EVROPSKA
KOMISIJA

Bruselj, 27.11.2013
COM(2013) 847 final

SPOROČILO KOMISIJE EVROPSKEMU PARLAMENTU IN SVETU

o delovanju varnega pristana z vidika državljanov EU in družb, ustanovljenih v EU

SPOROČILO KOMISIJE EVROPSKEMU PARLAMENTU IN SVETU

o delovanju varnega pristana z vidika državljanov EU in družb, ustanovljenih v EU

1. UVOD

Direktiva 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (v nadaljnjem besedilu: direktiva o varstvu podatkov) določa pravila za prenos osebnih podatkov iz držav članic EU v druge države zunaj EU[1], kolikor takšen prenos spada na področje uporabe tega instrumenta[2].

Komisija lahko v skladu z direktivo o varstvu podatkov ugotovi, da tretja država zagotavlja ustrezno raven varstva zaradi svoje nacionalne zakonodaje ali mednarodnih obveznosti, ki jih je prevzela za zaščito pravice posameznikov, v primeru katerih se posebne omejitve prenosa podatkov v takšno državo ne bi uporabljale. Ti sklepi se na splošno imenujejo „**sklepi o ustreznosti varstva**".

Komisija je 26. julija 2000 sprejela Odločbo 2000/520/ES[3] (v nadaljnjem besedilu: **odločba o varnem pristanu**), ki priznava načela zasebnosti varnega pristana (v nadaljnjem besedilu: načela), ki zagotavljajo ustrezno varstvo za prenos osebnih podatkov iz EU, in najpogosteje zastavljena vprašanja („Frequently Asked Questions", v nadaljnjem besedilu: FAQ), ki jih je izdalo ministrstvo za trgovino Združenih držav. Odločba o varnem pristanu je bila sprejeta po izdanem mnenju delovne skupine iz člena 29 in mnenju odbora iz člena 31, ki sta bili sprejeti s kvalificirano večino držav članic. V skladu s Sklepom Sveta 1999/468 je bila odločba o varnem pristanu predložena Evropskemu parlamentu v predhodni pregled.

Tako zdajšnja odločba o varnem pristanu omogoča prost prenos[4] osebnih podatkov iz držav članic EU[5] družbam v ZDA, ki so se zavezale k načelom v okoliščinah, ko prenos glede na znatne razlike v ureditvah varstva zasebnosti med EU in ZDA ne bi izpolnjeval standardov EU za ustrezno raven varstva podatkov.

Delovanje zdajšnje ureditve varnega pristana temelji na zavezah in samocertificiranju družb, ki so se zavezale k načelom varnega pristana. Uporaba teh ureditev je prostovoljna, vendar so pravila za tiste, ki se k njim zavežejo, zavezujoča. Temeljna načela te ureditve so:

a) preglednost politik družb, zavezanih k načelom varnega pristana, glede varovanja zasebnosti,

---

1 Člena 25 in 26 direktive o varstvu podatkov določata pravni okvir za prenos osebnih podatkov iz EU v tretje države zunaj EGP.

2 Dodatna pravila določa člen 13 Okvirnega sklepa 2008/977/PNZ z dne 27. novembra 2008 o varstvu osebnih podatkov, ki se obdelujejo v okviru policijskega in pravosodnega sodelovanja v kazenskih zadevah, kolikor tak prenos zadeva osebne podatke, ki se posredujejo drugi državi članici ali se do njih omogoči dostop ene države članice drugi državi članici, ki namerava te podatke pozneje prenesti tretji državi ali mednarodnemu organu za namene preprečevanja, preiskovanja, odkrivanja in pregona kaznivih dejanj ali izvrševanja kazni.

3 Odločba Komisije 2000/520/ES z dne 26. julija 2000 po Direktivi Evropskega parlamenta in Sveta 95/46/ES o primernosti zaščite, ki jo zagotavljajo načela zasebnosti varnega pristana in s tem povezana najpogosteje zastavljena vprašanja, ki jih je izdalo Ministrstvo za trgovino ZDA, UL L 215, 28.8.2000, str. 7.

4 Zgoraj navedeno ne izključuje uporabe drugih zahtev glede obdelave osebnih podatkov, ki jih morda predvideva nacionalna zakonodaja, ki prenaša direktivo EU o varstvu podatkov.

5 Podobno velja za prenos osebnih podatkov iz treh držav pogodbenic Sporazuma EGP po razširitvi Direktive 95/46/ES na Sporazum EGP, Sklep št. 83/1999 z dne 25. junija 1999, UL L 296, 23.11.2000, str. 41.

b) vključitev načel varnega pristana v politike družb glede varovanja zasebnosti in

c) izvrševanje, tudi s strani javnih organov.

To temeljno podlago varnega pristana je treba proučiti v **novem kontekstu**:

a) eksponentnega povečanja prenosa podatkov, ki je bil nekdaj zgolj v pomoč, danes pa je ključnega pomena za hitro rast digitalnega gospodarstva, ter znatnega razvoja zbiranja, obdelave in uporabe podatkov,

b) odločilnega pomena prenosa podatkov, zlasti za čezatlantsko gospodarstvo[6],

c) hitrega povečanja števila družb v ZDA, ki so se zavezale k shemi varnega pristana, pri čemer se je njihovo število od leta 2004 povečalo za osemkrat (s 400 leta 2004 na 3 246 leta 2013),

d) nedavno objavljenih informacij o programih nadzora v ZDA, ki sprožajo nova vprašanja o ravni zaščite, ki naj bi jo zagotovila ureditev varnega pristana.

Glede na navedena dejstva to sporočilo obravnava delovanje sheme varnega pristana. **Temelji na dokazih,** ki jih je zbrala Komisija, delu kontaktne skupine EU-ZDA o varstvu zasebnosti v letu 2009, študiji, ki jo je izdelal neodvisni pogodbenik leta 2008[7], in informacijah, pridobljenih v posebej ustanovljeni delovni skupini EU-ZDA (v nadaljnjem besedilu: delovna skupina), ki je bila ustanovljena po ugotovitvah o ameriških programih nadzora *(glej vzporedni dokument)*. To sporočilo temelji na dveh **ocenjevalnih poročilih Komisije**, pripravljenih v začetnem obdobju ureditve varnega pristana, in sicer iz leta 2002[8] in iz leta 2004[9].

2. STRUKTURA IN DELOVANJE VARNEGA PRISTANA

2.1. Struktura varnega pristana

Ameriška družba, ki se želi zavezati k načelom varnega pristana, mora: (a) v svoji javno dostopni politiki varovanja zasebnosti navesti, da je zavezana k načelom in dejansko ravna v skladu z njimi, ter (b) samocertificirati svojo zavezanost k načelom, tj. sporočiti ministrstvu za trgovino ZDA, da v celoti izpolnjuje načela. Samocertificiranje je treba obnoviti enkrat letno. Načela zasebnosti varnega pristana, navedena v Prilogi I k odločbi o varnem pristanu, zajemajo zahteve o vsebinski zaščiti osebnih podatkov (načela: neokrnjenost podatkov, varnost, možnost izbire in prenos tretjemu) in postopkovne pravice posameznikov, na katere se nanašajo osebni podatki (načela: obvestilo, dostop in izvrševanje).

---

6 Nekatere študije so pokazale, da bi v primeru motenj storitev in čezmejnega prenosa podatkov zaradi nekontinuitete zavezujočih poslovnih pravil, klavzul o vzorčnih pogodbah in varnega pristana, negativni vpliv na BDP Unije lahko dosegel od –0,8 % do –1,3 %, izvoz EU v ZDA pa bi zaradi zmanjšanja konkurenčnosti upadel za –6,7 %. Glej študijo Gospodarski pomen dobre ureditve varstva podatkov („The Economic Importance of Getting Data Protection Right“), ki jo je Evropski center za mednarodno politično ekonomijo („European Centre for International Political Economy“) marca 2013 izdelal za gospodarsko zbornico ZDA.

7 Študija o oceni učinka, ki jo je leta 2008 za Evropsko komisijo izdelal *Centre de Recherche Informatique et Droit* („CRID“) Univerze v Namurju.

8 Delovni dokument služb Komisije „Uporaba Odločbe Komisije 2000/520/ES z dne 26. julija 2000 po Direktivi Evropskega parlamenta in Sveta 95/46/ES o primernosti zaščite, ki jo zagotavljajo načela zasebnosti varnega pristana in s tem povezana najpogosteje zastavljena vprašanja, ki jih je izdalo Ministrstvo za trgovino ZDA“, SEC(2002) 196, 13.12.2002.

9 Delovni dokument služb Komisije „Izvajanje Odločbe Komisije 2000/520/ES o primernosti zaščite, ki jo zagotavljajo načela zasebnosti varnega pristana in s tem povezana najpogosteje zastavljena vprašanja, ki jih je izdalo Ministrstvo za trgovino ZDA“, SEC(2004) 1323, 20.10.2004.

Kar zadeva izvrševanje sheme varnega pristana v ZDA, imata ključno vlogo dve ameriški instituciji, in sicer ministrstvo za trgovino ZDA in zvezna komisija za trgovino ZDA.

Ministrstvo za trgovino pregleda vsako samocertificiranje glede varnega pristana in vsakokratno letno obnovitev samocertificiranja, ki jih predložijo družbe, da se zagotovi vključenost vseh elementov, zahtevanih za članstvo v tej shemi[10]. Posodablja seznam družb, ki so izpolnile samocertifikacijska pisma, ter objavlja seznam in pisma na svojem spletnem mestu. Nadzoruje tudi delovanje varnega pristana in s seznama črta družbe, ki ne izpolnjujejo načel.

Zvezna komisija za trgovino v okviru svojih pristojnosti na področju varstva potrošnikov ukrepa zoper nepoštena in goljufiva dejanja iz oddelka 5 zakona o zvezni komisiji za trgovino. Izvršilni ukrepi zvezne komisije za trgovino vključujejo poizvedbe o lažnih navedbah glede zavezanosti k varnemu pristanu in o neizpolnjevanju teh načel s strani družb, ki so se zavezale k načelom. Za pregon zaradi kršenja načel varnega pristana s strani letalskih prevoznikov je pristojno ministrstvo za promet ZDA[11].

Zdajšnja odločba o varnem pristanu je del zakonodaje EU, ki jo morajo uporabljati organi držav članic. Po tej odločbi smejo nacionalni **organi EU za varstvo podatkov** (DPA) v posebnih primerih začasno ustaviti prenos podatkov družbam, certificiranim v okviru varnega pristana[12]. Komisiji od vzpostavitve varnega pristana leta 2000 niso poznani primeri, ko bi nacionalni organ za varstvo podatkov začasno ustavil prenos podatkov. Nacionalni organi EU za varstvo podatkov imajo ne glede na svoje pristojnosti iz odločbe o varnem pristanu pristojnost ukrepati tudi v primeru mednarodnih prenosov, da se zagotovi skladnost s splošnimi načeli varstva podatkov, določenimi v direktivi o varstvu podatkov iz leta 1995.

Kot je poudarjeno v zdajšnji odločbi o varnem pristanu, je **pristojnost Komisije**, ki ravna v skladu s postopkom pregleda, določenim v Uredbi št. 182/2011, da Odločbo prilagodi, začasno prekine njeno uporabo ali omeji njen obseg glede na njeno preteklo izvajanje. To je predvideno zlasti ob sistematičnih nepravilnostih s strani ZDA, če na primer organ, ki je v Združenih državah pristojen za zagotavljanje izpolnjevanja načel zasebnosti varnega pristana, svojih nalog ne opravlja učinkovito ali če zakonodaja ZDA prevlada nad ravnjo zaščite, ki jo zagotavljajo načela varnega pristana. Kot vsak akt Komisije se lahko tudi ta iz katerih koli drugih razlogov spremeni ali celo razveljavi.

---

10 Če certificiranje ali obnovitev certificiranja družbe ne izpolnjuje zahtev varnega pristana, ministrstvo za trgovino o tem obvesti družbo in še pred končanim certificiranjem družbe od nje zahteva dopolnilne ukrepe (na primer pojasnila, spremembe opisa politik).

11 Pod naslovom 49 oddelka 41712 zakonika Združenih držav.

12 Natančneje, prekinitev prenosa se lahko zahteva v dveh primer, in sicer ko:
(a) vladni organ v ZDA ugotovi, da družba krši načela zasebnosti varnega pristana, ali
(b) obstaja precejšnja verjetnost, da se načela kršijo; obstaja utemeljena podlaga za prepričanje, da zadevni mehanizem uveljavljanja ne sprejema ali ne bo sprejel ustreznih in pravočasnih ukrepov za rešitev spornega primera; bi nadaljnji prenos podatkov povzročil neposredno nevarnost za nastanek velike škode za posameznike, na katere se nanašajo osebni podatki; in so si pristojni organi v državah članicah v danih okoliščinah razumno prizadevali, da bi družbo obvestili in ji dali priložnost za odgovor.

2.2. Delovanje varnega pristana

Med **3 246**[13] **certificiranimi družbami** so tako majhne kot velike družbe[14]. Čeprav sektor finančnih storitev in telekomunikacij ne spada pod izvedbena pooblastila zvezne komisije za trgovino in je zato izključen iz varnega pristana, so med certificiranimi družbami tudi številne družbe industrijskega in storitvenega sektorja, vključno z dobro poznanimi spletnimi podjetji in industrijo, ki zajema tako informacijske in računalniške storitve kot tudi farmacevtske, turistične, zdravstvene storitve ali storitve izdaje kreditnih kartic[15]. To so večinoma ameriške družbe, ki izvajajo storitve na notranjem trgu EU. So pa tudi hčerinske družbe nekaterih podjetij EU, kot sta Nokia ali Bayer. Od teh podjetij jih 51 % obdeluje podatke uslužbencev v Evropi, ki se v ZDA prenašajo iz zaposlitvenih razlogov[16].

Nekateri organi za varstvo podatkov v EU izražajo **vse večjo zaskrbljenost** nad prenosom podatkov v skladu z zdajšnjo shemo varnega pristana. Nekateri organi za varstvo podatkov držav članic kritizirajo celo splošno opredelitev načel ter veliko zanašanje na samocertificiranje in samourejanje. Podobne pomisleke je izrazila industrija, ki je opozorila na izkrivljanje konkurence zaradi nezadostnega izvrševanja.

Zdajšnja ureditev varnega pristana temelji na prostovoljni zavezanosti družb, njihovemu samocertificiranju in izvrševanju zavez samocertificiranja s strani javnih organov. V tem smislu vsakršna nepreglednost in slabo izvrševanje spodkopavata temelje, na katerih je zgrajena shema varnega pristana.

Vsakršno pomanjkanje preglednosti ali izvrševanja na strani ZDA se izraža v preusmeritvi odgovornosti na evropske organe za varstvo podatkov in družbe, ki shemo uporabljajo. Nemški organi za varstvo podatkov so 29. aprila 2010 izdali sklep, ki od družb, ki prenašajo podatke iz Evrope v ZDA, zahteva, da dejavno preverjajo, ali družbe v ZDA, ki uvažajo podatke, izpolnjujejo načela zasebnosti varnega pristana, in jim priporoča, da „naj vsaj družba izvoznica ugotovi, ali je certificiranje varnega pristana pri uvoznikih še veljavno“[17].

Po pridobljenih ugotovitvah o ameriških programih nadzora so nemški organi za varstvo podatkov 24. julija 2013 šli še korak dalje, ko so opozorili, da „obstaja precejšnja verjetnost kršenja načel odločb Komisije“[18]. Obstajajo nekateri primeri organov za varstvo osebnih

---

13 Na dan 26. septembra 2013 je bilo število organizacij, ki so se zavezale k načelom varnega pristana, navedenih pod kategorijo „**aktualni**“ člani na seznamu varnega pristanka **3 246**, pod kategorijo „**neaktualni**“ člani pa **935.**

14 Organizacije varnega pristana z 250 ali manj zaposlenimi: 60 **%** (1 925 od 3 246). Organizacije varnega pristana z 251 ali več zaposlenimi: **40 %** (1 295 od 3 246).

15 Na primer, podjetje MasterCard posluje z več tisoč bankami in je jasen primer, ko varnega pristana ni mogoče nadomestiti z drugimi pravnimi instrumenti za prenos osebnih podatkov, kot so zavezujoča poslovna pravila ali pogodbeni dogovori.

16 Organizacije varnega pristana, ki zajemajo podatke o človeških virih v okviru certificiranja varnega pristana (in so privolile v sodelovanje z organi za varstvo podatkov EU in v skladnost z njihovimi pravili): **51 %** (1 671 od 3 246).

17 Glej sklep Düsseldorfer Kreis z dne 28/29. aprila 2010. Glej: Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 28./29. April 2010 in Hannover: http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/290410_SafeHarbor.pdf?__blob=publicationFile. Vendar je Evropski nadzornik za varstvo podatkov (ENVP) Peter Hustinx 7. oktobra 2013 dal mnenje pred preiskovalnim odborom v okviru Odbora za državljanske svoboščine, pravosodje in notranje zadeve Evropskega parlamenta, in sicer, da so bile v zvezi z varnim pristanom „narejene bistvene izboljšave in je bila večina zadev rešenih“: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2013/13-10-07_Speech_LIBE_PH_EN.pdf.

18 Glej resolucijo nemške konference komisarjev za varstvo podatkov, na kateri je bilo poudarjeno, da pomenijo obveščevalne službe izredno veliko grožnjo izmenjavi podatkov med Nemčijo in državami

podatkov (npr. organ za varstvo osebnih podatkov v Bremnu), ki so od družb, ki prenašajo osebne podatke ameriškim ponudnikom storitev, zahtevali, naj jih obvestijo, ali in kako agenciji za nacionalno varnost preprečujejo dostop do podatkov. Irski organ za varstvo podatkov je poročal, da je nedavno prejel dve pritožbi v zvezi s poročanjem v medijih o programih ameriških obveščevalnih agencij, ki se sklicujeta na program varnega pristana, vendar je zavrnil preiskavo, ker naj bi prenos osebnih podatkov v tretjo državo izpolnjeval zahteve irske zakonodaje o varstvu podatkov. Na podlagi podobne pritožbe je luksemburški organ za varstvo podatkov ugotovil, da sta Microsoft in Skype pri prenosu podatkov v ZDA ravnala v skladu z luksemburškim zakonom o varstvu podatkov[19]. Nasprotno pa je irsko vrhovno sodišče pozneje ugodilo zahtevku za sodno presojo, v okviru katere bo preverilo pravilnost neukrepanja irskega komisarja za varstvo podatkov v zvezi z ameriškimi programi nadzora. Eno od dveh pritožb je vložila študentska skupina Europe v Facebook (EvF), ki je podobno pritožbo vložila tudi zoper Yahoo v Nemčiji, ki pa jo pristojni organi za varstvo podatkov še obdelujejo.

Ti različni odzivi organov za varstvo podatkov na ugotovitve nadzora kažejo na realno tveganje razdrobljenosti sheme varnega pristana in sprožajo vprašanje o obsegu njenega izvrševanja.

3. PREGLEDNOST POLITIK DRUŽB, ZAVEZANIH K NAČELOM VARNEGA PRISTANA, GLEDE VAROVANJA ZASEBNOSTI

Glede na FAQ 6, priložen odločbi o varnem pristanu (Priloga II), morajo družbe, ki želijo certificirati svojo zavezanost k načelom varnega pristana, ministrstvu za trgovino predložiti opis svoje politike varovanja zasebnosti in jo javno objaviti. Vsebovati mora obveznost zavezanosti k načelom varovanja zasebnosti. Zahteva o **javni objavi politik varovanja zasebnosti** samocertificiranih družb in njihova izjava o zavezanosti k načelom varovanja zasebnosti sta ključni za delovanje sheme.

Nezadostna dostopnost do politik varovanja zasebnosti takih družb škodi posameznikom, katerih osebni podatki se zbirajo in obdelujejo, in lahko pomeni **kršitev načela obvestila**. V takih primerih obstaja verjetnost, da posamezniki, katerih podatki se prenašajo iz EU, svojih pravic in obveznosti, ki veljajo za samocertificirane družbe, ne poznajo.

Poleg tega zavezanost družb, da izpolnjujejo načela varovanja zasebnosti, **daje zvezni komisiji za trgovino pristojnost, da izvršuje ta načela** v primeru družb, ki z nepoštenimi ali goljufivimi ravnanji ne izpolnjujejo načel. Zaradi nezadostne preglednosti družb v ZDA je zvezni komisiji za trgovino otežen nadzor in ogrožena učinkovitost izvrševanja.

V preteklih letih veliko samocertificiranih družb svojih politik varovanja zasebnosti ni objavilo in/ali ni dalo javne izjave o zavezanosti k načelom varovanja zasebnosti. Poročilo o varnem pristanu iz leta 2004 je opozorilo, da mora ministrstvo za trgovino **postati dejavnejše pri nadzoru izpolnjevanja** teh zahtev.

Od leta 2004 je ministrstvo za trgovino razvilo **novo informacijsko orodje,** namenjeno pomoči družbam pri izpolnjevanju njihovih obveznosti glede preglednosti. Zadevne informacije o shemi so na voljo na spletnem mestu o varnem pristanu ministrstva za trgovino[20], na katerega lahko družbe tudi naložijo svoje politike varovanja zasebnosti. Ministrstvo za trgovino je poročalo, da družbe uporabljajo to možnost in svoje politike

---

zunaj Evrope: http://www.bfdi.bund.de/EN/Home/homepage_Kurzmeldungen/PMDSK_SafeHarbor.html?nn=408870.

19 Glej izjavo za javnost luksemburškega organa za varstvo podatkov z dne 18. novembra 2013.

20 http://www.export.gov/SafeHarbour/.

varovanja zasebnosti nalagajo na njegovo spletno mesto, ko se prijavljajo za članstvo varnega pristana[21]. Ministrstvo za trgovino je v obdobju 2009–2013 objavilo tudi vrsto smernic za družbe, ki se želijo pridružiti varnemu pristanu, kot sta „Navodila za samocertificiranje“ in „Koristni nasveti o izvajanju samocertificiranja“[22].

Raven izpolnjevanja obveznosti glede preglednosti se med družbami razlikuje. Nekatere družbe opis svoje politike varovanja zasebnosti predložijo zgolj ministrstvu za trgovino kot del postopka samocertificiranja, večina pa svoje politike varovanja zasebnosti objavi na svojih spletnih mestih in jih tudi naloži na spletno mesto ministrstva za trgovino. Vendar te **niso zmeraj predstavljene na potrošniku prijazen in lahko berljiv način**. Hiperpovezave do politik varovanja zasebnosti ne delujejo zmeraj pravilno ali se ne nanašajo zmeraj na pravo spletno stran.

Kot izhaja iz Odločbe in njenih prilog, zahteva, da morajo družbe javno razkriti svoje politike varovanja zasebnosti, **presega samo uradno obveščanje** ministrstva za trgovino o samocertificiranju. Zahteve za certificiranje, določene v FAQ, vključujejo opis politike varovanja zasebnosti in pregledne informacije o tem, kje je na voljo za javni vpogled[23]. Izjave o varovanju zasebnosti morajo biti jasne in lahko dostopne za javnost. Vključevati morajo hiperpovezavo do spletnega mesta o varnem pristanu ministrstva za trgovino, ki vsebuje seznam „aktualnih“ članov sheme in povezavo do ponudnika alternativnega reševanja sporov. Vendar številne družbe, vključene v shemo v obdobju 2000–2013, niso izpolnjevale teh zahtev. Ministrstvo za trgovino je med delovnimi stiki s Komisijo februarja 2013 priznalo, da morda do 10 % certificiranih družb na svojih javnih spletnih mestih dejansko ni objavilo svojih politik varovanja zasebnosti, ki bi vključevale izjavo o zavezanosti k načelom varnega pristana.

Nedavna statistika kaže tudi na nenehne težave v zvezi z **lažnimi trditvami o zavezanosti k načelom varnega pristana**. Približno 10 % družb, ki trdijo, da so članice varnega pristana, na seznamu ministrstva za trgovino niso navedene kot aktualne članice sheme[24]. Takšne lažne trditve dajejo tako družbe, ki nikoli niso bile članice varnega pristana, kot tudi družbe, ki so se v preteklosti pridružile shemi, vendar niso vsako leto obnovile samocertificiranja pri ministrstvu za trgovino. V teh primerih so še vedno vključene na seznam na spletnem mestu o varnem pristanu, vendar je njihov status certificiranja naveden kot „neaktualen“, kar pomeni da je družba bila članica sheme in ima obveznost še naprej zagotavljati varstvo podatkov, ki so že v obdelavi. Zvezna komisija za trgovino je pristojna za ukrepanje v primerih goljufivih ravnanj in neizpolnjevanja načel varnega pristana (glej oddelek 5.1). Nejasnost glede „lažnih trditev“ vpliva na verodostojnost sheme.

Evropska komisija je med rednimi stiki v letih 2012 in 2013 opozorila ministrstvo za trgovino, da za izpolnjevanje obveznosti preglednosti ne zadostuje, da družbe ministrstvu za trgovino zgolj predložijo opis svojih politik varovanja zasebnosti. Izjave o varovanju zasebnosti morajo biti javno dostopne. Ministrstvo za trgovino je tudi pozvala, naj **zaostri redni nadzor spletnih mest družb** po opravljenih postopkih preverjanja, ki se izvede v

---

21 https://SafeHarbour.export.gov/list.aspx.

22 Priročnik je na voljo na spletnem mestu programa: http://export.gov/SafeHarbour/. Koristni nasveti: http://export.gov/SafeHarbour/eu/eg_main_018495.asp.

23 Ministrstvo za trgovino je 12. novembra 2013 potrdilo, da „morajo danes družbe na svojih spletnih mestih, kjer so navedene informacije za potrošnike/stranke/obiskovalce, objaviti politiko varovanja zasebnosti, skladno z načeli varnega pristana“ (dokument: „Sodelovanje med ZDA in EU pri izvajanju okvira varnega pristana“ z dne 12. novembra 2013).

24 Septembra 2013 je avstralsko podjetje za svetovanje Galexia primerjalo „lažne trditve“ o članstvu v letih 2008 in 2013. Njegova glavna ugotovitev je bila, da se je vzporedno s povečanjem članstva varnega pristana med leti 2008 in 2013 (s 1 109 na 3 246) število lažnih trditev povečalo z 206 na 427: http://www.galexia.com/public/about/news/about_news-id225.html.

okviru prvega postopka samocertificiranja ali njegove vsakoletne obnovitve, in naj ukrepa zoper tiste družbe, ki ne izpolnjujejo zahtev glede preglednosti.

Kot prvi odziv na opozorilo EU **je ministrstvo za trgovino marca 2013 uvedlo obveznost,** da morajo družbe, ki so članice varnega pristana in imajo svojo javno spletno mesto, na njem svojim strankam/uporabnikom dati na vpogled svojo politiko varovanja zasebnosti. Hkrati je ministrstvo za trgovino začelo vse družbe, katerih politike varovanja zasebnosti še niso vključevale povezave do spletnega mesta o varnem pristanu ministrstva za trgovino, uradno pozivati, naj dodajo povezavo in tako potrošnikom, ki obiščejo njihovo spletno mesto, omogočijo neposreden dostop do uradnega seznama varnega pristana in njegovega spletnega mesta. To bo evropskim posameznikom, na katere se nanašajo osebni podatki, omogočilo, da takoj in brez dodatnih poizvedb na spletu preverijo zaveze družb, predložene ministrstvu za trgovino. Poleg tega je ministrstvo za trgovino začelo družbe uradno pozivati, naj podatke za stik z njihovim neodvisnim ponudnikom alternativnega reševanja sporov vključijo v svojo objavljeno politiko varovanja zasebnosti[25].

Ta proces je treba pospešiti in tako zagotoviti, da bodo vse certificirane družbe najpozneje do marca 2014 v celoti izpolnjevale zahteve varnega pristana (tj. do roka za obnovitev vsakoletnega certificiranja družbe, šteto od uvedbe novih zahtev marca 2013).

Kljub temu ostajajo dvomi, ali samocertificirane družbe v celoti izpolnjujejo zahteve o preglednosti. Ministrstvo za trgovino mora strožje nadzorovati in preiskovati skladnost z obveznostmi, sprejetimi ob izvedbi začetnega samocertificiranja in vsakoletni obnovitvi.

4. VKLJUČITEV NAČEL ZASEBNOSTI VARNEGA PRISTANA V POLITIKE DRUŽB GLEDE VAROVANJA ZASEBNOSTI

Samocertificirane družbe morajo izpolnjevati načela varovanja zasebnosti, določena v Prilogi I k Odločbi, da bi pridobile in obdržale ugodnosti varnega pristana.

Komisija je v svojem poročilu iz leta 2004 ugotovila, da veliko **družb ni pravilno vključilo načel zasebnosti varnega pristana** v svoje politike obdelave podatkov. Na primer, posameznikom niso bile zmeraj dane jasne in pregledne informacije o namenih, za katere se njihovi podatki obdelujejo, ali niso imeli možnosti zavrnitve, če se naj bi njihovi osebni podatki razkrili tretji strani ali bi se uporabili za namen, ki ni združljiv z namenom, za katerega so bili prvotno zbrani. Komisija je v svojem poročilu iz leta 2004 menila, da bi moralo biti ministrstvo za trgovino *„dejavnejše pri dostopanju do varnega pristana in ozaveščanju o načelih“*[26].

V zvezi s tem je bil napredek skromen. Od 1. januarja 2009 ministrstvo za trgovino družbam, ki želijo obnoviti svoj status certificiranja za varni pristan, kar je treba storiti vsako leto, še pred obnovitvijo statusa pregleda politike varovanja zasebnosti. Vendar je ta presoja po obsegu omejena. Ne izvaja se **popolna presoja dejanskega stanja** v samocertificiranih družbah, kar bi bistveno povečalo verodostojnost postopka samocertificiranja.

---

[25] Od marca do septembra 2013 je ministrstvo za trgovino:
• uradno pozvalo 101 družbo, *ki je na spletno mesto o varnem pristanu že naložila svojo politiko varovanja zasebnosti, skladno z varnim pristanom,* naj svojo politiko varovanja zasebnosti objavi tudi na svojih spletnih mestih,
• uradno pozvalo 154 družb, ki v svojo politiko varovanja zasebnosti še niso vključile povezave do spletnega mesta o varnem pristanu, naj to storijo,
• uradno pozvalo več kot 600 družb, naj podatke za stik z njihovim neodvisnim ponudnikom alternativnega reševanja sporov vključijo v svojo politiko varovanja zasebnosti.

[26] Glej str. 8 poročila iz leta 2004 (SEC (2004) 1323).

Poleg zahtev Komisije, da ministrstvo za trgovino izvaja strožji in bolj sistematičen pregled nad samocertificiranimi družbami, **se zdaj več pozornosti namenja novo predloženim vlogam**. Število novo predloženih vlog, ki niso bile sprejete, temveč so bile vrnjene družbam z zahtevo, naj izboljšajo politike varovanja zasebnosti, se je med leti 2010 in 2013 znatno povečalo, in sicer se je podvojilo za družbe z obnovitvijo certificiranja in potrojilo za družbe, ki so vlogo predložile prvič[27]. Ministrstvo za trgovino je Komisiji zagotovilo, da je certificiranje ali obnovitev certificiranja končano šele, ko politika varovanja zasebnosti družbe izpolnjuje vse zahteve, zlasti obveznost zavezanosti k zadevnemu sklopu načel zasebnosti varnega pristana, in ko je javno dostopna. Družba mora v svoji evidenci seznama varnega pristana določiti lokacijo zadevne politike. Nadalje mora na svojem spletnem mestu jasno opredeliti ponudnika alternativnega reševanja sporov in vključiti povezavo do samocertificiranja varnega pristana na spletnem mestu ministrstva za trgovino. Kljub vsemu je bilo ocenjeno, da več kot 30 % članov varnega pristana v politikah varovanja zasebnosti na svojih spletnih mestih ne navaja informacij o reševanju sporov[28].

Večina družb, ki jih je ministrstvo za trgovino črtalo s seznama varnega pristana, je bila črtanih na izrecno zahtevo samih družb (na primer družb, ki so se združile ali bile prevzete, spremenile svojo dejavnost ali prenehale poslovati). Manjše število družb, katerih zaveze so potekle, je bilo črtanih po ugotovitvi, da spletna mesta, navedena v evidencah, ne delujejo in je status certificiranja družb že nekaj let „neaktualen“[29]. Pomembno je poudariti, da nobena družba ni bila črtana, ker bi ministrstvo za trgovino v svojih preverjanjih ugotovilo neizpolnjevanje načel.

Evidenca seznama varnega pristana je namenjena obveščanju javnosti in velja kot evidenca družbe o zavezanosti k varnemu pristanu. **Zavezanost k načelom varnega pristana ni časovno omejena**, kar zadeva podatke, pridobljene v času, ko družba uživa ugodnosti varnega pristana, zato mora načela za take podatke uporabljati, dokler jih hrani, uporablja ali razkriva, četudi pozneje iz kakršnega koli razloga izstopi iz varnega pristana.

Število **prosilcev** varnega pristana**, ki niso uspešno opravili upravnega pregleda** ministrstva za trgovino in zato nikoli niso bili vključeni na seznam varnega pristana, je sledeče: **leta 2010** zgolj **6 %**(ali 33 družb) od 513 prvič certificiranih družb nikoli ni bilo vključenih na seznam varnega pristana, ker niso ravnale v skladu s standardi ministrstva za trgovino glede samocertificiranja. Leta **2013 12 %** (ali 75 družb) od 605 prvič certificiranih družb nikoli ni bilo vključenih na seznam varnega pristana, ker niso ravnale v skladu s standardi ministrstva za trgovino glede samocertificiranja.

Za povečanje preglednosti pregleda bi moralo ministrstvo za trgovino na svojem spletnem mestu vsaj objaviti vse družbe, ki so bile črtane s seznama varnega pristana, in navesti razloge, zaradi katerih certificiranje ni bilo obnovljeno. Oznaka „neaktiven“ na seznamu družb članic varnega pristana ministrstva za trgovino se ne sme obravnavati zgolj kot

---

[27] Ministrstvo za trgovino je v svoji statistiki, ki jo je pripravilo septembra 2013, navedlo, da je leta 2010 uradno pozvalo 18 % (ali 93 družb) od 512 družb, ki so se certificirale prvič, in 16 % (ali 231 družb) od 1 417 družb, ki so se ponovno certificirale, naj izboljšajo svoje politike varovanja zasebnosti in/ali vloge za varni pristan. Potem ko je Komisija zahtevala strog, strokovno vesten in sistematični pregled vseh vlog, je v sredini septembra 2013 ministrstvo za trgovino uradno pozvalo 56 % (ali 340 družb) od 602, ki so se certificirale prvič, in 27 % (ali 493 družb) od 1 809 družb, ki so se ponovno certificirale, naj izboljšajo svoje politike varovanja zasebnosti.

[28] Nastop Chrisa Connollya (Galexia) pred preiskovalnem odborom v okviru Odbora za državljanske svoboščine, pravosodje in notranje zadeve Evropskega parlamenta 7. oktobra 2013.

[29] Ministrstvo za trgovino ZDA je od decembra 2011 s seznama varnega pristana črtalo 323 družb: 94 družb je bilo črtanih, ker niso več poslovale, 88 zaradi prevzema ali združitve družb, 95 na zahtevo matičnih družb, 41 družb zaradi večkratne nepredložitve obnovitve certificiranja in 5 družb zaradi raznih razlogov.

informacija, temveč ji mora biti pripisano **jasno opozorilo**, tako z besedami kot tudi grafično, da družba v tem času ne izpolnjuje zahtev varnega pristana.

Poleg tega nekatere družbe še zmeraj ne vključujejo vseh načel varnega pristana. Poleg vprašanja preglednosti, obravnavnega v oddelku 3 zgoraj, politike varovanja zasebnosti samocertificiranih družb pogosto niso jasne glede namenov, za katere se podatki zbirajo, in pravice do izbire, ali se podatki lahko razkrijejo tretjim stranem; tako se zastavlja vprašanje skladnosti z načeli obvestila in možnosti izbire. Ti dve načeli sta bistveni za zagotovitev, da lahko imajo posamezniki, na katere se nanašajo osebni podatki, nadzor nad tem, kaj se dogaja z njihovimi osebnimi podatki.

Ta ključni prvi korak v postopku zagotavljanja skladnosti, tj. vključitev načel zasebnosti varnega pristana v politike varovanja zasebnosti družb, ni zagotovljen v zadostni meri. Ministrstvo za trgovino bi ga moralo obravnavati prednostno in razviti metodologijo zagotavljanja skladnosti v operativni praksi družb in pri njihovem sodelovanju s strankami. **Ministrstvo za trgovino mora dejavno preverjati učinkovito vključitev načel varnega pristana v politike družb glede varovanja zasebnosti**, ne pa s pregonom čakati do vložitev pritožb posameznikov.

5. IZVRŠEVANJE S STRANI JAVNIH ORGANOV

Na voljo so številni mehanizmi za zagotovitev učinkovitega izvrševanja sheme varnega pristana in nudenje pravnih sredstev posameznikom v primerih, ko neizpolnjevanje načel varovanja zasebnosti vpliva na varstvo njihovih osebnih podatkov.

V skladu z načelom izvrševanja morajo politike varovanja zasebnosti samocertificiranih organizacij vsebovati učinkovite mehanizme skladnosti. V skladu z načelom izvrševanja, ki ga podrobneje pojasnjujejo FAQ 11, FAQ 5 in FAQ 6, je mogoče to zahtevo izpolniti z zavezanostjo k **neodvisnim pritožbenim mehanizmom** (IRM), ki so javno navedli, da imajo pristojnost za obravnavo posameznih pritožb glede neizpolnjevanja zavezanosti k načelom. Drugače pa je mogoče to doseči z zavezo organizacije, da bo sodelovala s **forumom za varstvo podatkov EU**[30]**.** Poleg tega spadajo samocertificirane družbe v pristojnost zvezne komisije za trgovino v skladu z oddelkom 5 zakona o zvezni komisiji za trgovino, ki prepoveduje nepoštena in goljufiva dejanja ali ravnanja v trgovini ali v zvezi s trgovino[31].

Komisija je v svojem poročilu iz leta 2004 izrazila zaskrbljenost glede izvajanja sheme varnega pristana in opozorila, da mora biti zvezna komisija za trgovino dejavnejša pri uvajanju preiskav in ozaveščanju posameznikov glede njihovih pravic. Skrb vzbuja tudi nezadostna jasnost v zvezi s pristojnostjo zvezne komisije za trgovino glede izvrševanja načel pri podatkih o človeških virih.

---

30 Forum za varstvo podatkov EU je organ, pristojen za preiskovanje in reševanje pritožb, ki jih vložijo posamezniki zaradi domnevnih kršitev načel varnega pristana s strani družbe iz ZDA, ki je članica varnega pristana. Družbe, ki certificirajo zavezanost k načelom varnega pristana, morajo izbrati, ali bodo upoštevale neodvisni pritožbeni mehanizem ali pa sodelovale s forumom za varstvo podatkov EU za namen odpravljanja težave zaradi neizpolnjevanja načel varnega pristana. Sodelovanje s forumom za varstvo podatkov EU je kljub vsemu obvezno, če družba iz ZDA obdeluje osebne podatke o človeških virih, ki jih prejme iz EU, za uporabo v okviru zaposlitvenih razmerij. Če se družba zaveže k sodelovanju s forumom EU, se mora zavezati tudi, da bo upoštevala vse nasvete tega foruma, kadar ta meni, da mora družba s posebnim ukrepom poskrbeti za izpolnjevanje načel varnega pristana, vključno s popravnimi ukrepi in plačilom odškodnin.

31 Ministrstvo za promet izvaja podobne pristojnosti nad letalskimi prevozniki v skladu z oddelkom 41712 iz naslova 49 zakonika Združenih držav.

Forum za varstvo podatkov EU, tj. pritožbeni organ, pristojen za podatke o človeških virih, je prejel eno pritožbo v zvezi s podatki o človeških virih[32]. Vendar na podlagi dejstva, da skoraj ni pritožb, ni mogoče sklepati, da shema v celoti deluje. Uvesti bi bilo treba preverjanje po uradni dolžnosti izpolnjevanja načel s strani družb, da bi se tako preverilo dejansko izvajanje zavez o varstvu podatkov. Organi za varstvo podatkov EU bi morali sprejeti tudi ukrepe za ozaveščanje o obstoju foruma.

Opozorjeno je bilo na težave v zvezi z načinom, kako alternativni pritožbeni mehanizmi delujejo kot organi pregona. Več teh organov nima ustreznih sredstev za odpravo primerov neizpolnjevanja načel. To pomanjkljivost je treba obravnavati.

5.1. Zvezna komisija za trgovino

Zvezna komisija za trgovino lahko v primeru kršitev zavez varnega pristana družb sprejme izvršilne ukrepe. Ob vzpostavitvi varnega pristana se je zvezna komisija za trgovino zavezala k prednostnemu pregledu vseh naznanitev, ki jih ji posredujejo organi držav članic EU[33]. Ker prvih deset let ureditve ni bila vložena nobena pritožba, se je zvezna komisija za trgovino odločila, da bo poskušala poiskati vse kršitve varnega pristana v vsaki preiskavi zasebnosti in varnosti podatkov, ki jo izvede. Od leta 2009 je zvezna komisija za trgovino uvedla deset pregonov zoper družbe zaradi kršenja varnega pristana. Njihov rezultat so odredbe za poravnavo – naložene stroge kazni – ki prepovedujejo lažne navedbe o zasebnosti, tudi o izpolnjevanju načel varnega pristana, in naložitev družbam obveznosti celovitih programov za varstvo in revizij za 20 let. Družbe morajo na zahtevo zvezne komisije za trgovino sprejeti neodvisne ocene svojih programov varovanja zasebnosti. O teh ocenah se redno poroča zvezni komisiji za trgovino. Njene odredbe tem družbam tudi prepovedujejo dajanje lažnih navedb o svojih praksah varovanja zasebnosti in o svoji udeležbi v varnem pristanu ali podobnih shemah varovanja zasebnosti. Takšen primer so preiskave zvezne komisije za trgovino zoper Google, Facebook in Myspace[34]. Leta 2012 je Google privolil v plačilo kazni v višini 22,5 milijona USD zaradi obtožb, da je kršil odredbo o soglasju. V vseh preiskavah varovanja zasebnosti zvezna komisija za trgovino po uradni dolžnosti preverja, ali gre za kršitev varnega pristana.

Zvezna komisija za trgovino je nedavno ponovila svoje izjave in zavezo k prednostnemu pregledu vseh naznanitev, ki jih predložijo družbe s samourejevalnim sistemom in države članice EU, ki domnevajo, da družba ne izpolnjujejo načel varnega pristana[35]. Evropski organi za varstvo podatkov so v zadnjih treh letih zvezni komisiji za trgovino predložili le nekaj naznanitev.

---

32 Pritožbo je vložil švicarski državljan in jo je zato forum za varstvo podatkov EU odstopil švicarskemu organu za varstvo podatkov (ZDA ima za Švico ločeno shemo varnega pristana).

33 Glej Prilogo V k Odločbi Komisije 2000/520/ES z dne 26. julija 2000.

34 V obdobju 2009–2012 je zvezna komisija za trgovino izvedla deset pregonov zaradi kršitev zavez varnega pristana: zvezna komisija za trgovino proti Javian Karnani, and Balls of Kryptonite, LLC (2009), World Innovators, Inc. (2009), Expat Edge Partners, LLC (2009), Onyx Graphics, Inc. (2009), Directors Desk LLC (2009), Progressive Gaitways LLC (2009), Collectify LLC (2009), Google Inc. (2011), Facebook, Inc. (2011) in Myspace LLC (2012). Glej: Zvezna komisija za trgovino za zaveze varnega pristana („Federal Trade Commission of Safe Harbour Commitments“): http://export.gov/build/groups/public/@eg_main/@SafeHarbour/documents/webcontent/eg_main_052211.pdf. Glej tudi: Odmevni primeri („Case Highlights“): http://business.ftc.gov/us-eu-Safe-Harbour-framework. Večina teh zadev je obravnavala težave z družbami, ki so se pridružile varnemu pristanu in se vseskozi predstavljale kot članice, ne da bi obnovile letno certificiranje.

35 To zavezo je komisarka Julie Brill ponovila na srečanju zvezne komisije za trgovino z organi za varstvo podatkov EU (delovna skupina iz člena 29) v Bruslju 17. aprila 2013.

V zadnjih mesecih se je začelo razvijati čezatlantsko sodelovanje med organi za varstvo podatkov. Zvezna komisija za trgovino je na primer 26. junija 2013 s komisarjem irskega urada za varstvo podatkov podpisala memorandum o soglasju o medsebojni pomoči pri izvrševanju zakonov o varstvu osebnih podatkov v zasebnem sektorju. Memorandum vzpostavlja okvir za tesnejše, bolj usmerjeno in učinkovitejše sodelovanje na področju izvrševanja varovanja zasebnosti[36].

Avgusta 2013 je zvezna komisija za trgovino najavila nadaljnje okrepitve pregledov družb z nadzorom nad večjo zbirko osebnih podatkov. Vzpostavila je tudi portal, na katerem lahko potrošniki vložijo pritožbo zaradi varovanja zasebnosti zoper ameriško družbo[37].

Zvezna komisija za trgovino mora tudi okrepiti prizadevanja za preiskave lažnih trditev o zavezanosti k varnemu pristanu. Družba, ki na svojem spletnem mestu trdi, da izpolnjuje zahteve o varnem pristanu, ampak na seznamu ministrstva za trgovino ni navedena kot „aktualen“ član sheme, zavaja potrošnike in zlorablja njihovo zaupanje. Lažne trditve slabijo verodostojnost celotnega sistema in jih je treba nemudoma odstraniti s spletnih mest družb. Družbe morajo biti vezane na izvršljive zahteve, da ne zavajajo potrošnikov. Zvezna komisija za trgovino mora še naprej poskušati identificirati lažne trditve o varnem pristanu kot v zadevi *Karnani*, ko je zaprla kalifornijsko spletno mesto zaradi lažnih navedb o registraciji varnega pristana, ter goljufivega ravnanja pri elektronskem trgovanju, namenjenem evropskim potrošnikom[38].

Zvezna komisija za trgovino je 29. oktobra 2013 objavila, da je v zadnjih mesecih uvedla „številne preiskave glede izvajanja varnega pristana“ in da je mogoče „v naslednjih mesecih“ pričakovati še več pregonov na tem področju. Potrdila je tudi, da „je odločena poiskati načine za izboljšanje učinkovitosti“ in da bo „tudi v prihodnje vesela zanesljivih informacij, kakršne je vsebovala pritožba, ki jo je pred meseci vložil evropski zagovornik potrošnikov in v kateri navaja domneve o večjem številu kršitev, povezanih z varnim pristanom“[39]. Agencija se je zavezala tudi k „sistematičnemu nadzoru izpolnjevanja odredb, kot to počnemo z vsemi našimi odredbami“[40].

Zvezna komisija za trgovino je 12. novembra 2013 obvestila Evropsko komisijo, da „**če družba v svoji politiki varovanja zasebnosti obljublja zaščito varnega pristana, neuspešna registracija ali nezmožnost njene ohranitve sami po sebi še ne razrešujeta zadevne družbe, da zvezna komisija za trgovino glede nje ne bi izvrševala zavez varnega pristana**“[41].

Novembra 2013 je ministrstvo za trgovino obvestilo Evropsko komisijo, da „bo za pomoč pri preprečevanju ‚lažnih trditev' o sodelovanju v varnem pristanu začelo vzpostavljati stik z udeleženci varnega pristana mesec pred njihovim rokom za obnovitev certificiranja in jim pojasnilo ukrepe, ki jih morajo sprejeti, če se ne odločijo za obnovitev certificiranja“. **Ministrstvo za trgovino „bo opozorilo družbe** v tej kategoriji, naj odstranijo vse sklice na udeležbo v varnem pristanu iz svojih politik varovanja zasebnosti in spletnih mest, tudi

---

36 http://www.dataprotection.ie/viewdoc.asp?Docid=1317&Catid=66&StartDate=1+January+2013&m=n.

37 Potrošniki lahko svoje pritožbe vložijo prek pomočnika za pritožbe zvezne komisije za trgovino (https://www.ftccomplaintassistant.gov/), mednarodni potrošniki pa lahko svoje pritožbe vložijo prek econsumer.gov (http://www.econsumer.gov).

38 http://www.ftc.gov/os/caselist/0923081/090806karnanicmpt.pdf.

39 http://www.ftc.gov/speeches/brill/131029europeaninstituteremarks.pdf in http://www.ftc.gov/speeches/ramirez/131029tacdremarks.pdf.

40 Pismo predsednice zvezne komisije za trgovino Edith Ramirez podpredsednici Komisije Viviane Reding.

41 Pismo predsednice zvezne komisije za trgovino Edith Ramirez podpredsednici Komisije Viviane Reding.

oznako certificiranja varnega pristana, **in jih bo jasno seznanilo z možnostjo uvedbe pregona s strani zvezne komisije za trgovino, če teh zahtev ne izpolnijo“**[42].

Za preprečevanje lažnih trditev o zavezanosti k varnemu pristanu morajo politike varovanja zasebnosti na spletnih mestih samocertificiranih družb vedno vključevati povezavo do spletnega mesta o varnem pristanu ministrstva za trgovino, na katerem so navedeni vsi „aktualni“ člani sheme. To bo evropskim posameznikom, na katere se nanašajo osebni podatki, omogočilo, da takoj in brez dodatnih poizvedb na spletu preverijo, ali je družba aktualna članica varnega pristana. Ministrstvo za trgovino je marca 2013 začelo to od družb zahtevati, vendar je treba proces pospešiti.

Stalno spremljanje in dosledno izvrševanje načel varnega pristana s strani zvezne komisije za trgovino sta poleg zgoraj navedenih ukrepov ministrstva za trgovino še naprej ključni prednostni nalogi za zagotovitev pravilnega in učinkovitega delovanja sheme. Zlasti je treba povečati **število pregledov po uradni dolžnosti in preiskav izpolnjevanja** načel varnega pristana s strani družb. Nadalje je treba olajšati vlaganje pritožb pri zvezni komisiji za trgovino zaradi kršitev zavez.

5.2. Forum za varstvo podatkov EU

Forum za varstvo podatkov EU je organ, ustanovljen z odločbo o varnem pristanu. Pristojen je za preiskave pritožb, ki jih vložijo posamezniki v zvezi z zbiranjem osebnih podatkov v okviru zaposlitvenega razmerja in v zvezi s certificiranimi družbami, ki so za reševanje sporov v okviru varnega pristana izbrale to možnost (53 % vseh družb). Sestavljajo ga predstavniki različnih organov za varstvo podatkov EU.

Do zdaj je forum prejel štiri pritožbe (dve leta 2010 in dve leta 2013). Pritožbi iz leta 2010 je posredoval nacionalnima organoma za varstvo podatkov (Združenega kraljestva in Švice). Preostali dve pritožbi se še proučujeta. Razlog za tako malo pritožb je lahko dejstvo, da so pristojnosti foruma, kot je bilo že omenjeno, načeloma omejene na določeno vrsto podatkov.

Delni razlog za omejeno število zadev je tudi, da forum ni dovolj dobro poznan. Komisija je leta 2004 zagotovila, da so informacije o forumu na njenem spletnem mestu vidnejše[43].

Da bi lahko družbe v ZDA, ki so se odločile sodelovati s forumom in ravnati v skladu z njegovimi odločbami za nekatere ali vse kategorije osebnih podatkov, zajete v njihovih samocertificiranjih, forum bolje izkoristile, morajo v svojih politikah varovanja zasebnosti to jasno in dobro prikazati, da se ministrstvu za trgovino omogoči, da opravi pregled v zvezi s tem. Za ozaveščanje evropskih družb in posameznikov, na katere se nanašajo osebni podatki, o varnem pristanu je treba na spletnih mestih vseh organov za varstvo podatkov EU vzpostaviti posebno stran, namenjeno varnemu pristanu.

---

42 „Sodelovanje med ZDA in EU pri izvajanju okvira varnega pristana“ z dne 12. novembra 2013.

43 Na podlagi poročila iz leta 2004 je bilo na spletnem mestu Komisije (GD za pravosodje) objavljeno informativno obvestilo v obliki vprašanj in odgovorov foruma za varstvo podatkov EU, da bi povečali ozaveščenost posameznikov in jim pomagali vložiti pritožbo, kadar menijo, da so bili njihovi osebni podatki obdelani na način, da so bila kršena načela varnega pristana: http://ec.europa.eu/justice/policies/privacy/docs/adequacy/information_Safe_harbour_en.pdf. Standardni obrazec za pritožbe je na voljo na: http://ec.europa.eu/justice/policies/privacy/docs/adequacy/ complaint_form_en.pdf.

5.3. Izboljšanje izvrševanja

Zgoraj ugotovljena šibkost pri preglednosti in izvrševanju je pri evropskih družbah vzbudila skrb o negativnem vplivu sheme varnega pristana na konkurenčnost evropskih družb. Kadar evropske družbe konkurirajo z ameriškimi družbami, ki so sicer zavezane k varnemu pristanu, v praksi pa njegovih načel ne spoštujejo, je evropska družba v podrejenem konkurenčnem položaju glede na ameriško družbo.

Poleg tega se pristojnosti zvezne komisije za trgovino razširjajo na nepoštena ali goljufiva dejanja ali ravnanja „v trgovini ali v zvezi s trgovino“. Oddelek 5 zakona o zvezni komisiji za trgovino je glede pooblastil zvezne komisije za trgovino v zvezi z nepoštenimi in goljufivimi dejanji in ravnanji uveljavil izjeme, med drugim v zvezi s **telekomunikacijami.** Ker telekomunikacijske družbe ne spadajo v pristojnost izvrševanja zvezne komisije za trgovino, se ne smejo zavezati k varnemu pristanu. Vendar so zaradi vse večje konvergence tehnologij in storitev številni njihovi neposredni tekmeci v ameriškem sektorju IKT člani varnega pristana. Izključitev telekomunikacijskih družb iz izmenjave podatkov v okviru sheme varnega pristana vzbuja skrb nekaterim evropskim telekomunikacijskim operaterjem. Po mnenju Združenja evropskih operaterjev telekomunikacijskih omrežij (ETNO) je „to v jasnem nasprotju z najpomembnejšo zahtevo telekomunikacijskih operaterjev v zvezi s potrebo po enakih konkurenčnih pogojih“[44].

6. OKREPITEV NAČEL ZASEBNOSTI VARNEGA PRISTANA

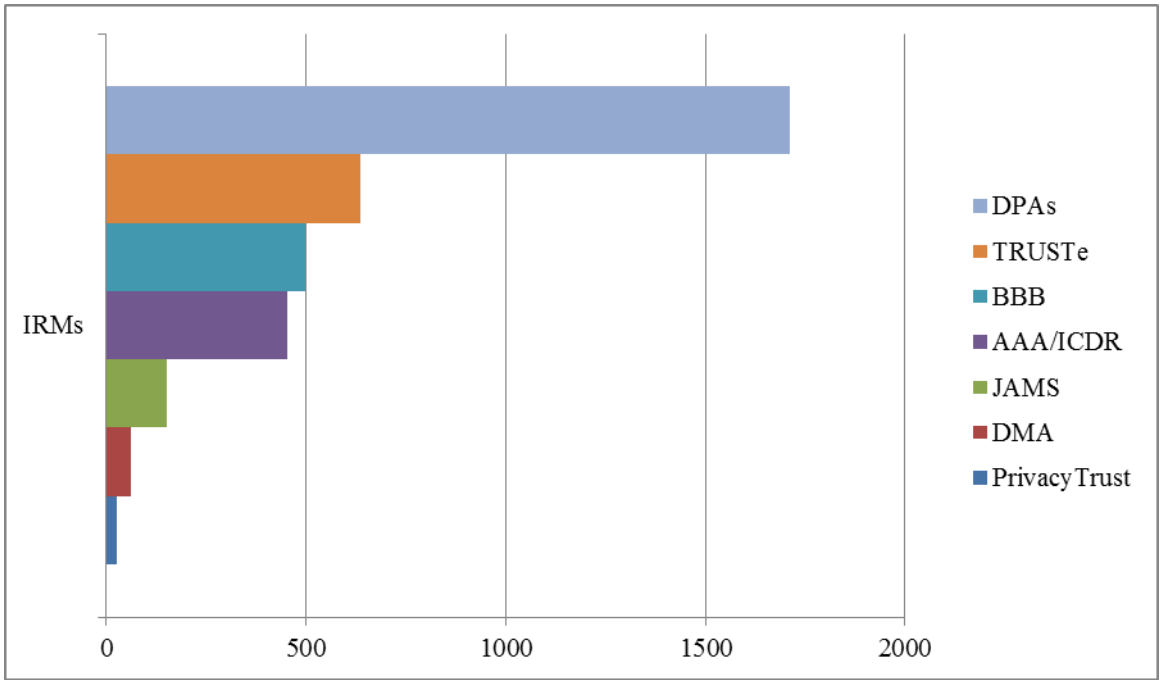
6.1. Alternativno reševanje sporov

Načelo izvrševanja zahteva „**lahko dostopne in stroškovno ugodne neodvisne pritožbene mehanizme,** ki omogočajo, da se pritožbe in spori vsakega posameznika preiščejo“. V ta namen vzpostavlja shema varnega pristana sistem alternativnega reševanja sporov (ARS), ki ga izvede neodvisna tretja stran[45], da bi posameznikom ponudila hitre rešitve. Trije najpomembnejši organi pritožbenega mehanizma so forum za varstvo podatkov EU, BBB (Better Business Bureaus) in TRUSTe.

---

[44] „Premisleki ETNO“, ki so jih 4. oktobra 2013 prejele službe Komisije, obravnavajo tudi 1) opredelitev osebnih podatkov v varnem pristanu, 2) pomanjkanje nadzora nad varnim pristanom in 3) dejstvo, da „lahko ameriške družbe podatke prenašajo z veliko manj omejitvami kot evropske družbe“, kar povzroča „jasno diskriminacijo evropskih družb in vpliva na njihovo konkurenčnost“. V skladu s pravili varnega pristana morajo organizacije ob razkritju podatkov tretji strani uporabiti načeli obvestila in možnosti izbire. Kadar želi organizacija razkriti podatke tretji strani, ki je v vlogi posrednika, lahko to stori, če je bodisi tretja stran pristopila k načelom ali je podvržena Direktivi ali je zajeta z drugo primerno zaščito podatkov bodisi da s to tretjo stranjo sklene pisni sporazum, po katerem mora tretja stran zagotoviti vsaj takšno raven varstva zasebnosti, kakor jo zahtevajo ustrezna načela.

[45] Direktiva 2013/11/EU o alternativnem reševanju potrošniških sporov poudarja pomen neodvisnih, nepristranskih, preglednih, učinkovitih, hitrih in pravičnih postopkov alternativnega reševanja sporov.



Uporaba ARS se je od leta 2004 povečala in ministrstvo za trgovino je okrepilo nadzor nad ameriškimi ponudniki ARS, da bi se zagotovilo, da so informacije, ki jih ponujajo glede pritožbenega postopka, jasne, dostopne in razumljive. Vendar pa je treba učinkovitost tega sistema še dokazati glede na to, da je bilo do zdaj obravnavano le omejeno število zadev[46].

Čeprav je bilo ministrstvo za trgovino uspešno pri znižanju provizij, ki jih zaračunavajo ponudniki ARS, dva od sedmih večjih ponudnikov ARS posameznikom, ki vložijo pritožbo, še naprej zaračunavajo provizijo[47]. To so ponudniki ARS, ki jih uporablja 20 % družb iz varnega pristana. Te družbe so izbrale ponudnika ARS, ki potrošnikom zaračunava provizijo za vložitev pritožbe. Takšne prakse niso v skladu z načelom izvrševanja varnega pristana, ki daje posameznikom pravico dostopa do „lahko dostopnih in stroškovno ugodnih neodvisnih pritožbenih mehanizmov“. V Evropski uniji je dostop do neodvisne storitve reševanja sporov, ki jo nudi forum za varstvo podatkov EU, brezplačen za vse posameznike, na katere se nanašajo osebni podatki.

---

46 Na primer, eden večjih ponudnikov storitev („TRUSTe“) je poročal, da je leta 2010 prejel 881 zahtevkov, vendar so bili le trije ustrezni in utemeljeni ter je bilo mogoče na njihovi podlagi od zadevne družbe zahtevati, da spremeni svojo politiko varovanja zasebnosti in spletno mesto. Leta 2011 je bilo 879 pritožb in le v enem primeru je bila družba pozvana, naj spremeni svojo politiko varovanja zasebnosti. Po navedbah ministrstva za trgovino gre pri veliki večini pritožb pri ponudnikih ARS za zahtevke potrošnikov, na primer uporabnikov, ki so pozabili svoje geslo in ga niso mogli pridobiti od ponudnika internetne storitve. Po pozivu Komisije je ministrstvo za trgovino razvilo nova merila za statistično poročanje, ki ga morajo uporabljati vsi ponudniki ARS. Ta razlikujejo med zahtevki in pritožbami ter jasno opredeljujejo vrsto prejete pritožbe. Vendar je treba ta merila še obravnavati, da bo lahko nova statistika za leto 2014 zajela vse ponudnike ARS, da bo primerljiva in da bo zagotovila potrebne informacije za oceno učinkovitosti pritožbenega mehanizma.

47 Mednarodni center za reševanje sporov/Ameriško arbitražno združenje (ICDR/AAA) zaračunavata 200 USD, JAMS pa 250 USD „provizije za vložitev pritožbe“. Ministrstvo za trgovino je Komisijo obvestilo, da je sodelovalo z AAA, tj. najdražjim ponudnikom storitev reševanja sporov, pri razvoju posebnega programa o varnem pristanu, s katerim so se znižali stroški za potrošnike z več tisoč dolarjev na pavšalni znesek 200 USD.

Ministrstvo za trgovino je 12. novembra 2013 potrdilo, da „se bo v imenu EU še naprej zavzemalo za varnost zasebnosti državljanov EU in da bo sodelovalo s ponudniki ARS, da se ugotovi, ali je mogoče njihove provizije še znižati“.

Kar zadeva sankcije, nimajo vsi ponudniki ARS potrebnih orodij za odpravo kršitev načel varovanja zasebnosti. Poleg tega objava ugotovitev o neizpolnjevanju načel ni predvidena med naborom sankcij in ukrepov nobenega od ponudnikov storitev ARS.

Ponudniki ARS so bili tudi pozvani, naj zadeve predložijo zvezni komisiji za trgovino, če družba ne ravna tako, kot predvideva izid postopka ARS ali zavrača odločitev ponudnika ARS, da lahko zvezna komisija za trgovino zadevo prouči in preišče ter po potrebi sprejme izvršilne ukrepe. Vendar do zdaj še noben ponudnik ARS zvezni komisiji za trgovino ni predložil takšne zadeve[48].

Ponudniki storitev alternativnega reševanja sporov vodijo na svojih spletnih mestih seznam družb (udeležencev reševanja spora), ki uporabljajo njihove storitve. To omogoča potrošnikom, da lahko preprosto preverijo, ali lahko v primeru spora z družbo posameznik vloži pritožbo pri opredeljenem ponudniku reševanja sporov. Tako denimo vodi ponudnik reševanja sporov BBB seznam vseh družb v sistemu za reševanje sporov BBB. Vendar številne družbe trdijo, da so vključene v poseben sistem reševanja sporov, vendar pri ponudniku storitev ARS niso navedene kot članice njihove sheme za reševanje sporov[49].

Mehanizmi ARS morajo biti za posameznike lahko dostopni, neodvisni in stroškovno ugodni. Posameznik, na katerega se nanašajo osebni podatki, mora imeti možnost vložitve pritožbe brez pretiranih omejitev. Vsi organi ARS morajo na svojih spletnih mestih objaviti statistiko o obdelanih pritožbah in posebne informacije o njihovem izidu. Organe ARS je treba še naprej spremljati, da se zagotovi, da so predložene informacije o postopku in o tem, kako vložiti pritožbo, jasne in razumljive, tako da bo postalo reševanje sporov učinkovit in verodostojen mehanizem, ki prinaša rezultate. Ponovno je treba tudi poudariti, da je treba objavo ugotovitev o neizpolnjevanju načel vključiti med nabor obveznih sankcij organov ARS.

6.2. Prenos tretjemu

Zaradi eksponentnega naraščanja prenosa podatkov je treba zagotoviti stalno varstvo osebnih podatkov na vseh stopnjah obdelave podatkov, zlasti ko družba, zavezana k varnemu pristanu, prenaša podatke **tretji strani, ki izvaja obdelavo**. Zato potreba po boljšem izvrševanju varnega pristana ne zadeva le članov varnega pristana, temveč tudi podizvajalce.

Shema varnega pristana omogoča prenos tretjim stranem v vlogi „posrednika“, če družba, ki je članica sheme varnega pristana, potrdi, da je „bodisi tretja stranka pristopila k načelom ali je podvržena Direktivi ali je zajeta z drugo primerno zaščito podatkov bodisi da s to tretjo stranko sklene pisni sporazum, po katerem mora tretja stranka zagotoviti vsaj takšno raven varstva zasebnosti, kakor jo zahtevajo ustrezna načela“[50]. Na primer, ministrstvo za trgovino od ponudnika storitve računalništva v oblaku zahteva podpis pogodbe, četudi „se ravna v

---

48 Glej FAQ 11.

49 Primeri: Amazon je obvestil ministrstvo za trgovino, da kot ponudnika reševanja sporov uporablja BBB. Vendar ni naveden na BBB-jevem seznamu udeležencev reševanja sporov. Nasprotno pa je družba Arsalon Technologies (www.arsalon.net), ki je ponudnik storitve računalništva v oblaku, na BBB-jevem seznamu reševanja sporov v zvezi z varnim pristanom, ni pa aktualna članica varnega pristana (stanje na dan 1. oktobra 2013). BBB, TRUSTe in drugi ponudniki storitve ARS morajo odstraniti ali popraviti trditve o certificiranju. Zavezani morajo biti izvršljivi zahtevi, da certificirajo samo družbe, ki so članice varnega pristana.

50 Glej Odločbo Komisije 2000/520/ES, str. 7 (prenos tretjemu).

skladu z varnim pristanom“ in dobiva osebne podatke v obdelavo[51]. Vendar ta določba v Prilogi II k odločbi o varnem pristanu ni jasna.

Zaradi znatnega povečanja uporabe podizvajalcev v zadnjih letih, zlasti pri računalništvu v oblaku, mora družba, ki je članica varnega pristana, o podpisu take pogodbe obvestiti ministrstvo za trgovino in mora biti zavezana objaviti takšne ukrepe za varstvo zasebnosti[52].

Tri zgoraj navedena vprašanja, tj. mehanizem alternativnega reševanja sporov, okrepljen pregled in prenos podatkov tretjemu, je treba podrobneje razjasniti.

7. DOSTOP DO PODATKOV, PRENESENIH V OKVIRU SHEME VARNEGA PRISTANA

Med letom 2013 so informacije o obsegu programov nadzora v ZDA vzbudile skrb o kontinuiteti varstva osebnih podatkov, zakonito prenesenih v ZDA v okviru sheme varnega pristana. Tako se na primer zdi, da so vse družbe, ki so vključene v program PRISM in ki organom v ZDA dovoljujejo dostop do podatkov, shranjenih in obdelanih v ZDA, certificirane za varni pristan. S tem je shema varnega pristana postala ena od kanalov, po katerih je ameriškim obveščevalnim organom omogočen dostop do zbiranja osebnih podatkov, prvotno obdelanih v EU.

Odločba o varnem pristanu v Prilogi I določa, da je zavezanost k načelom lahko omejena, če je to potrebno za izpolnjevanje zahtev nacionalne varnosti, javnega interesa ali odkrivanja in pregona ali je omejena z zakonom, vladnim podzakonskim aktom ali sodno prakso. Da bi bile omejitve in zadržki glede uživanja temeljnih pravic veljavne, jih je treba razlagati ozko; določene morajo biti v javno dostopni zakonodaji ter morajo biti nujno potrebne in sorazmerne v demokratični družbi. Odločba o varnem pristanu določa zlasti, da so takšne omejitve dovoljene le, **„če je to potrebno“** za izpolnjevanje zahtev nacionalne varnosti, javnega interesa ali odkrivanja in pregona[53]. Izredna obdelava podatkov za namene nacionalne varnosti, javnega interesa ali odkrivanja in pregona je v okviru sheme varnega pristana sicer dovoljena, vendar v času sprejemanja varnega pristana tako obsežen dostop

---

[51] Glej: Pojasnila glede okvira varnega pristana med ZDA in EU ter računalništva v oblaku („Clarifications Regarding the U.S.-EU Safe Harbor Framework and Cloud Computing“): http://export.gov/static/Safe%20Harbor%20and%20Cloud%20Computing%20Clarification_April%2012%202013_Latest_eg_main_060351.pdf.

[52] Te pripombe se nanašajo na ponudnike računalništva v oblaku, ki niso člani varnega pristana. Po informacijah podjetja za svetovanje Galexia je „raven članstva v varnem pristanu (in upoštevanje načel) med ponudniki računalništva v oblaku kar visoka. Ponudniki računalništva v oblaku imajo praviloma več plasti varstva zasebnosti, saj pogosto kombinirajo neposredne pogodbe s strankami in obsežne politike varovanja zasebnosti. Z eno ali dvema pomembnima izjemama ponudniki računalništva v oblaku, ki so člani varnega pristana, upoštevajo glavne določbe v zvezi z reševanjem sporov in izvrševanjem. V tem času ni večjih ponudnikov računalništva v oblaku, ki bi bili zabeleženi na seznamu kot tisti, ki lažno trdijo, da so člani varnega pristana.“ (nastop Chrisa Connollya iz podjetja Galexia pred preiskovalnim odborom v okviru Odbora za državljanske svoboščine, pravosodje in notranje zadeve o „elektronskem množičnem nadzoru državljanov EU“).

[53] Glej Prilogo I k odločbi o varnem pristanu: „Zavezanost k načelom je lahko omejena: (a) če je to potrebno za izpolnjevanje zahtev nacionalne varnosti, javnega interesa ali odkrivanja in pregona; (b) z zakonom, vladnim podzakonskim aktom ali sodno prakso, ki ustvarijo nezdružljivost obveznosti ali izrecnih pooblastil, pod pogojem, da lahko organizacija pri izvajanju takih pooblastil dokaže, da je njeno neizpolnjevanje načel toliko omejeno, kolikor je potrebno za izpolnitev prednostnih zakonitih interesov na podlagi takšnih pooblastil; ali (c) če direktiva ali pravo države članice dovoljuje izjeme in odstopanja, če da se te izjeme in odstopanja uporabljajo v primerljivih okoliščinah. V skladu s ciljem krepitve varstva zasebnosti si morajo organizacije prizadevati, da načela uveljavijo v celoti in pregledno, vključno z navedbo v svoji politiki varstva zasebnosti, kdaj se bodo izjeme, dovoljene z (b) zgoraj, redno uporabljale. Iz istega razloga se od organizacij pričakuje, da se, kadar načela in/ali pravo ZDA dopuščajo izbiro, po možnosti odločijo za možnost večjega varstva.“

obveščevalnih agencij do podatkov, prenesenih v ZDA v okviru trgovinskih poslov, ni bil predviden.

Poleg tega bi zaradi preglednosti in pravne varnosti ministrstvo za trgovino moralo obvestiti Evropsko komisijo o vseh zakonih ali vladnih podzakonskih aktih, ki bi lahko vplivali na zavezanost k načelom zasebnosti varnega pristana[54]. Uporabo izjem je treba strogo nadzorovati in se jih ne sme uporabljati na način, ki ogroža zaščito, zagotovljeno z **načeli**[55]. Zlasti obsežen dostop ameriških organov do podatkov, ki jih obdelujejo samocertificirane družbe v okviru varnega pristana, pomeni tveganje za razvrednotenje zaupnosti elektronske komunikacije.

7.1. Sorazmernost in nujnost

Kot kažejo ugotovitve posebej ustanovljene delovne skupine za varstvo podatkov EU-ZDA, številne pravne podlage zakonodaje ZDA omogočajo obsežno zbiranje in obdelovanje osebnih podatkov, ki jih shranjujejo ali drugače obdelujejo družbe s sedežem v ZDA. Zadeva lahko podatke, ki so bili predhodno preneseni iz EU v ZDA v okviru sheme varnega pristana, in zato zastavlja vprašanje stalnega izpolnjevanja načel varnega pristana. Zaradi obsežne narave teh programov lahko ameriški organi dostopajo do podatkov, prenesenih v okviru sheme varnega pristana, in jih nadalje obdelujejo v večji meri, kot je nujno potrebno in sorazmerno za zaščito nacionalne varnosti, kot to predvidevajo izjeme v odločbi o varnem pristanu.

7.2. Omejitve in možnosti pravnega varstva

Kot kažejo ugotovitve posebej ustanovljene delovne skupine za varstvo podatkov EU-ZDA, je varstvo, ki ga določa pravo ZDA, večinoma zagotovljeno ameriškim državljanom ali tamkajšnjim zakonitim prebivalcem. Poleg tega ni mogoče, da bi posamezniki iz EU ali ZDA, na katere se nanašajo osebni podatki, lahko dostopali do podatkov, jih popravljali ali izbrisali ali imeli dostop do upravnega ali sodnega varstva zaradi zbiranja in nadaljnje obdelave svojih osebnih podatkov v okviru ameriških programov nadzora.

7.3. Preglednost

Družbe v svojih politikah varovanja zasebnosti ne navajajo sistematično, kdaj uporabljajo izjeme od načel. Tako posamezniki in družbe ne vedo, kaj se dogaja z njihovimi podatki. To je še zlasti pomembno v zvezi z delovanjem zadevnih programov nadzora ZDA. Zato morda Evropejce, katerih podatki se prenesejo družbi v ZDA v okviru varnega pristana, zadevne družbe ne obvestijo, da lahko do njihovih podatkov dostopajo tretje strani[56]. To sproža vprašanje skladnosti z načeli varnega pristana glede preglednosti. Preglednost je treba zagotoviti v največji možni meri, ne da bi bila ogrožena nacionalna varnost. Poleg obstoječih zahtev, da morajo družbe v svojih politikah varovanja zasebnosti navesti, kdaj so načela lahko

---

54 Mnenje 4/2000 o ravni zaščite, ki jo zagotavljajo „načela varnega pristana“, ki ga je 16. maja 2000 sprejela delovna skupina o varstvu podatkov iz člena 29.

55 Mnenje 4/2000 o ravni zaščite, ki jo zagotavljajo „načela varnega pristana“, ki ga je 16. maja 2000 sprejela delovna skupina o varstvu podatkov iz člena 29.

56 Razmeroma pregledne informacije v zvezi s tem ponujajo nekatere evropske družbe v okviru varnega pristana. Nokia na primer, ki posluje v ZDA in je članica varnega pristana, ima v svoji politiki varovanja zasebnosti zapisano naslednje obvestilo: *„Zaradi veljavne zakonodaje bomo morda morali razkriti vaše osebne podatke določenim organom ali drugim tretjim stranem, na primer organom pregona v državah, v katerih poslujemo mi ali tretje strani v vlogi našega posrednika.“*

omejena z zakonom, vladnim podzakonskim aktom ali sodno prakso, je treba družbe spodbujati tudi k temu, da v svojih politikah varovanja zasebnosti navedejo, kdaj uporabljajo izjeme od načel, da izpolnijo zahteve nacionalne varnosti, javnega interesa ali odkrivanja in pregona.

8. ZAKLJUČKI IN PRIPOROČILA

Od sprejetja varnega pristana leta 2000 je ta postal nosilec prenosa osebnih podatkov med EU in ZDA. Učinkovita zaščita pri prenosu osebnih podatkov je zaradi eksponentnega naraščanja prenosa podatkov, ključnih za digitalno gospodarstvo, ter pomembnega razvoja pri zbiranju, obdelavi in uporabi podatkov postala še pomembnejša. Spletna podjetja, kot so Google, Facebook, Microsoft, Apple in Yahoo, imajo več sto milijonov strank v Evropi in prenašajo osebne podatke za obdelavo v ZDA v obsegu, ki je bil ob sprejetju varnega pristana leta 2000 nepredstavljiv.

Zaradi nezadovoljive preglednosti in nepravilnosti pri izvajanju te ureditve še vedno obstajajo določene težave, ki jih je treba obravnavati:

a) preglednost politik članov varnega pristana glede varovanja zasebnosti,

b) učinkovita uporaba načel zasebnosti s strani družb v ZDA in

c) učinkovitost pri njihovem izvrševanju.

Poleg tega **obsežen dostop obveščevalnih agencij do podatkov, ki jih v ZDA prenašajo družbe, certificirane v okviru varnega pristana**, sproža še dodatna resna vprašanja glede kontinuitete pravic do varstva podatkov Evropejcev, kadar se njihovi podatki prenašajo v ZDA.

Komisija je na podlagi zgoraj navedenega opredelila naslednja **priporočila**:

Preglednost

1. *Samocertificirane družbe bi morale javno objaviti svoje politike varovanja zasebnosti*. Ne zadostuje, če družbe ministrstvu za trgovino predložijo opis svoje politike varovanja zasebnosti. Te politike morajo biti javno dostopne na spletnih mestih družb, napisane pa morajo biti v jasnem in nedvoumnem jeziku.

2. *Politike varovanja zasebnosti na spletnih mestih samocertificiranih družb bi morale vedno vključevati povezavo do spletnega mesta o varnem pristanu ministrstva za trgovino, na katerem so navedeni vsi „aktualni" člani sheme*. To bo evropskim posameznikom, na katere se nanašajo osebni podatki, omogočilo, da takoj in brez dodatnih poizvedb na spletu preverijo, ali je družba aktualna članica varnega pristana. To bi pripomoglo k povečanju verodostojnosti sheme, saj bi se zmanjšale možnosti lažnih navedb o zavezanosti k varnemu pristanu. Ministrstvo za trgovino je marca 2013 začelo to od družb zahtevati, vendar je treba proces pospešiti.

3. *Samocertificirane družbe bi morale objaviti pogoje varovanja zasebnosti iz vseh pogodb, ki jih sklenejo s podizvajalci, na primer pri storitvah računalništva v oblaku*. Varni pristan omogoča prenos podatkov družb, samocertificiranih v okviru varnega pristana, tretjim stranem v vlogi „posrednika", na primer ponudnikom storitev računalništva v oblaku. Kolikor nam je znano, v takšnih primerih ministrstvo za trgovino od samocertificiranih družb zahteva, da sklenejo pogodbo. Vendar bi morala družba iz varnega pristana o sklenitvi pogodbe obvestiti ministrstvo za trgovino in bi morala biti zavezana objaviti takšne ukrepe varovanja zasebnosti.

4. *Na spletnem mestu ministrstva za trgovino bi bilo treba jasno označiti vse družbe, ki niso aktualne članice sheme.* Oznaki „neaktualni“ član na seznamu družb članic varnega pristana ministrstva za trgovino mora biti pripisano jasno opozorilo, da družba v tem času ne izpolnjuje zahtev varnega pristana. Vendar je družba tudi v primeru, ko ni aktualna članica varnega pristana, obvezana, da še naprej izpolnjuje zahteve varnega pristana za podatke, ki jih je prejela v okviru varnega pristana.

Pravna sredstva

5. *Politike varovanja zasebnosti na spletnih mestih družb bi morale vključevati povezavo na ponudnika alternativnega reševanja sporov (ARS) in/ali forum EU.* To bo evropskim posameznikom, na katere se nanašajo osebni podatki, omogočilo, da v primeru težav nemudoma vzpostavijo stik s ponudnikom ARS ali forumom EU. Ministrstvo za trgovino je marca 2013 začelo to od družb zahtevati, vendar je treba proces pospešiti.
6. *ARS bi moral biti lahko dostopen in stroškovno ugoden*. Nekateri organi ARS v shemi varnega pristana od posameznikov še zmeraj zaračunavajo provizijo za obdelavo pritožbe, ki pa je lahko za posameznega uporabnika zelo visoka (200–250 USD). Nasprotno pa je v Evropi dostop do foruma za varstvo podatkov, katerega naloga je reševanje pritožb v okviru varnega pristana, brezplačen.

7. *Ministrstvo za trgovino bi moralo bolj sistematično spremljati ponudnike ARS glede preglednosti in dostopnosti do informacij, ki jih zagotovijo o postopku, ki ga uporabljajo, in o nadaljnjih ukrepih glede pritožb.* S tem bo postalo reševanje sporov učinkovit in verodostojen mehanizem, ki prinaša rezultate. Ponovno bi bilo treba tudi poudariti, da je treba objavo ugotovitev o neizpolnjevanju načel vključiti med nabor obveznih sankcij organov ARS.

Izvrševanje

8. *Po certificiranju ali ponovnem certificiranju družb v okviru varnega pristana bi bilo treba pri določenemu odstotku teh družb po uradni dolžnosti preveriti, ali učinkovito uveljavljajo svoje politike varovanja zasebnosti (preveriti več kot le izpolnjevanje formalnih zahtev).*

9. *Kadar se na podlagi pritožbe ali preiskave ugotovi, da družba ne izpolnjuje načel varnega pristana, bi bilo treba pri njej po enem letu opraviti posebno naknadno preiskavo.*

10. *V primeru dvomov o izpolnjevanju načel s strani družbe ali še nerešene pritožbe mora ministrstvo za trgovino o tem obvestiti pristojni organ za varstvo podatkov EU.*

11. *Še naprej bi bilo treba preiskovati lažne trditve o zavezanosti k varnemu pristanu.* Družba, ki na svojem spletnem mestu trdi, da izpolnjuje zahteve o varnem pristanu, vendar na seznamu ministrstva za trgovino ni navedena kot „aktualen“ član sheme, zavaja potrošnike in zlorablja njihovo zaupanje. Lažne trditve slabijo verodostojnost celotnega sistema in bi jih bilo treba nemudoma odstraniti s spletnih mest družbe.

Dostop organov ZDA

12. *Politike samocertificiranih družb glede varovanja zasebnosti bi morale vsebovati informacije o obsegu, v katerem pravo ZDA javnim organom dovoljuje, da zbirajo in obdelujejo podatke, prenesene v okviru varnega pristana. Družbe bi bilo treba predvsem spodbujati, da v svojih politikah varovanja zasebnosti navedejo, kdaj uporabljajo izjeme od načel, da izpolnijo zahteve nacionalne varnosti, javnega interesa ali odkrivanja in pregona.*

13. *Pomembno je, da se izjema, ki jo odločba o varnem pristanu določa za zagotavljanje nacionalne varnosti, uporablja le v obsegu, ki je nujno potreben ali sorazmeren.*