sustav SAD-a koji se odnosi na pravosudne lijekove sadržava važno ograničenje: Ustav SAD-a zahtijeva da osoba dokaže da ima aktivnu legitimaciju: „uvjet da su tužitelji pretrpjeli ili će pretrpjeti izravnu štetu i da se ta šteta može otkloniti pravnom zaštitom. Na federalnoj razini, nije moguće pokrenuti pravne postupke tek na osnovi toga što je pojedinac ili skupina nezadovoljna postupkom vlade ili zakonom."[56] Čini se da je takav uvjet poništen izostankom obavijesti pojedincima koji su podvrgnuti nadzoru čak i nakon što su takve mjere okončane. Sud EU-a i ESLJP opetovano su naveli kako pojedinci moraju imati mogućnost pristupa upravnoj ili pravnoj zaštiti. ESLJP je u svojoj odluci u predmetu Zakharov potvrdio da, na temelju sudske prakse, svatko može otići na sud ako ima legitiman razlog sumnjati na uplitanje u svoja temeljna prava.[57]

Štoviše, strancima koji se nalaze izvan SAD-a nije ponuđena puna ustavna zaštita u SAD-u u skladu s praksom Vrhovnog suda Sjedinjenih Američkih Država[58]. To posebice vrijedi u pogledu četvrtog amandmana koji štiti državljane SAD-a – ali ne osobe koje nisu državljani SAD-a – od nerazumnih pretraga i zapljena, od kojega je izveden velik dio prava na

[55] Izvješće PCLOB-a o programu nadzora na temelju članka 702. FISA-e, str. 11.
[56] https://www.law.cornell.edu/wex/standing; https://www.law.cornell.edu/wex/standinghttps://www.law.cornell.edu/wex/standing; Clapper v. Amnesty International USA
[57] ESLJP, Zakharov, t. 171.
[58] SAD protiv Verdugo – Urquidez, str. 264.–266.

privatnost u SAD-u. Europski građani i druge osobe iz Europe koje žive izvan SAD-a jednostavno su isključeni iz zaštite četvrtog amandmana.[59]

Ograničena primjena Zakona o pravnoj zaštiti (u pogledu materije jer se njime isključuje nacionalna sigurnost i u odnosu na osobe koje se mogu pozvati na njega), brojna izuzeća i pravna nesigurnost u pogledu agencija na koje se Zakon o pravoj zaštiti primjenjuje ne zadovoljavaju uvjet ponude učinkovitog mehanizma pravne zaštite svih pojedinaca na koje se odnosi nadzor obavještajnih aktivnosti u predmetima nacionalne sigurnosti.

3.5.1.2. Predsjednički ukaz br. 28.

Radna skupina primjećuje da je Predsjednički ukaz br. 28. samo direktiva i stoga ne može stvoriti ikakva prava za pojedince. To se može postići samo zakonodavstvom. Stoga se osobe ne mogu obratiti sudu na temelju navodnog kršenja mjera zaštite iz Predsjedničkog ukaza br. 28.

3.5.1.3. Zakon o nadzoru stranih obavještajnih službi

Temeljem FISA-e, postoje određeni pravni lijekovi za pojedince u slučajevima nezakonitog nadzora. Prema FISA-i, „osoba čija su prava prekršena, osim strane sile odnosno predstavnika strane sile […], koja je podvrgnuta elektroničkom nadzoru ili na koju se odnose informacije pribavljene elektroničkim nadzorom objavljene suprotno odredbama članka 1809. ove glave, imaju pravo podnijeti tužbu protiv svake osobe koja je počinila takvo kršenje." To ipak izrijekom isključuje stranu silu ili predstavnika strane sile podvrgnute toj mjeri. Ipak, kako je već rečeno, tužitelj mora dokazati da ima aktivnu legitimaciju, što nije moguće u praksi.

Zakon o slobodi SAD-a stvorio je *Amicus Curiae* savjetodavni odbor sudu FISA-e radi davanja (neobveznih) savjeta u slučaju važnih novih pravnih tumačenja. Njihov je zadatak dati nepristran savjet i ne braniti interese određenog pojedinca na njegov/njezin zahtjev.

3.5.2. Upravni lijekovi

3.5.2.1. Glavni inspektori

Drugi način upotrebe lijekova jest obratiti se glavnom inspektoru kojemu se može podnijeti pritužba. Ipak, glavni inspektori nemaju nikakvu obvezu razmotriti svaku pritužbu: nema prava na saslušanje, već je riječ o diskrecijskoj ovlasti. Glavni inspektor također može izdati izvješća s otkrivenim kršenjima u slučajevima gdje informacije nisu tajne. Kada bi pojedinac mogao pretpostaviti da se izvješće odnosi na njega, on bi se tada mogao obratiti sudu na temelju utvrđenog kršenja zakona.

3.5.2.2. Zakon o pravu na pristup informacijama

Pravni lijek dostupan svim osobama je podnošenje zahtjeva za slobodni pristup informacijama na temelju Zakona o pravu na pristup informacijama (FOIA). Prema vladi

[59] Izvješće europskih supredsjedatelja, točka 2.

SAD-a, zahtjev na temelju FOIA-e može podnijeti općenito bilo tko – bez obzira na to je li državljanin SAD-a – jednostavno zatraživši bilo koji zapis neke agencije. To uključuje zapise o tom pojedincu, iako je u takvom slučaju potrebno pribaviti potvrdu identiteta. Ipak, ako je informacija tajna radi zaštite nacionalne sigurnosti, malo je vjerojatno da će zahtjev na temelju FOIA-e biti uspješan jer se primjenjuje izuzeće: agencije nisu obvezne osigurati pristup informacijama koje su tajne, čak i ako se te informacije odnose na pojedinca koji je postavio zahtjev. Informacije iz kaznenih progona u tijeku u potpunosti su isključene iz zahtjeva na temelju FOIA-e. Konačno, Radna skupina shvaća da zahtjev na temelju FOIA-e ne osigurava pravo da neovisno tijelo provjeri zakonitost obrade.

3.5.3. Pravobranitelj za sustav zaštite privatnosti

3.5.3.1. Uspostava Pravobranitelja

Sustav zaštite privatnosti uspostavlja novi mehanizam za „pojedince iz EU-a" za podnošenje zahtjeva u pogledu „SAD-ova elektroničkog izviđanja " novostvorenom Pravobranitelju za sustav zaštite privatnosti. Funkciju Pravobranitelja, kako je objašnjena u memorandumu priloženom dopisu Državnog tajnika Johna Kerryja od 22. veljače 2016., izvršavat će zamjenica tajnika C. Novelli. Bit će na toj funkciji uz njezinu ulogu „višeg koordinatora međunarodne diplomacije u području informacijske tehnologije", ulogu stvorenu člankom 4(d) Predsjedničkog ukaza br. 28. U dopisu i memorandumu je naglašeno da je „zamjenica tajnika izravno odgovorna Državnom tajniku i neovisna o obavještajnoj zajednici".

Unatoč njegovu imenu, u memorandumu se objašnjava da će Pravobranitelj za sustav zaštite privatnosti obrađivati ne samo zahtjeve koji se odnose na pristup podacima koji se prenose iz EU-a u SAD na temelju sustava zaštite privatnosti u okviru nacionalne sigurnosti, već i one predmete gdje su podaci preneseni na temelju standardnih ugovornih odredbi, obvezujućih korporativnih pravila, odstupanja (na temelju članka 26. Direktive 95/46/EZ) ili „mogućih budućih odstupanja", definiranih u bilješci 2 uz memorandum.

Način na koji bi taj mehanizam trebao djelovati može se sažeti na sljedeći način: Pojedinac iz EU-a podnosi zahtjev tijelu države članice nadležnom za nadzor službi nacionalne sigurnosti ili centraliziranom „tijelu EU-a za rješavanje pojedinačnih pritužbi", ako se potonje stvori ili imenuje. Tijelo koje prosljeđuje zahtjev Pravobranitelju morat će prvo provjeriti je li zahtjev potpun, kako je definirano točkom 3(b) dopisa.[60] Kada se proslijedi Pravobranitelju za sustav zaštite privatnosti i kada se utvrdi sukladnost s točkom 3(b), Pravobranitelj za sustav zaštite

[60] b. Tijelo EU-a za rješavanje pojedinačnih pritužbi osigurat će, u skladu sa sljedećim aktivnostima, da je zahtjev potpun:
i. provjeravanjem identiteta pojedinca i da taj pojedinac djeluje u vlastito ime, a ne kao predstavnik vladine ili međuvladine organizacije;
ii. osiguravajući da je zahtjev načinjen u pismenom obliku i da sadržava sljedeće osnovne informacije:
• sve informacije koje čine osnovu zahtjeva,
• prirodu traženih informacija ili zaštite,
• tijela vlasti Sjedinjenih Američkih Država za koje se vjeruje da su uključena, ako ih ima, i
• druge mjere koje se poduzimaju radi pribavljanja zatraženih informacija ili zaštite i odgovor primljen tim drugim mjerama;
iii. potvrđujući da se zahtjev odnosi na podatke za koje se razumno vjeruje da su preneseni iz EU-a u Sjedinjene Američke Države na temelju sustava zaštite privatnosti, standardnih ugovornih odredbi (SCC), obvezujućih korporativnih pravila (BCR), odstupanja ili mogućih budućih odstupanja;
iv. izradivši početnu ocjenu da zahtjev nije neozbiljan, neugodan ili podnesen u lošoj vjeri.

privatnosti dat će odgovor, što znači da će konačno potvrditi da je „(i) prigovor istražen na ispravan način i (ii) da se postupilo u skladu s pravom, zakonima, izvršnim nalozima, predsjedničkim ukazima i politikama agencija SAD-a kojima se pružaju ograničenja i mjere zaštite opisane u dopisu Ureda direktora nacionalne obavještajne službe (ODNI) ili, u slučaju neusklađenosti, da je takva neusklađenost otklonjena."[61] Odgovorom se „neće potvrditi ili zanijekati da je nadzor bio usmjeren na tog pojedinca niti će Pravobranitelj za sustav zaštite privatnosti potvrditi da je primijenjen određeni pravni lijek".[62] U pogledu pitanja kako se izvršava Pravobraniteljeva istraga, objašnjeno je da će Pravobranitelj za sustav zaštite privatnosti „blisko surađivati s drugim službenicima Sjedinjenih Američkih Država, uključujući odgovarajuća neovisna nadzorna tijela"[63] i, točnije, da će „biti u mogućnosti blisko koordinirati aktivnosti s ODNI-jem, ministarstvom pravosuđa i drugim ministarstvima i agencijama uključenima u nacionalnu sigurnost Sjedinjenih Američkih Država, ovisno o tome što je prikladno, te glavnim inspektorima, službenicima iz Zakona o pravu na pristup informacijama i službenicima za zaštitu privatnosti i građanskih sloboda[64]." Ta će koordinacija osiguravati da Pravobranitelj za sustav zaštite privatnosti može poslati odgovor, uključujući prethodno opisane potvrde.

3.5.3.2. Procjena novog mehanizma Pravobranitelja

Radna skupina prepoznaje napore Europske komisije i vlade SAD-a u pogledu uvođenja novog mehanizma s ciljem poboljšanja mogućnosti pravne zaštite u pogledu aktivnosti nadzora SAD-a. Ona shvaća da je procjena ovog mehanizma, kao novosti u međunarodnim odnosima u pogledu informacija prikupljenih elektroničkim izviđanjem ili nacionalne sigurnosti, od posebne važnosti.

U ovom će odjeljku Radna skupina ocijeniti kako se uspostava Pravobranitelja za sustav zaštite privatnosti odnosi na nužne uvjete za pojedince u smislu traženja pravne zaštite u skladu s odredbama Povelje, sudskom praksom ESLJP-a i europskim sudovima.

3.5.3.3. Može li uspostava Pravobranitelja sama po sebi biti dovoljna?

Za početak, treba se zapitati može li se uopće smatrati da je uspostava „pravobranitelja" u skladu s člankom 47. Povelje – koji spominje učinkoviti pravni lijek pred neovisnim sudom[65] – barem ako nema nikakvog drugog načina za pribavljanje učinkovite pravne zaštite. To je važno zato što Sud EU-a u predmetu Schrems, u svojem važnom razmatranju 95., upućuje na članak 47. Povelje, i to bez ikakve naznake da članak 47. treba tumačiti uz preinake u

[61] Sustav zaštite privatnosti, Prilog III., članak 4.e
[62] Sustav zaštite privatnosti, Prilog III., članak 4.e
[63] Sustav zaštite privatnosti, Prilog III., članak 2.a
[64] Sustav zaštite privatnosti, Prilog III., članak 2.a
[65] U objašnjenjima koja se odnose na Povelju o temeljnim pravima, navodi se da članak 47. treba tumačiti na takav način da on daje jamstvo na pravo na učinkovit pravni lijek pred sudom (Objašnjenje koje se odnosi na Povelju o temeljnim pravima, objašnjenje članka 47. (2007/C 303/02)).

kontekstu mjera nadzora. Naprotiv, Sud EU-a je već primijenio članak 47. Povelje u predmetu Kadi II[66] na mjere nadzora u pogledu nacionalne odnosno međunarodne sigurnosti[67].

Sudska praksa ESLJP-a ipak vrlo jasno ističe da pravna zaštita običnih sudova nije uvjet da bi se smatralo kako su sustavi nadzora u skladu s člankom 8. (i člankom 13. EKLJP-a).[68] Umjesto toga, Sud je razvio praksu, na temelju članka 8, kao nužnu mjeru zaštite kod aktivnosti nadzora, prema kojoj zaštita pred drugim tijelima može biti prikladna. ESLJP ipak ima visoka očekivanja od drugih tijela koja pružaju učinkovite pravne lijekove i navodi da takvo tijelo mora biti „neovisno o tijelima koja izvršavaju nadzor i povjerene su mu dovoljne ovlasti za izvršavanje učinkovite neprekinute kontrole"[69].

U predmetima Kennedy i Klass ESLJP je pružio uvid u ono što ta očekivanja mogu značiti u kontekstu tajnog nadzora kada osoba čiji se podaci obrađuju nije obaviještena o obradi njezinih podataka. U obje presude ESLJP je smatrao tijela vlasti neovisnima, posebno neovisnima o tijelima koja izvršavaju nadzor, ali i o uputama[70] svih drugih tijela vlasti. Točnije, u predmetu Kennedy, sud je s odobravanjem prihvatio neovisno i nepristrano tijelo koje je donijelo vlastita pravila i postupke, a sastojalo se od članova koji su tada ili prije bili na visokim pravosudnim funkcijama ili su bili iskusni pravnici[71].

Pri ispitivanju prigovora koje podnose pojedinci, tijela vlasti u obje su presude osim toga imala pristup svim relevantnim informacijama, uključujući materijale kojima se štiti pristup. Naposljetku, u oba slučaja imala su ovlasti ispraviti neusklađenosti.[72]

Uz pitanje može li se Pravobranitelj smatrati „sudom", primjena članka 47. stavka 2. Povelje implicira dodatni izazov jer određuje da taj sud mora biti „osnovan u skladu sa zakonom". Dvojbeno je može li se memorandum kojim se opisuje funkcioniranje novog mehanizma smatrati „zakonom".

Posljedično – imajući na umu načelo bitne ekvivalentnosti – umjesto da ocjenjuje može li se Pravobranitelj formalno smatrati sudom osnovanim u skladu sa zakonom, Radna skupina odlučila je dodatno razmotriti nijanse sudske prakse u pogledu posebnih uvjeta potrebnih kako bi se „pravni lijekovi" i „pravna zaštita" smatrali usklađenima s temeljnim pravima iz članaka 7., 8. i 47. Povelje i članka 8. (i 13.) EKLJP-a. U svojoj daljnjoj analizi, nakon rasprave o području primjene novog mehanizma, Radna skupina stoga će se fokusirati na sljedeće kriterije: uvjet za podnošenje zahtjeva Pravobranitelju i primanje odgovora („aktivna legitimacija"), neovisnost Pravobranitelja, njegove istražne ovlasti u pogledu pristupa

[66] Spojeni predmeti C-584/10 P, C-593/10 P i C-595/10 P, Europska komisija i Ujedinjena Kraljevina protiv Kadi, 18. srpnja 2013.
[67] Kadi II, t. 97. i 100.: svi akti Unije, uključujući one čiji je cilj provedba odluka koje je usvojilo Vijeće sigurnosti na temelju VII. poglavlja Povelje Ujedinjenih naroda, podliježu preispitivanju zakonitosti od strane sudova Europske unije (VII. poglavlje odnosi se na prijetnje miru, narušavanja mira i činove agresije).
[68] Članak 13. EKLJP-a obvezuje države članice da osiguraju da „svatko čija su prava i slobode (…) prekršena ima na raspolaganju učinkovit pravni lijek pred nacionalnim tijelom". To ne mora nužno biti pravosudno tijelo kao što je ESLJP već pojasnio u predmetu Klass, t. 56. i 67.
69 Klass, t. 56. i 67.
[70] ESLJP, Klass, t. 21. i 53.
[71] Komisija G 10 (u vrijeme donošenja presude) sastoji se od triju članova, od kojih predsjednik mora biti kvalificiran za obnašanje pravosudne dužnosti (Klass, t. 21. i 53.)
[72] ESLJP, Kennedy, t. 167.; Klass, t. 21. i 53.

potrebnim materijalima, uključujući tajne dokumente, zahtijevanje pomoći od drugih agencija i, konačno, njegove ovlasti za ispravljanjem nesukladnosti.

3.5.3.4. Područje primjene mehanizma Pravobranitelja

U pogledu pristupa mehanizmu Pravobranitelja, Radna skupina smatra da sve osobe koje podliježu pravu EU-a trebaju biti obuhvaćene zaštitnim mjerama koje se temelje na sustavu zaštite privatnosti. Ne bi bilo prihvatljivo praviti razliku temeljenu na državljanstvu, osobito uzimajući u obzir da se temeljna prava EU-a primjenjuju na sve, a ne samo na one koji posjeduju putovnicu države članice EU-a. Prilog III. odnosi se na „pojedinca iz EU-a" bez dodatnog definiranja tko je to. Radna skupina žali zbog te nesigurnosti i predlaže pružanje pojašnjenja u smislu da sve osobe koje podliježu pravu EU-a imaju pravo da se njihov zahtjev Pravobranitelju obradi u skladu s uvjetima iz memoranduma. Dodatno, Komisija i SAD trebaju obraditi pitanje u kojoj će se mjeri sustav zaštite privatnosti također primjenjivati na građane/stanovnike zemalja EGP-a i Švicarske koje je u prošlosti obuhvaćao mehanizam „sigurne luke".

Nadalje, Radna skupina primjećuje određenu nesigurnost u pogledu područja primjene mehanizma Pravobranitelja. Dok memorandum određuje da je Pravobranitelj zadužen za obradu zahtjeva koji se odnose na nacionalnu sigurnost i podatke prenesene iz EU-a u SAD na temelju svih alata za prijenos koji su dostupni na temelju prava EU-a, jednako je razjašnjeno u memorandumu da se njime opisuje mehanizam „u pogledu informacija prikupljenih elektroničkim izviđanjem". Potonji pojam upućuje na to da su obuhvaćeni samo onakvi prijenosi podataka gdje se podaci prikupljaju pomoću elektroničkog izviđanja, što dovodi do pitanja smatraju li se podaci prikupljeni na temelju FISA-e „informacijama prikupljenima elektroničkim izviđanjem". Čini se da je tako u pogledu članka 702., kako je objašnjeno u izjavi ODNI-ja, str. 10.[73] Ipak, Radna skupina žali što upotreba pojma „elektroničko izviđanje" u ovom kontekstu stvara nepotrebnu nesigurnost.

Kao dodatna posljedica, prema shvaćanju Radne skupine, mehanizam Pravobranitelja ne obuhvaća zahtjeve povezane s pristupom agencija za kazneni progon.[74] Ako je tako, ostaje nejasno bi li zahtjevi koje su uputile agencije, posebno CIA, bili obuhvaćeni tim mehanizmom.

3.5.3.5. „Aktivna legitimacija" i postupak zahtjeva

Vrlo je teško pokrenuti postupak protiv mjera nadzora vlade SAD-a pred redovitim sudovima u Sjedinjenim Američkim Državama. Radna je skupina svjesna da je Vrhovni sud zanijekao aktivnu legitimaciju u slučajevima obavještajnih aktivnosti, gdje podnositelj zahtjeva nije mogao prikazati „konkretnu, određenu i stvarnu ili neposredno prijeteću štetu."[75] U ovom pogledu, uspostava Pravobranitelja važan je korak jer pruža način za određeni oblik pravne zaštite koji inače ne bi postojao. Radna skupina stoga pozdravlja pojašnjenje u točki 3(c). Na

[73] Sustav zaštite privatnosti, Prilog VI., str. 10.
[74] Memorandum o uspostavu Pravobranitelja, str. 1.
[75] Clapper protiv Amnesty International USA, 568 U.S. ___ (2013.) II., str. 10.

temelju te točke, dokaz da je zaista izvršen pristup podacima podnositelja zahtjeva elektroničkim izviđanjem nije potreban kako bi se podnio zahtjev u okviru novog mehanizma.

Radna skupina uvelike podupire postupak za identifikaciju podnositelja prigovora na temelju mehanizma Pravobranitelja. Savršeno je razumno da se identifikacija provodi na području EU-a, kao što je i slučaj kod pristupnog mehanizma na temelju TFTP2 sporazuma između EU-a i SAD-a. Ipak, Radna skupina ne uspijeva shvatiti zašto bi provjeru u EU-u trebala izvršavati „tijela država članica nadležna za nadzor službi nacionalne sigurnosti". Kao prvo, čini se nevjerojatnim da bi na temelju članka 4. stavka 2. Ugovora o Europskoj uniji Europska komisija bila u položaju davati zadatke tim tijelima koja jasno pripadaju području nadležnosti država članica.

Nadalje, s obzirom na raznolikost mehanizama nadzora službi nacionalne sigurnosti u državama članicama, uključenost odgovarajućih tijela može ozbiljno utjecati na učinkovitost sustava za građane u državama članicama. Na primjer, u slučajevima gdje je nekoliko tijela zaduženo za nadzor službi nacionalne sigurnosti, pojedincu može biti teško identificirati onu koja je mjerodavna, gdje primjenjiva nacionalna zakonska pravila ne daju mogućnost pojedincima da stupe u kontakt s relevantnim nadzornim tijelom ili gdje ta tijela nisu uspostavljena na takav način da su podesna za provedbu zadataka koji im se nameću nacrtom odluke o primjerenosti[76]. Uzimajući u obzir uključenost nacionalnih tijela za nadzor zaštite podataka (DPA) u primjenu i nadzor sustava zaštite privatnosti i njihovu sličnu ulogu na temelju TFTP2 sporazuma, čini se razumnijim dodijeliti taj zadatak nacionalnim tijelima za nadzor zaštite podataka država članica. Radna skupina naglašava da smatra malo vjerojatnim da će se tajne informacije obrađivati kao dio postupka pred Pravobraniteljem za sustav zaštite privatnosti jer će svaki odgovor biti isključivo „u skladu je ili nije u skladu, no ispravljeno je."

3.5.3.6. Neovisnost

Izjave Državnog tajnika razjašnjavaju da će funkciju Pravobranitelja izvršavati zamjenica Državnog tajnika. Nju imenuje Predsjednik i imenovanje zahtijeva potvrdu Senata. Uloga Pravobranitelja ne zahtijeva dodatno potvrđivanje; dodjela uloge Pravobranitelja je zadovoljavajuća. Zamjenicu tajnika imenuje Predsjednik SAD-a, Državni tajnik određuje je kao Pravobranitelja, a Senat SAD-a je potvrđuje u ulozi zamjenice tajnika. Kako se u dopisu i izjavama u memorandumu naglašava, Pravobranitelj je „neovisan o obavještajnoj zajednici SAD-a". Radna skupina ipak postavlja pitanja je li Pravobranitelj uspostavljen unutar najprikladnijeg ministarstva. Čini se da je potrebno određeno znanje i razumijevanje načina rada obavještajne zajednice kako bi se učinkovito izvršavala uloga Pravobranitelja, dok je istodobno zaista potrebna dovoljna udaljenost od obavještajne zajednice kako bi se moglo neovisno djelovati.

Sustav zaštite privatnosti ne stvara određene kriterije za razrješenje Pravobranitelja. Stoga je shvaćanje Radne skupine da Pravobranitelj može biti razriješen svoje uloge Pravobranitelja na

[76] Primjerice, u nekim državama članicama EU-a pojedinci informacijama koje su u posjedu nacionalnih sigurnosnih službi mogu pristupiti jedino zahtjevom upućenom sucu visokog suda.

isti način na koji može biti razriješen svoje uloge zamjenika tajnika Ministarstva vanjskih poslova, što potencijalno može potkopati neovisan položaj Pravobranitelja.

Samo po sebi, očigledno je kako je imenovanje zamjenika tajnika Ministarstva vanjskih poslova kao Pravobranitelja različito u pogledu neovisnosti o uspostavi sudske nadležnosti redovitog suda za pravnu zaštitu pojedinca. Stoga je pitanje može li se Pravobranitelj smatrati, u pogledu neovisnosti, jednakim drugim tijelima za nadzor za koja je utvrđeno da su u skladu s odredbama. U kontekstu nadzora, to bi posebice bio Investigatory Powers Tribunal (sud s istražiteljskim ovlastima, IPT) u Ujedinjenoj Kraljevini i komisija G10 u Njemačkoj.

Je li tako, treba dodatno ocijeniti analizom ovlasti koje su dane u smislu „neovisnosti".

3.5.3.7. Istražne ovlasti

U predmetu Kadi II, Sud EU-a je u pogledu članka 47. Povelje odlučio da „predmetna osoba mora biti sposobna ocijeniti razloge ne temelju kojih je donesena odluka u pogledu nje, bilo razmatranjem same odluke ili podnošenjem zahtjeva i pribavljanjem objave tih razloga, ne dovodeći u pitanje ovlasti nadležnog suda da zatraži od predmetnog tijela da objavi te informacije kako bi joj omogućio da brani svoja prava u najboljim mogućim uvjetima."[77] Sudovi Europske unije trebaju osigurati da se ta odluka donese na dovoljno čvrstoj činjeničnoj osnovi[78]. Jasno navodi da „tajnost ili povjerljivost […] informacija ili dokaza nije valjan prigovor", barem ne pred sudovima Europske unije[79]. Stoga Radna skupina zaključuje kako Pravobranitelju moraju biti dane informacije i dokazi koji podupiru dokaze na koje se oslanja za potrebe provedbe mjere – kako bi se zadovoljilo uvjete Suda EU-a[80].

Još je uvijek nejasno kakav bi bio opseg istražnih ovlasti Pravobranitelja. Nacrt odluke Komisije i Prilog III. Ministarstva vanjskih poslova nisu posve jasni u ovom pogledu. U onoj mjeri u kojoj to Radna skupina razumije, Pravobranitelj bi trebao dobiti dovoljno informacija kako bi mogao dati izjavu odvija li se postupak obrade podataka koji provode sigurnosne službe u skladu sa zakonom i, ako nije tako, osigurati ispravljanje okolnosti koje nisu u skladu s njime. Dopis Ministarstva vanjskih poslova i nacrt odluke Komisije ipak ne navode da bi Pravobranitelj imao izravan pristup podacima o predmetnom pojedincu kako bi mogao provesti vlastitu istragu ili se može isključivo osloniti na izvješća drugih službenika vlade SAD-a.

3.5.3.8. Ovlasti za zaštitu prava

Iz memoranduma je i dalje prilično nejasno na koji način Pravobranitelj može narediti ispravljanje neusklađenosti s propisima. U kombinaciji s nedostatkom jasnoće u pogledu istražnih ovlasti, nadalje ostaje nejasno u kojem će opsegu Pravobranitelj kao takav biti stvarno sposoban narediti ispravljanje neusklađenosti s propisima i kakav bi bio rezultat

[77] Kadi II, t. 100.
78 Kadi II, t. 119.
79 Kadi II, t. 125.
[80] Kadi II, t. 122. premda predmetno tijelo ne mora dati sve informacije i dokaze na kojima se temelje razlozi za neku mjeru.

takvog postupka. Bi li to moglo značiti da se podaci prikupljeni na neusklađen način (tj. nezakonito) više ne mogu upotrebljavati ni u kakvom postupku i da ih treba obrisati?

Nadalje, shvaćanje je Radne skupine da sustav zaštite privatnosti ne pruža nikakvu mogućnost žalbe protiv ili revizije „odluke" Pravobranitelja.

Konačno, u pogledu komunikacija Pravobranitelja prema podnositelju pritužbe nakon što se prigovor ispita, Pravobranitelj ne smije otkriti je li bilo nezakonitog postupka -obavještajne zajednice. Pruženi odgovor uvijek će biti jednak i neće biti određen. U predmetu Kadi II, Sud EU-a je odlučio da je nadležno tijelo (nadzorno tijelo) obvezno navesti razloge koji uključuju sve okolnosti, iako članak 296. UFEU-a ne zahtijeva detaljan odgovor[81].

3.5.4. Zaključak

Postojanje učinkovitih pravnih lijekova za pojedince ostaje razlog zabrinutosti Radne skupine. Prije svega, nacrt odluke o primjerenosti ne daje jasan odgovor na pitanje u kojim situacijama i uz koje preduvjete pojedinci mogu pokrenuti postupak radi utvrđivanja njihovih prava.

Radna skupina prepoznaje i pozdravlja uvođenje alternativnog mehanizma pravne zaštite u obliku Pravobranitelja, što je jedinstven događaj u odnosima između EU-a i treće zemlje. Osim potrebe za pojašnjavanjem pojma „pojedinaca iz EU-a" kako je navedeno u prethodnom tekstu, taj mehanizam stvara dodatan način na koji oni mogu tražiti pravnu zaštitu od vlasti SAD-a kako bi osigurali da se osobni podaci podnositelja zahtjeva ne obrađuju u skladu sa zakonima SAD-a.

Istodobno, pri ocjenjivanju mehanizma Pravobranitelja u pogledu standarda neovisnog suda u smislu članka 47. Povelje i uvjeta koje su uspostavili Sud EU-a i ESLJP u svojoj sudskoj praksi u predmetima koji se odnose na nadzor, Radna skupina primjećuje važne nedostatke. Prije svega, postoji zabrinutost u smislu može li se Pravobranitelj smatrati (formalno i u potpunosti) neovisnim, osobito zbog razmjerne jednostavnosti načina na koji se politički imenovane osobe mogu razriješiti dužnosti. Drugo, ostaju razlozi za zabrinutost u pogledu ovlasti Pravobranitelja u smislu izvršavanja učinkovite i neprekidne kontrole. Na temelju dostupnih informacija u Prilogu III., Radna skupina ne može zaključiti da će Pravobranitelj u svakom trenutku imati izravan pristup svim informacijama, spisima i informacijskim sustavima potrebnima za donošenje vlastite procjene ni da može zaista prisiliti nadležne obavještajne agencije da obustave svaku obradu podataka koja nije u skladu s propisima, osobito u slučaju izostanka suglasnosti oko pitanja je li obrada podataka u skladu sa zakonom. Moguće je da dodatna pojašnjenja o položaju i ovlastima Pravobranitelja mogu otkloniti razloge za zabrinutost Radne skupine.

[81] Kadi II, t. 116.

3.6. Zaključna opažanja o zaštitnim mjerama i ograničenjima primjenjivima na tijela nacionalne sigurnosti SAD-a

Radna skupina prije svega pohvaljuje Komisiju i tijela vlasti SAD-a za sve napore koji su učinjeni radi povećanja transparentnosti u pogledu mogućeg učinka programa nadzora SAD-a na podatke prenesene sustavom zaštite privatnosti – ili zapravo bilo kojim drugim alatom za prijenos. Poduzeti su važni koraci od prvih otkrića informacija u slučaju Snowden u lipnju 2013. Ipak, Radna skupina primjećuje kako ostaju razlozi za zabrinutost. U najmanju ruku, potrebna su dodatna objašnjenja i pojašnjenja prava i obveza na temelju sustava zaštite privatnosti.

Dva glavna razloga za zabrinutost Radne skupine su što tijela vlasti SAD-a nisu u potpunosti isključila masovno i neselektivno prikupljanje podataka i što ovlasti i položaj Pravobranitelja nisu detaljnije opisani. Štoviše, za pokretanje postupka pred Pravobraniteljem u ime pojedinca trebaju biti nadležna nacionalna tijela za zaštitu podatka, umjesto tijela za nadzor obavještajnih agencija. Dodatno, iako Radna skupina sigurno prepoznaje pokušaje odgovora na pitanja koja su istaknula tijela za zaštitu podatka, dodatne mjere zaštite kojima bi se osiguralo da svako uplitanje koje mogu prouzročiti programi nadzora SAD-a bude potrebno u demokratskom društvu bile bi dobrodošle.

4. PROCJENA JAMSTAVA SUSTAVA ZAŠTITE PRIVATNOSTI U POGLEDU KAZNENOG PROGONA

4.1. Uvod

U pogledu javnog pristupa osobnim podacima za potrebe kaznenog progona, Radna skupina primjećuje kako načela privatnosti iz Priloga II. sustava zaštite privatnosti sadržavaju odstupanje koje je identično odstupanju koje je opisano u načelima privatnosti „sigurne luke”. Održana je općenita priroda odstupanja, što znači da nova načela sustava zaštite privatnosti omogućavaju uplitanje u temeljna prava osoba čiji se osobni podaci prenose iz EU-a u SAD „utemeljeno na uvjetima nacionalne sigurnosti i javnog interesa ili na domaćem zakonodavstvu Sjedinjenih Američkih Država”.[82]

Jedna od glavnih kritika koju je Sud uputio naspram odluke „sigurna luka” u predmetu Schrems bila je pak da ona „ne sadržava nikakav zaključak u pogledu postojanja, u Sjedinjenim Američkim Državama, pravila koje je usvojila država u smislu ograničavanja svakog uplitanja u temeljna prava osoba čiji se podaci prenose iz Europske unije u Sjedinjene Američke Države.”

Radna skupina stoga pozdravlja napore vlade SAD-a da pruže bolji uvid u pravni okvir koji se odnosi na uplitanje u osobne podatke prenošene sustavom zaštite privatnosti za potrebe kaznenog progona, uključujući primjenjiva ograničenja i mjere zaštite. Istodobno, Radna skupina naglašava da razmatra pitanje javnog pristupa, imajući u vidu da svako uplitanje u temeljna prava na privatan život i zaštitu podataka u demokratskom društvu treba biti

[82] Schrems, t. 87.

opravdano. Radna skupina stoga je analizirala jamstva sustava zaštite privatnosti u pogledu kaznenog progona koristeći se okvirom opisanim točkom 1.2. ovog Mišljenja.

4.2. Primjena europskih ključnih jamstava na pristup tijela kaznenog progona podacima koje čuvaju korporacije

4.2.1. Pristup tijela kaznenog progona osobnim podacima treba biti u skladu sa zakonom i temeljen na jasnim, preciznim i pristupačnim pravilima

Prilog VII. sustava zaštite privatnosti sadržava dopis Ministarstva pravosuđa SAD-a „koje daje kratak pregled primarnih istražnih alata korištenih za pribavljanje poslovnih podataka i drugih informacija iz evidencija od korporacija u Sjedinjenim Američkim Državama za (građanske i regulatorne) potrebe kaznenog progona ili javnog interesa, uključujući ograničenja pristupa opisana kod tih tijela vlasti."

Svi postupci spomenuti u Prilogu VII. potječu izravno iz ustava SAD-a (četvrti amandman), iz zakonskih ili postupovnih propisa ili iz smjernica i politika Ministarstva pravosuđa. Ipak, Prilog VII. ne upućuje izrijekom na sve propise kojima se propisuju ti postupci, već se fokusira na sažeto opisivanje samih postupaka. Prilog VII. također spominje kako „postoje druge pravne osnove po kojima društva mogu osporavati zahtjeve za podacima koje postave upravne agencije na temelju njihovih određenih grana gospodarstva i vrsta podataka koje posjeduju", dajući nekoliko neiscrpnih primjera, kao što su Zakon o bankarskoj tajni, Zakon o pravičnom kreditnom izvješćivanju i Zakon o pravu na financijsku privatnost.

Radna skupina primjećuje kako je okvir propisa, postupaka i politika rascjepkan i da će primjenjiva pravna osnova za određeni zahtjev za pristup ovisiti o prirodi traženih podataka, prirodi društva, prirodi pravnih postupaka (kazneni, upravni, povezan s drugim javnim interesom) i prirodi subjekta koji traži pristup.

Kako se sva primjenjiva pravila za ograničavanje pristupa tijela kaznenog progona podacima prenesenima na temelju sustava zaštite privatnosti temelje na ustavu, zakonima i transparentnim politikama Ministarstva pravosuđa, Radna skupina uzima u obzir presumpciju pristupačnosti tih pravila. Ipak, jasnoća i preciznost pravila mogu se procijeniti samo za svaku pojedinačnu vrstu postupka i zahtjeva za pristupom. Radna skupina stoga žali što mora primijetiti, na temelju dostupnih pojedinosti u Prilogu VII. sustava zaštite privatnosti i zaključaka iz nacrta odluke, da takvu procjenu nije moguće napraviti u ovom trenutku.

4.2.2. Potrebno je pokazati potrebu i razmjernost u pogledu legitimnih ciljeva

Radna skupina primjećuje da se može smatrati da zahtjev za pristup podacima za potrebe kaznenog progona ima legitiman cilj. Primjerice, članak 8. stavak 2. EKLJP-a prihvaća uplitanja javnog tijela vlasti u pravo na zaštitu privatnog života „u interesu (…) javne

sigurnosti, (…) radi sprečavanja nereda ili kaznenih djela." Ipak, takva su uplitanja jedino prihvatljiva kada su potrebna i razmjerna[83].

U skladu s utvrđenom sudskom praksom Suda EU-a, načelo razmjernosti zahtijeva da zakonodavne mjere kojima se predlaže uplitanje u prava na privatni život i zaštitu osobnih podataka „budu prikladne za postizanje legitimnih ciljeva *predmetnog zakonodavstva* i da ne premašuju ograničenja onoga što je prikladno i potrebno kako bi se postiglo te ciljeve"[84] (naše isticanje). Stoga se procjena potrebe i razmjernosti uvijek provodi u odnosu na određenu mjeru predviđenu zakonodavstvom.

Tijela vlasti SAD-a navode u Prilogu VII. kako federalni tužitelji i federalni istražni agenti mogu pribaviti pristup dokumentima i drugim informacijama u evidenciji organizacija preko „nekoliko vrsta obveznih pravnih procesa, uključujući pozive velike porote, upravne naloge i naloge za pretragu" i mogu pribaviti druge komunikacije „u skladu sa saveznim tijelima nadležnim za prikupljanje podataka prislušnim uređajima"[85]. Dodatno, agencije s građanskim i regulatornim ovlastima mogu izdavati sudske pozive organizacijama za „poslovnu evidenciju, elektronički pohranjene podatke ili ostale opipljive stavke[86]." Prilog VII. dodatno određuje da se ti pravni postupci upotrebljavaju općenito kako bi se pribavile informacije od „korporacija" u SAD-u, bez obzira na to jesu li one certificirane u okviru sustava zaštite privatnosti i „bez obzira na državljanstvo osobe čiji se podaci obrađuju". Drugim riječima, čini se kako su subjekti tih zaštita organizacije, a ne sami pojedinci.

Dodatno uz Prilog VII., nacrt odluke – koja se temelji na načelima sustava zaštite privatnosti – sadržava zaključke Komisije u pogledu postojanja pravila u SAD-u kojima se ograničava uplitanje u temeljna prava osoba čiji se podaci prenose iz EU-a u SAD na temelju sustava zaštite privatnosti.

Posebice, zaključci u nacrtu odluke odnose se na primjenjiva ograničenja i mjere zaštite u skladu s četvrtim amandmanom na ustav SAD-a prema kojemu pretrage i zapljene koje su učinila tijela kaznenog progona načelno zahtijevaju sudski nalog izdan na temelju prikazane opravdane sumnje[87]. Zaključci se također odnose na činjenicu da u iznimnim slučajevima, u kojima se uvjet naloga ne primjenjuje, kazneni progon podliježe provjeri razumnosti[88].

Ipak, ti zaključci ne razjašnjavaju na koji se način te mjere zaštite primjenjuju na osobe koje nisu državljani SAD-a. Zapravo, nacrt odluke potvrđuje u uvodnoj napomeni da „zaštita na temelju četvrtog amandmana ne obuhvaća osobe koje nisu državljani SAD-a i koje nemaju prebivalište u Sjedinjenim Američkim Državama"[89]. Osim toga se u istim stavcima nacrta odluke navodi kako osobe koje nisu državljani SAD-a „imaju neizravne pogodnosti preko

[83] Vidjeti radni dokument o europskim ključnim jamstvima, str. 7.–9. Za općenitu procjenu koncepata potrebe i razmjernosti, vidjeti „Mišljenje 01/2014 o primjeni koncepata potrebe i razmjernosti i zaštiti podataka u sektoru kaznenog progona" Radne skupine od 27. veljače 2014.
[84] Digital Rights Ireland, t. 46. i sudska praksa citirana u odluci.
[85] Prilog VII., str. 2.
[86] Prilog VII., str. 4.
[87] Nacrt odluke o primjerenosti, t. 107.
[88] Sustav zaštite privatnosti, t. 107.
[89] Nacrt odluke o primjerenosti, t. 108.

zaštite osigurane društvima iz SAD-a koje čuvaju osobne podatke i koje su primatelji zahtjeva u pogledu kaznenog progona". Radna skupina ipak sa žaljenjem primjećuje kako ovaj zaključak ni na koji način ne upućuje na neki pravni izvor, bilo na propis ili na sudsku praksu.

Sve u svemu, Radna skupina primjećuje da je sustav istražnih alata korištenih za pribavljanje poslovnih podataka i drugih informacija iz evidencija od korporacija u Sjedinjenim Američkim Državama za potrebe kaznenog progona ili javnog interesa, uključujući ograničenja pristupa i mjere zaštite, složeno okruženje mjera. Na temelju dostupnih informacija, u ovom trenutku nije moguće općenito procijeniti ovaj sustav. Potrebna je posebna procjena u pojedinačnim slučajevima radi istinske procjene potrebe i razmjernosti istražnih mjera kaznenog progona u odnosu na temeljna prava na privatan život i zaštitu podataka.

4.2.3. Treba postojati neovisan mehanizam nadzora

Radna skupina primjećuje da većina postupaka opisanih u Prilogu VII. predmnijeva uključenost odluke suda prije nego što tijela vlasti pribave pristup podacima (npr. sud izdaje nalog za upotrebu uređaja za bilježenje ulaznih i izlaznih poziva, sud izdaje nalog za nadzor na temelju Saveznog zakona o prisluškivanju, nalozi za pretragu – pravilo 41.). Ipak, čini se da neki od njih ne zahtijevaju a priori uključenost suda. Primjerice, građanska i regulatorna tijela „mogu izdavati sudske naloge"[90]. U tim slučajevima postoji mogućnost ex post sudske kontrole razumnosti naloga jer „primatelj sudskog naloga može osporiti provedbu sudskog naloga na sudu"[91].

Na temelju dostupnih informacija, Radna skupina primjećuje da se čini kako je uspostavljen prilično robustan neovisan mehanizam nadzora u pogledu pristupa tijela kaznenog progona podacima koje čuvaju društva u SAD-u.

4.2.4. Pojedincima trebaju biti dostupni učinkoviti pravni lijekovi

Kako je prethodno spomenuto, „Zaštita na temelju četvrtog amandmana ne obuhvaća osobe koje nisu državljani SAD-a i koje nemaju prebivalište u Sjedinjenim Američkim Državama"[92]. To znači da osoba koja nije državljanin SAD-a ne bi mogla osporiti sudske i druge naloge pred sudom pozvavši se na četvrti amandman. Nacrta odluke o primjerenosti određuje kako osobe koje nisu državljani SAD-a imaju neizravne pogodnosti preko zaštite osigurane društvima iz SAD-a koje čuvaju osobne podatke i koje su primatelji zahtjeva u pogledu kaznenog progona. Radna skupina ipak primjećuje da, čak i kad bi ta zaštita bila učinkovita, to ne znači da su učinkoviti pravni lijekovi dostupni pojedincima jer se čini da je u ovom scenariju subjekt prava na učinkoviti pravni lijek društvo koje prima zahtjev za pristup, a ne pojedinac o čijim je podacima riječ.

[90] Prilog VII., str. 4.
[91] Prilog VII., str. 4.
[92] Nacrt odluke o primjerenosti, stavak 108.

Prilog VII. ne sadržava nikakve dodatne informacije u pogledu mogućih pravnih lijekova koji proistječu iz propisa dostupnima osobama koje nisu državljani SAD-a kada tijela vlasti ili društva nezakonito omoguće ili pribave pristup sadržaju njihovih podataka.

Radna skupina pozdravlja činjenicu da nedavno doneseni Zakon o pravnoj zaštiti[93] sadržava odredbe o pravu na pravnu zaštitu za osobe koje nisu državljani SAD-a. Ta su prava, međutim, ograničena na jasno definirane razloge za djelovanje: pravo na pribavljanje ispravka i pristupa podacima i na odvjetničke naknade kada „imenovana federalna agencija ili komponenta" uskrati izmjenu podataka ili uskrati pristup takvim podacima i pravo na pribavljanje građanskih lijekova u slučajevima „namjernog ili svjesnog" objavljivanja podataka.

Dodatno, sudska praksa iz SAD-a spomenuta u bilješkama relevantnih uvodnih napomena nacrta odluke, posebice City of Ontario protiv Quon[94], Maryland protiv King[95] i Samson protiv California[96], nije relevantna za procjenu mogu li osobe koje nisu državljani SAD-a pokrenuti postupak pred sudom kako bi osporile zakonitost uplitanja u njihovu privatnost[97]. Svi predmeti odnose se na pravo na privatan život građana SAD-a i svi sadržavaju odluke Vrhovnog suda SAD-a koje u stvarnosti ograničavaju primjenu četvrtog amandmana.

Sve u svemu, Radna skupina potvrđuje i pozdravlja usvajanje Zakona o pravnoj pomoći, no ostaje dvojbeno jesu li učinkoviti pravni lijekovi stvarno dostupni pojedinačnim osobama čiji se podaci obrađuju.

4.3. Zaključne primjedbe

Radna skupina pozdravlja i prepoznaje napore vlade SAD-a da pruže bolji uvid u pravni okvir koji se odnosi na uplitanje u osobne podatke prenošene sustavom zaštite privatnosti EU-a i SAD-a za potrebe kaznenog progona, uključujući primjenjiva ograničenja i mjere zaštite.

Radna skupina primjećuje da je sustav istražnih alata tijela kaznenog progona, uključujući primjenjiva ograničenja i mjere zaštite, opsežan i složen te da su informacije sadržane u sustavu zaštite privatnosti kratke. Radna skupina stoga žali što nije u mogućnosti, na temelju ograničenih informacija (tj. u Prilogu VII. sustava zaštite privatnosti i zaključaka u nacrtu odluke), dati sveobuhvatnu procjenu u pogledu pristupačnosti, predvidivosti te potrebe i razmjernosti primjenjivih pravila u ovom trenutku. Bez obzira na ostale zaključke Radne

[93] Zakon o pravnoj zaštiti iz 2015., Zast. Dom 1428.
[94] *City of Ontario, Cal. protiv Quon*, 130 S. Ct. 2619, 2630 (2010.).
[95] *Maryland protiv King*, 133 S. Ct. 1958, 1970 (2013.).
[96] *Samson protiv California*, 547 U.S. 843, 848 (2006.).
[97] U predmetu *Ontario protiv Quon* sud je smatrao kako grad Ontario nije prekršio prava svog zaposlenika proistekla iz četvrtog amandmana jer je pristup grada sadržaju privatnih poruka predmetnog zaposlenika bio razuman jer je bio motiviran legitimnim ciljem povezanim s poslom i nije bio pretjeran obujmom. U predmetu *Samson protiv California* sud je utvrdio da „četvrti amandman ne zabranjuje policajcu provedbu pretrage bez sumnje osobe puštene iz zatvora na uvjetnu slobodu". U predmetu *Maryland protiv King* sud je utvrdio da je, kada policajci izvrše uhićenje na osnovi opravdane sumnje kako bi priveli osumnjičenika za teško kazneno djelo i doveli ga u postaju radi zadržavanja u pritvoru, prikupljanje i analiza brisa DNK s obraza uhićenika, poput uzimanja otisaka prstiju ili fotografiranja, legitiman policijski postupak registriranja uhićenika koji je razuman na temelju četvrtog amandmana.

skupine u pogledu sustava zaštite privatnosti u ovom Mišljenju, takva bi procjena mogla biti dio godišnjeg preispitivanja sustava zaštite privatnosti.

Radna skupina primjećuje da se čini kako je uspostavljen prilično robustan neovisan mehanizam nadzora u pogledu pristupa tijela kaznenog progona. Štoviše, Radna skupina pozdravlja donošenje Zakona o pravnoj zaštiti koji daje pravo na pravnu zaštitu osobama koje nisu državljani SAD-a. Ipak, Radna skupina primjećuje kako su ta prava ograničene prirode. Dodatno, uz utvrđivanje da osoba koja nije državljanin SAD-a ne bi mogla osporiti sudske i druge naloge pred sudom pozvavši se na četvrti amandman, ostaju pitanja jesu li učinkoviti pravni lijekovi stvarno dostupni pojedinačnim osobama čiji se podaci obrađuju u području kaznenog progona.

5. ZAKLJUČCI I PREPORUKE

Radna skupina prije svega pozdravlja činjenicu da je u roku od pet mjeseci nakon poništavanja „sigurne luke" predstavljen nacrt nove odluke o primjerenosti koji sadržava brojna poboljšanja u odnosu na prethodni mehanizam. Posebno je zadovoljna povećanom transparentnošću koja se nudi uvođenjem dvaju Popisa organizacija u sustavu zaštite privatnosti na internetskoj stranici Ministarstva trgovine: jedan popis sadržava zapise onih organizacija koje se pridržavaju sustava zaštite privatnosti, a drugi popis sadržava zapise onih organizacija koje su se pridržavale sustava zaštite privatnosti u prošlosti, no više to ne čine. Pozdravlja se također povećana transparentnost u odnosu na javni pristup podacima prenošenima na temelju sustava zaštite privatnosti za potrebe nacionalne sigurnosti ili kaznenog progona. Konačno, Radna skupina vrlo je zadovoljna saznanjem da će svi prijenosi podataka u SAD od ovog trenutka podlijegati jednakoj zaštiti: nema nikakvih uspostavljenih specifičnih pravnih odredbi kojima bi se dala prednost jednom alatu u odnosu na druge.

5.1. Tri razloga za zabrinutost

Ipak, ostaju tri velika razloga za zabrinutost koje će, prema viđenju Radne skupine, trebati obraditi.

Prvi razlog za zabrinutost je to što jezik upotrijebljen u nacrtu odluke o primjerenosti ne obvezuje organizacije na brisanje podataka ako oni više nisu nužni. To je bitan element zakonodavstva EU-a o zaštiti podataka kojim se osigurava da se podaci ne drže duže nego što je potrebno za ostvarivanje svrhe zbog koje su ti podaci prikupljeni. Drugo, Radna skupina razumije iz Priloga VI. da administracija SAD-a ne isključuje u potpunosti nastavak prikupljanja masovnih i neselektivnih podataka. Radna je skupina dosljedno smatrala da je takvo prikupljanje podataka neopravdano uplitanje u temeljna prava pojedinaca. Treći razlog za zabrinutost odnosi se na uvođenje mehanizma Pravobranitelja. Iako Radna skupina pozdravlja ovaj korak bez presedana kojim se stvara dodatni mehanizam pravne zaštite i nadzora za pojedince, ostaju pitanja u pogledu toga ima li Pravobranitelj dovoljne ovlasti za učinkovito funkcioniranje. Kao minimum, potrebno je pojasniti i ovlasti i položaj Pravobranitelja kako bi se dokazalo da je ta funkcija stvarno neovisna i da može ponuditi učinkovit pravni lijek kod obrade podataka koja nije usklađena s propisima.

5.2. Preporučena pojašnjenja

Uz navedena pitanja, Radna skupina naznačila je razna pitanja u ovom Mišljenju gdje je potrebno dodatno pojašnjenje odluke o primjerenosti. Još važnije, to se odnosi na potrebu osiguravanja da se ključni pojmovi zaštite podataka korišteni u sustavu zaštite privatnosti definiraju i primjenjuju na dosljedan način. To trenutačno nije tako. Poželjno bi bilo uvođenje pojmovnika u često postavljana pitanja o sustavu zaštite privatnosti, s definicijama o kojima bi u idealnom slučaju bio postignut dogovor između EU-a i SAD-a. Radna skupina također zaključuje kako daljnji prijenosi osobnih podataka iz EU-a nisu dovoljno ograničeni, osobito u pogledu njihova opsega, ograničenja njihove svrhe i jamstava koja se odnose na prijenose agentima. U pogledu pristupa tijela kaznenog progona podacima sustava zaštite privatnosti, posebno u pogledu predvidivosti zakonodavstva, razlog za zabrinutost postoji zbog opsežne i složene prirode sustava kaznenog progona u SAD-u, kako na federalnoj razini tako i na razini države, kao i ograničenih informacija uključenih u odluku o primjerenosti.

Sustav zaštite privatnosti prva je odluka o primjerenosti koja je izrađena nakon što je postignut načelni sporazum o Općoj uredbi o zaštiti podataka. Ipak, brojna poboljšanja na razini zaštite podataka koja se nude pojedincima nisu odražena u sustavu zaštite privatnosti. Radna skupina stoga preporučuje da se preispitivanje ove odluke o primjerenosti i odluka o primjerenosti izdanih za ostale treće zemlje održi ubrzo nakon što Opća uredba o zaštiti podataka stupi na snagu.

Završna preporuka Radne skupine koja se ovdje ističe tiče se zajedničkog preispitivanja. Radna skupina pozdravlja činjenicu da će odluka o primjerenosti sustava zaštite privatnosti zaista biti preispitivana jednom godišnje uz široko sudjelovanje tijela za zaštitu podataka i drugih relevantnih stranaka. Ona bi pozdravila sporazum o elementima zajedničkih preispitivanja te o izradi i predstavljanju izvješća o preispitivanju od strane svih stranaka dovoljno prije prvog preispitivanja.